DEGENERATE FOURFOLD MASSEY PRODUCTS OVER ARBITRARY FIELDS

ALEXANDER MERKURJEV AND FEDERICO SCAVIA

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 DGA of the absolute Galois group is not formal.

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 an absolute Galois group: it admits a presentation with generators in degree 1 and relations in degree 2.

Let p be a prime number, F be a field, and Γ_F be the absolute Galois group of F. For all $n \geq 3$ and $\chi_1, \dots, \chi_n \in H^1(F, \mathbb{Z}/p\mathbb{Z})$, 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 that $\langle \chi_1, \dots, \chi_n\rangle$ is defined if it is non-empty, and that it vanishes if it contains 0. In [HW15], Hopkins and Wickelgren proved that all Massey products vanish when $n = 3$, $p = 2$ and F is a number field. This was later generalized to the case when the field F is arbitrary by Mináč and Tân [MT17b]. Inspired by these results, Mináč and Tân [MT15a] made 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 $\langle \chi_1, \dots, \chi_n\rangle \in H^2(F, \mathbb{Z}/p\mathbb{Z})$ is defined, then it vanishes.*

Date: August 2022.

2020 *Mathematics Subject Classification.* 12G05; 55S30, 11E04.

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

It was observed by Mináč and Tân that the all mod p Massey products are defined and vanish when F has characteristic p; see [MT17b, Remark 4.1]. Therefore, one may assume that $\mathrm{char}(F) \neq p$ in Conjecture 1.1. Moreover, if F contains a primitive p-th root of unity (this is automatic if $p = 2$), then by Kummer theory homomorphisms $\Gamma_F \to \mathbb{Z}/p\mathbb{Z}$ correspond to elements of $F^\times/F^{\times p}$, 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 $a_1, \ldots, a_n \in F^\times$, the Massey product $\langle a_1, \ldots, a_n\rangle$ 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–Matzri and Mináč–Tân [Mat14, EM17, MT16]. Conjecture 1.1 is also true when F is a number field, by Guillot–Mináč–Topaz–Wittenberg [GMT18] for the case $p = 2$ and $n = 4$, and Harpaz–Wittenberg [HW19] for the case of arbitrary p and $n \geq 3$.

If the mod p Massey product $\langle \chi_1, \ldots, \chi_n\rangle$ is defined, then $\chi_1 \cup \chi_2 = \cdots = \chi_{n-1} \cup \chi_n = 0$ in $H^2(F, \mathbb{Z}/p\mathbb{Z})$; see Remark 2.2. In [MT17a, Question 4.2], Mináč and Tân asked whether the converse is also true.

Question 1.2 (Mináč, Tân)**.** *Let F be a field, p be a prime number and $n \geq 3$ be an integer. Is it true that for all $\chi_1, \ldots, \chi_n \in H^1(F, \mathbb{Z}/p\mathbb{Z})$ such that $\chi_1 \cup \chi_2 = \cdots = \chi_{n-1} \cup \chi_n = 0$ in $H^2(F, \mathbb{Z}/p\mathbb{Z})$, the Massey product $\langle \chi_1, \ldots, \chi_n\rangle$ is defined?*

Again, if F contains a primitive p-th root of unity, by Kummer theory we may replace elements of $H^1(F, \mathbb{Z}/p\mathbb{Z})$ by elements of $F^\times$. Question 1.2 has affirmative answer when $n = 3$. However, Harpaz and Wittenberg produced a counterexample to Question 1.2, for $n = 4$, $p = 2$ and $F = \mathbb{Q}$; see [GMT18, Example A.15]. More precisely, if $b = 2$, $c = 17$ and $a = d = bc = 34$, then $(a, b) = (b, c) = (c, d) = 0$ in $\mathrm{Br}(\mathbb{Q})$ but $\langle a, b, c, d\rangle$ is not defined over $\mathbb{Q}$. We will refer to this example as the Harpaz–Wittenberg example. In contrast, [GMT18, Theorem 6.2] shows that over any number field F and a, b, c, d are independent in $F^\times/F^{\times 2}$, the identity $(a, b) = (b, c) = (c, d) = 0$ in $\mathrm{Br}(F)$ 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. This is the topic of the present article. 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 $p = 2$, F be a field of characteristic different from 2, and $a, b, c, d \in F^\times$ 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 $p = 2$, F be a field of characteristic different from 2, and $a, b, c, d \in F^\times$ 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 $\mathrm{Br}(F)$ and $-1 \in N_{b,c}$.

Here $N_{b,c}$ denotes the image of the norm map $F_{b,c}^{\times} \to F^{\times}$, 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 write $C^{\cdot}(F, \mathbb{Z}/p\mathbb{Z})$ for the DGA of mod p continuous cochains of Γ_F. We say that $C^{\cdot}(F, \mathbb{Z}/p\mathbb{Z})$ is formal if it is quasi-isomorphic to its cohomology algebra $H^{\cdot}(F, \mathbb{Z}/p\mathbb{Z})$, viewed as a DGA with zero differential. If $C^{\cdot}(F, \mathbb{Z}/p\mathbb{Z})$ is formal, then Conjecture 1.1 holds for F and Question 1.2 has a positive answer for F. In [HW15, Question 1.4], Hopkins and Wickelgren asked whether $C^{\cdot}(F, \mathbb{Z}/p\mathbb{Z})$ is formal for every field F. Positselski [Pos17, Example 6.3] showed that the answer to Hopkins and Wickelgren's question is negative. More precisely, Positselski showed that $C^{\cdot}(F, \mathbb{Z}/p\mathbb{Z})$ 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 affirmative answer for local fields.) The Harpaz–Wittenberg example shows that $C^{\cdot}(F, \mathbb{Z}/p\mathbb{Z})$ is not formal for $F = \mathbb{Q}(\sqrt{2}, \sqrt{17})$. The following refinement of the question of Hopkins and Wickelgren, due to Positselski [Pos17, p. 226], is well known among experts.

Question 1.5 (Positselski)**.** *Do there exist a prime number p and field F of characteristic different from p and containing all the p-power roots of unity such that $C^{\cdot}(F, \mathbb{Z}/p\mathbb{Z})$ 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 exist 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, when $n = 4$ there are no such examples if we further assume that $a = bc$.) In view of recent work of Quadrelli [Qua22], 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 $U_{n+1} \subset \mathrm{GL}_{n+1}(\mathbb{F}_2)$ be the group of unipotent upper triangular matrices, and let $\overline{U}_{n+1}$ be the group of unipotent upper triangular matrices with entry $(1, n+1)$ erased; see (2.3). 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 [Dwy75], the Massey product $\langle a, b, c, d \rangle$ is defined (resp. vanishes) if and only $F_{a,b,c,d}/F$ can be embedded into a Galois $\overline{U}_5$-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 $F_u^\times \to F^\times$, where $F_u \coloneqq F[x_u]/(x_u^2 - u)$. Suppose that $(a,b) = (b,c) = (c,d) = 0$ in $\mathrm{Br}(F)$. (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 $\overline{U}_5$-algebras over F, in Proposition 3.7 we associate to a,b,c,d a scalar $e \in F^\times$, uniquely determined in $F^\times/N_aN_{ac}N_dN_{bd}$, such that $\langle a,b,c,d\rangle$ is defined if and only if $e \in N_aN_{ac}N_dN_{bd}$. The scalar e is defined in terms of a pair $(\epsilon,\nu) \in F_{a,c}^\times \times F_{b,d}^\times$ satisfying certain properties: roughly speaking, ϵ and ν 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 $\overline{U}_5$-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 α and δ exist because $(a,b) = (c,d) = 0$.) It was shown in [GMT18, 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 $\mathrm{Br}(F_{a,d})$; 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 [GMT18, 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 $(b,c)=0$, replacing 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:

$$\begin{array}{ccccc} r \in N_aN_{ab}N_{ac} & \overset{4.2}{\Longleftrightarrow} & s \in N_bN_{ab}N_{bc} & \overset{4.2}{\Longleftrightarrow} & t \in N_cN_{ac}N_{bc} \\ \Big\Updownarrow {\scriptstyle 4.1(a)} & & & & \Big\Updownarrow {\scriptstyle 4.1(b)} \\ \langle a,b,c,a\rangle \text{ defined} & & & & \langle a,b,c,a\rangle \text{ vanishes.} \end{array}$$

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

For the vertical equivalence on the right, we show that $t \in N_cN_{ac}N_{bc}$ is equivalent to the condition of [GMT18, Theorem A]. The key point is that, under the assumption $a=d$, the condition of [GMT18, Theorem A] may be replaced by the system of two equations $(\alpha x, \delta y) = 0$ and $(\alpha x, c) = 0$ in $\mathrm{Br}(F_a)$; see Corollary 3.13. The first equation has a solution $(x,y) \in F^\times \times F^\times$ if and only if $x \in N_cN_{bc}$: 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 $x \in tN_cN_{ac}$. All in all, the condition of [GMT18, Theorem A] is satisfied if and only if $tN_cN_{ac} \cap N_cN_{bc} \neq \emptyset$, that is, $t \in N_cN_{ac}N_{bc}$. 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 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 [GMT18, 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 Proposition 4.1 and Proposition 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_{sep} be a separable closure of F, and $\Gamma_F \coloneqq \mathrm{Gal}(F_{\mathrm{sep}}/F)$ be the absolute Galois group of F. We often use additive notation while working with elements of Γ_F: for all $\sigma, \tau \in \Gamma_F$ and $x \in F$, we have $(\sigma + \tau)(x) = \sigma(x)\tau(x)$ and $(\sigma\tau)(x) = \sigma(\tau(x))$.

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

Suppose that $\mathrm{char}(F) \neq 2$. If E is an F-algebra and $a_1, \ldots, a_n \in E^\times$, we define the étale E-algebra $E_{a_1,\ldots,a_n}$ by

$$E_{a_1,\ldots,a_n} \coloneqq E[x_1, \ldots, x_n]/(x_1^2 - a_1, \ldots, x_n^2 - a_n)$$

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

We write $\mathrm{Br}(F)$ for the Brauer group of F. The group operation on $\mathrm{Br}(F)$ is denoted additively. If $\mathrm{char}(F) \neq 0$ and $a, b \in F^\times$, we write (a, b) for the corresponding quaternion algebra over F and for its class in $\mathrm{Br}(F)$. We write $N_{a_1,\ldots,a_n} \colon \mathrm{Br}(F_{a_1,\ldots,a_n}) \to \mathrm{Br}(F)$ for the corestriction map along $F_{a_1,\ldots,a_n}/F$.

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 [KMRT98, Definitions (18.15)]. A G-algebra L/F is Galois if and only if the morphism of schemes $\mathrm{Spec}(L) \to \mathrm{Spec}(F)$ is an étale G-torsor. By [KMRT98, Example (28.15)], we have a canonical bijection

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

which is functorial in F and G.

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

$$\mathrm{Hom}(\Gamma_F, \mathbb{Z}/2\mathbb{Z}) = H^1(F, \mathbb{Z}/2\mathbb{Z}) \simeq H^1(F, \mu_2) \simeq F^\times/F^{\times 2}. \tag{2.2}$$

For every $a \in F^\times$, we let $\chi_a\colon \Gamma_F \to \mathbb{Z}/2\mathbb{Z}$ be the homomorphism corresponding to the coset $aF^{\times 2}$ under (2.2). Explicitly, letting $a' \in F_{\mathrm{sep}}^\times$ be such that $(a')^2 = a$, we have $g(a') = (-1)^{\chi_a(g)} a'$ for all $g \in \Gamma_F$. (This definition does not depend on the choice of a'.)

Now let $n \geq 1$ be an integer and set $G = (\mathbb{Z}/2\mathbb{Z})^n$. For all $i = 1, \dots, n$, let σ_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 (2.2) 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

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

For all $a, b \in F^\times$, $\iota(\chi_a \cup \chi_b)$ is equal to (a, b); see [Ser79, Chapter XIV, Proposition 5]. The next lemma is well known and will be used several times in what follows.

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

(i) $(a, b) = 0$ *in* $\mathrm{Br}(F)$*;*

(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 $\mathbb{P}^1_F$).

Proof. See [GS17, Propositions 1.1.7 and 1.3.2]. □

2.2. **Massey products.** Let A be a commutative ring with identity, and $(C^\cdot, \partial)$ be a DGA over A, that is, a graded-commutative A-algebra $C^\cdot = \oplus_{i\geq 0} C^i$ with a homomorphism $\partial\colon C^\cdot \to C^{\cdot+1}$ (called the differential) such that $\partial(ab) = \partial(a)b + (-1)^i \partial(b)$ for all $a \in C^i$ and all $b \in C^\cdot$ and $\partial \circ \partial = 0$. We denote by $H^\cdot(C^\cdot) \coloneqq \mathrm{Ker}\,\partial / \mathrm{Im}\,\partial$ the cohomology of $(C^\cdot, \partial)$.

Let $n \geq 2$ be an integer and $a_1, \dots, a_n \in H^1(C^\cdot)$. Consider a collection $M = (a_{ij})$ of elements of C^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 $H^1(C^\cdot)$.

(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 $\langle a_1, \dots, a_n \rangle_M \in H^2(C^\cdot)$ for its cohomology class. By definition, the *Massey product* of $a_1, \dots, a_n$ is the subset $\langle a_1, \dots, a_n \rangle \subset H^2(C^\cdot)$ 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. Let $a_1, \dots, a_n \in H^1(C^\cdot)$ 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 $H^2(C^\cdot)$. 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 $H^2(C^\cdot)$.

Example 2.3. (a) Let Γ be a profinite group. The complex $(C^\cdot(\Gamma, \mathbb{Z}/2\mathbb{Z}), \partial)$ of mod 2 non-homogeneous continuous cochains of Γ with the standard cup product is a DGA. We write $H^{\cdot}(\Gamma, \mathbb{Z}/2\mathbb{Z})$ for the cohomology of $(C^{\cdot}(\Gamma, \mathbb{Z}/2\mathbb{Z}), \partial)$. 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 $\mathrm{char}(F) \neq 2$. 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 $U_{n+1} \subset \mathrm{GL}_{n+1}(\mathbb{F}_2)$ be the subgroup of all upper-triangular unipotent matrices. For all $1 \leq i < j \leq n+1$, we denote by $u_{i,j} \colon U_{n+1} \to \mathbb{Z}/2\mathbb{Z}$ the (i,j)-th coordinate 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

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & Z_{n+1} & \longrightarrow & U_{n+1} & \longrightarrow & \overline{U}_{n+1} & \longrightarrow & 1 \\
 & & & & & \searrow & \downarrow & & \\
 & & & & & & (\mathbb{Z}/2\mathbb{Z})^n & &
\end{array}
\tag{2.3}
$$

where the row is short exact and the homomorphism $U_{n+1} \to (\mathbb{Z}/2\mathbb{Z})^n$ is given by $(u_{1,2}, u_{2,3}, \dots, u_{n,n+1})$. The group $\overline{U}_{n+1}$ 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. We also let

$$Q_{n+1} \coloneqq \mathrm{Ker}(U_{n+1} \to (\mathbb{Z}/2\mathbb{Z})^n), \quad \overline{Q}_{n+1} \coloneqq \mathrm{Ker}(\overline{U}_{n+1} \to (\mathbb{Z}/2\mathbb{Z})^n) = Q_{n+1}/Z_{n+1}.$$

The induced maps

$$H^1(F, U_{n+1}) \to H^1(F, (\mathbb{Z}/2\mathbb{Z})^n), \qquad H^1(F, \overline{U}_{n+1}) \to H^1(F, (\mathbb{Z}/2\mathbb{Z})^n)$$

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

The following result is due to Dwyer [Dwy75]. (We do not need to assume that $\mathrm{char}(F) \neq 2$.)

Theorem 2.4. *Let $\chi = (\chi_1, \dots, \chi_n) \colon \Gamma_F \to (\mathbb{Z}/2\mathbb{Z})^n$ be a group homomorphism. The Massey product $\langle \chi_1, \dots, \chi_n\rangle$ is defined (resp. vanishes) if and only if χ lifts to a homomorphism $\Gamma_F \to \overline{U}_{n+1}$ (resp. $\Gamma_F \to U_{n+1}$).*

Proof. See [Dwy75] or [HW19, Proposition 2.2]. □

Corollary 2.5. *Suppose that the maximal pro-2 quotient of Γ_F is a free pro-2 group. Then, for all $n \geq 1$ and all homomorphisms $\chi_1, \dots, \chi_n \colon \Gamma_F \to \mathbb{Z}/2\mathbb{Z}$, the Massey product $\langle \chi_1, \dots, \chi_n\rangle$ vanishes.*

The assumptions of Corollary 2.5 are satisfied, for example, when F is a finite field.

Proof. Let $\Gamma_F(2)$ be the maximal pro-2 quotient of Γ_F. For all finite 2-groups G, every homomorphism $\Gamma_F \to G$ factors through $\Gamma_F(2)$. By assumption $\Gamma_F(2)$ is free, hence every homomorphism $\Gamma_F(2) \to (\mathbb{Z}/2\mathbb{Z})^n$ lifts to U_{n+1}. The conclusion now follows from Theorem 2.4. □

Corollary 2.6. *Suppose that* $\mathrm{char}(F) \neq 2$, *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* $\overline{U}_{n+1}$*-algebra* K/F *(resp. Galois* U_{n+1}*-algebra* L/K*) such that* $K^{\overline{Q}_{n+1}} = F_{a_1,\dots,a_n}$ *(resp.* $L^{Q_{n+1}} = F_{a_1,\dots,a_n}$*).*

Proof. Immediate consequence of Theorem 2.4, Example 2.3(b) and (2.1). □

We conclude Section 2.2 with some observations. We have a cartesian square of groups

$$\begin{array}{ccc} \overline{U}_{n+1} & \xrightarrow{\varphi_{n+1}} & U_n \\ \downarrow{\scriptstyle \varphi'_{n+1}} & & \downarrow{\scriptstyle \varphi'_n} \\ U_n & \xrightarrow{\varphi_n} & U_{n-1} \end{array} \tag{2.4}$$

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

Proposition 2.7. *The map*

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

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

Proof. Since (2.4) is cartesian, to give a continuous group homomorphism $\Gamma_F \to \overline{U}_{n+1}$ is the same as giving two homomorphisms $f, f' \colon \Gamma_F \to U_n$ such that $\varphi_n \circ f = \varphi'_n \circ f'$. It follows that the square of pointed sets

$$\begin{array}{ccc} \mathrm{Hom}(\Gamma_F, \overline{U}_{n+1}) & \xrightarrow{(\varphi_{n+1})_*} & \mathrm{Hom}(\Gamma_F, U_n) \\ \downarrow{\scriptstyle (\varphi'_{n+1})_*} & & \downarrow{\scriptstyle (\varphi'_n)_*} \\ \mathrm{Hom}(\Gamma_F, U_n) & \xrightarrow{(\varphi_n)_*} & \mathrm{Hom}(\Gamma_F, U_{n-1}) \end{array} \tag{2.5}$$

is also cartesian.

Recall that, for every finite group G, $H^1(F, G) = \mathrm{Hom}(\Gamma_F, G)/\sim$, where if $\psi, \psi' \colon \Gamma_F \to G$ are 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 $\psi, \psi' \colon \Gamma_F \to U_n$ and $g \in U_{n-1}$ such that

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

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 (2.5) is cartesian, there exists $\Psi \in \mathrm{Hom}(\Gamma_F, \overline{U}_{n+1})$ lifting ψ and $\tilde{g}\psi'\tilde{g}^{-1}$. This completes the proof. □

Lemma 2.8. *Suppose that* $\mathrm{char}(F) \neq 2$. *Let* $n \geq 2$ *be an integer and* K *be a Galois* $\overline{U}_{n+1}$*-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 (2.3) yields an exact sequence of pointed sets

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

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

2.3. **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* $\mathrm{char}(k) \neq 2$. *Let $a_1,\dots,a_n \in R^\times$, and let $\overline{a}_1,\dots,\overline{a}_n \in k^\times$ be their reductions.*

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

(b) If the Massey product $\langle a_1,\dots,a_n\rangle$ vanishes over K, then $\langle \overline{a}_1,\dots,\overline{a}_n\rangle$ 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, $q = \mathrm{char}(K)$ if $\mathrm{char}(K) > 0$ and $q = 1$ if $\mathrm{char}(K) = 0$. Let $\pi \in R$ be a uniformizer. For every $d \geq 1$ prime to q, choose a d-th root $\pi^{1/d}$ of π such that for all $d_1, d_2 \geq 1$ prime to q we have $(\pi^{1/d_1 d_2})^{d_1} = \pi^{1/d_2}$. Define $K_\infty := \cup_d K(\pi^{1/d})$, where $d \geq 1$ ranges over all integers prime to q. Let $\Delta := \Gamma_{K_\infty}$, and define $L := K_{\mathrm{nr}}K_\infty$. Then Γ_L is a pro-q-group (trivial if $q=1$) and $\mathrm{Gal}(L/K_\infty) = \mathrm{Gal}(K_{\mathrm{nr}}/K) = \Gamma_k$. It follows that for every finite 2-group G the natural map

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

is an isomorphism. We obtain a map

$$\mathrm{Hom}(\Gamma_K, G) \to \mathrm{Hom}(\Delta, G) = \mathrm{Hom}(\Gamma_k, G),$$

which induces a map

$$s\colon H^1(K,G) \to H^1(k,G)$$

which is covariant in G. This map is sometimes called the specialization map in Galois cohomology.

For all $a \in R^\times$, we denote by $\overline{a} \in k^\times$ the reduction of a modulo the maximal ideal of R. Under the identification of (2.2), $s\colon H^1(K,\mathbb{Z}/2\mathbb{Z}) \to H^1(k,\mathbb{Z}/2\mathbb{Z})$ sends $aK^{\times 2}$ to $\overline{a}k^{\times 2}$. Therefore for all $n \geq 1$:

(2.6)
The map $s\colon H^1(K,(\mathbb{Z}/2\mathbb{Z})^n) \to H^1(k,(\mathbb{Z}/2\mathbb{Z})^n)$ sends $(a_1,\dots,a_n)$ to $(\overline{a}_1,\dots,\overline{a}_n)$.

(a) We have a commutative square of pointed sets

$$\begin{array}{ccc} H^1(K,\overline{U}_{n+1}) & \xrightarrow{s} & H^1(k,\overline{U}_{n+1}) \\ \downarrow & & \downarrow \\ H^1(K,(\mathbb{Z}/2\mathbb{Z})^n) & \xrightarrow{s} & H^1(k,(\mathbb{Z}/2\mathbb{Z})^n). \end{array} \tag{2.7}$$

By Corollary 2.6, $(a_1,\dots,a_n)$ lifts to $H^1(K,\overline{U}_{n+1})$, hence (2.6) and (2.7) imply that $(\overline{a}_1,\dots,\overline{a}_n) \in H^1(k,(\mathbb{Z}/2\mathbb{Z})^n)$ lifts to $H^1(k,\overline{U}_{n+1})$. The conclusion follows from Theorem 2.4.

(b) We may argue as in the proof of (a), replacing $\overline{U}_{n+1}$ 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 $\mathrm{char}(F) \neq p$ 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 Section 2.2 and Section 2.3 extend to arbitrary p, with the same proofs.

3. Massey products and Galois algebras

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

3.1. **Galois U_3-algebras.** Let $a, b \in F^\times$, and suppose that $(a, b) = 0$ in $\mathrm{Br}(F)$. 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

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

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

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

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

$$\sigma_a(\sqrt{\alpha}) = -x\sqrt{b}/\sqrt{\alpha}, \qquad \sigma_b(\sqrt{\alpha}) = \sqrt{\alpha}. \tag{3.2}$$

Then $\sigma_b \colon K^+ \to K^-$ is an isomorphism of Galois U_3-algebras.

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

Proof. For all $\eta \in (F_{a,b})_\alpha$, we write η^+ and η^- for the element η, viewed as an element of K^+ and K^-, respectively. Then $\sigma_b \colon K^+ \to K^-$ sends η^+ to $\sigma_b(\eta^+) = \sigma_b(\eta)^-$. Since σ_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

$$\sigma_b(\sigma_a(\sqrt{\alpha}^+)) = \sigma_b(x\sqrt{b}^+/\sqrt{\alpha}^+) = -x\sqrt{b}^-/\sqrt{\alpha}^- = \sigma_a(\sqrt{\alpha}^-) = \sigma_a(\sigma_b(\sqrt{\alpha}^+)). \quad \square$$

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

$$\sigma_a(\sqrt{\beta}) = \sqrt{\beta}, \qquad \sigma_b(\sqrt{\beta}) = y\sqrt{b}/\sqrt{\beta}. \tag{3.3}$$

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

(a) Every Galois U_3-algebra over $F_{a,b}$ 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 over $F_{a,b}$ 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 (3.3).

(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 (3.3), respectively) are isomorphic if and only there exists $\omega \in F_{a,b}^\times$ such that

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

Proof. (a) Consider the two subgroups of U_3 given by

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

We have $U_3 = N \rtimes S$. Let π be the cocycle of a in $H^1(F, S) = F^\times/F^{\times 2}$. The twist of N by π is the induced module

$$N_\pi = \mathrm{Ind}_{F_a}^F(\mathbb{Z}/2\mathbb{Z}),$$

hence by Faddeev-Shapiro's lemma,

$$H^1(F, N_\pi) = H^1(F_a, \mathbb{Z}/2\mathbb{Z}) = F_a^\times/F_a^{\times 2}.$$

The twist $N_\pi \to \mathbb{Z}/2\mathbb{Z}$ of the projection $u_{23} \colon N \to \mathbb{Z}/2\mathbb{Z}$ yields the norm map

$$F_a^\times/F_a^{\times 2} = H^1(F, N_\pi) \to H^1(F, \mathbb{Z}/2\mathbb{Z}) = F^\times/F^{\times 2}.$$

We write $\varphi \colon H^1(F, U_3) \to H^1(F, S)$ for the map induced by the projection $U_3 \to S$. Then the natural surjection

$$F_a^\times/F_a^{\times 2} = H^1(F, N_\pi) \to \varphi^{-1}([\pi])$$

takes the class of an element $\alpha \in F_a^\times$ with $N_a(\alpha) = b$ in $F^\times/F^{\times 2}$ to the class of U_3-algebra $(F_{a,b})_\alpha$.

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

$$\begin{bmatrix} 1 & * & * \\ & 1 & 0 \\ & & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 \\ & 1 & * \\ & & 1 \end{bmatrix},$$

respectively.

(c) Suppose there is 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 β under the isomorphism and set $\omega \coloneqq \sqrt{\alpha}\cdot\sqrt{\beta}$. Clearly, $[\sigma_a, \sigma_b]\omega = \omega$, that is, ω is invariant under the center of U_3, hence $\omega \in F_{a,b}^\times$. Moreover,

$$(\sigma_a - 1)(\sigma_b - 1)\omega = (\sigma_a - 1)(\sqrt{a}/\sqrt{\beta'}) = -1.$$

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

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

Replacing x by $-x$ if necessary (by Lemma 3.1, this does not change the 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 $\mathrm{Br}(F)$. 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 $\epsilon \in F_{a,c}^\times$ satisfy $N_{a,c}(\epsilon) = bx^2$ for some $x \in F^\times$. Set $\alpha = N_c(\epsilon) \in F_a^\times$ and $\gamma = N_a(\epsilon) \in F_c^\times$.

We have

$$\begin{aligned} U_4 = \langle\sigma_a, \sigma_b, \sigma_c\colon \quad & \sigma_a^2 = \sigma_b^2 = \sigma_c^2 = 1, \\ & [\sigma_a, \sigma_b]^2 = [\sigma_b, \sigma_c]^2 = [\sigma_a, \sigma_c] = 1, \\ & [[\sigma_a, \sigma_b], \sigma_c] = [\sigma_a, [\sigma_b, \sigma_c]], \\ & [[\sigma_a, \sigma_b], \sigma_c]^2 = 1\rangle. \end{aligned}$$

The quotient map $U_4 \to (\mathbb{Z}/2\mathbb{Z})^3$ is given by $\sigma_a \mapsto \sigma_a$, $\sigma_b \mapsto \sigma_b$ and $\sigma_c \mapsto \sigma_c$. The étale F-algebra $(F_{a,b,c})_{\alpha,\gamma,\epsilon}$ 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

$$\sigma_a(\sqrt{\epsilon}) = \sqrt{\gamma}/\sqrt{\epsilon}, \qquad \sigma_c(\sqrt{\epsilon}) = \sqrt{\alpha}/\sqrt{\epsilon},$$
$$\sigma_a(\sqrt{\alpha}) = x\sqrt{b}/\sqrt{\alpha}, \qquad \sigma_c(\sqrt{\gamma}) = x\sqrt{b}/\sqrt{\gamma},$$
$$(\sigma_b - 1)\alpha = (\sigma_b - 1)\gamma = (\sigma_b - 1)\epsilon = 1.$$

We leave it to the reader to verify that this defines a Galois U_4-algebra structure on $(F_{a,b,c})_{\alpha,\gamma,\epsilon}$, that is, that $\sigma_a, \sigma_b, \sigma_c$ act via F-algebra automorphisms, that the above relations of among them are satisfied, 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 $(F_{a,b,c})_{N_c(\epsilon),N_a(\epsilon),\epsilon}$ for some $\epsilon \in F_{a,c}^\times$ with the property $N_{a,c}(\alpha) = b$ in $F^\times/F^{\times 2}$.*

Proof. We have $U_4 = N \rtimes S$, where $N \subset U_4$ is the subgroup defined by $u_{12} = u_{34} = 0$ and S is the subgroup defined by $u_{13} = u_{14} = u_{23} = u_{24} = 0$. The coordinate functions u_{12} and u_{34} determine a group isomorphism $S \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

Let π be a cocycle representing $([a], [c])$ in $H^1(F, S) = (F^\times/F^{\times 2})^2$. Write N_π for the twist of N by the S-action via π. We have

$$N_\pi = \mathrm{Ind}_{F_{a,c}}^F(\mathbb{Z}/2\mathbb{Z}),$$

hence by Faddeev-Shapiro's lemma

$$H^1(F, N_\pi) = F_{a,c}^\times/F_{a,c}^{\times 2}.$$

Identifying U_3 with the top-left 3×3 corner of U_4 we set $N' = N \cap U_3$ and $S' = S \cap U_3$. Then $U_3 = N' \rtimes S'$ as in the proof of Proposition 3.2(a). The twist $N_\pi \to N'_\pi$ of the natural projection $N \to N'$ yields the norm map

$$F_{a,c}^\times/F_{a,c}^{\times 2} = H^1(F, N_\pi) \to H^1(F, N') = F_a^\times/F_a^{\times 2}.$$

Similarly, the bottom-right 3×3 corner yields the norm map

$$F_{a,c}^\times/F_{a,c}^{\times 2} \to H^1(F, N') = F_c^\times/F_c^{\times 2}.$$

We write $\varphi\colon H^1(F, U_4) \to H^1(F, S)$ for the map induced by the projection $U_4 \to U_4/N \simeq S$. Then the natural surjection

$$H^1(F, N_\pi) \to \varphi^{-1}([\pi]).$$

takes the class of an element $\epsilon \in F_{a,c}^\times$ with $N_{a,c}(\alpha) = b$ in $F^\times/F^{\times 2}$ to the class of the Galois U_4-algebra $(F_{a,b,c})_{\alpha,\gamma,\epsilon}$. □

The following theorem was proved by Hopkins–Wickelgren [HW15] when F is a number field, and Mináč–Tân [MT15b] when F is arbitrary. We offer a short 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 $\mathrm{Br}(F)$. 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 $\epsilon \in F_{a,c}^\times$ such that $N_{a,c}(\epsilon) = b$ in $F^\times/F^{\times 2}$. By the discussion preceding Proposition 3.3, $K := (F_{a,b,c})_{N_c(\epsilon),N_a(\epsilon),\epsilon}$ is a Galois U_4-algebra such that $K^{Q_4} = F_{a,b,c}$. The conclusion follows from Corollary 2.6. □

3.3. **Galois $\overline{U}_5$-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 $\epsilon \in F_{a,c}^\times$, $\nu \in F_{b,d}^\times$ and $\omega \in F_{b,c}^\times$ such that*

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

Proof. Denote by U_4^+ and U_4^- the top-left and bottom-right 4×4 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 kernel of the maps $U_4^+ \to (\mathbb{Z}/2\mathbb{Z})^3$ and $U_4^- \to (\mathbb{Z}/2\mathbb{Z})^3$, respectively, and P_4^+ and P_4^- be the kernel of the maps $U_4^+ \to U_3$ and $U_4^- \to U_3$, respectively. By Proposition 2.7, to give a Galois $\overline{U}_5$-algebra over $F_{a,b,c,d}$ is the same as giving 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, to give K_1 and K_2 satisfying (i) is equivalent to giving two elements $\epsilon \in F_{a,c}^\times$ and $\nu \in F_{b,d}^\times$ such that $N_{a,c}(\epsilon) = b$ and $N_{b,d}(\nu) = c$ in $F^\times/F^{\times 2}$. By 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 $N_a(\epsilon)N_d(\nu) = \omega^2$ and $(\sigma_b - 1)(\sigma_c - 1)\omega = -1$. □

Remark 3.6. Let $\epsilon \in F_{a,c}^\times$, $\nu \in F_{b,d}^\times$, $e \in F^\times$ and $\omega \in F_{b,c}^\times$ such that $N_a(\epsilon)N_d(\nu) = e\omega^2$. Then $(\sigma_b - 1)N_a(\epsilon) = 1$ and $(\sigma_c - 1)N_d(\nu) = 1$, 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 $\epsilon \in F^\times_{a,c}$, $\nu \in F^\times_{b,d}$ such that $N_{a,c}(\epsilon) = b$ in $F^\times/F^{\times 2}$ and $N_{b,d}(\nu) = c$ in $F^\times/F^{\times 2}$. Even if $\langle a,b,c,d\rangle$ is defined, it is not true that one may find $\omega \in F^\times_{b,c}$ such that (ϵ,ν,ω) satisfies the equations of Proposition 3.5: one might need to change ϵ and ν. It will be useful to have a criterion for $\langle a,b,c,d\rangle$ to be defined in terms of any given ϵ and ν. 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 $\nu \in F^\times_{b,d}$ be such that $N_{a,c}(\epsilon) = b$ in $F^\times/F^{\times 2}$ and $N_{b,d}(\nu) = c$ in $F^\times/F^{\times 2}$.*

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

$$N_a(\epsilon)N_d(\nu) = e\omega^2, \qquad (\sigma_b - 1)(\sigma_c - 1)\omega = -1.$$

(b) Letting ϵ and ν vary, the corresponding e form a $N_aN_{ac}N_dN_{bd}$-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 $(F_{b,c})_{N_a(\epsilon)} \simeq (F_{b,c})_{eN_d(\nu)}$. Thus Proposition 3.2(c) implies the existence of $\omega \in F^\times_{b,c}$ such that

$$N_a(\epsilon)N_d(\nu) = e\omega^2, \qquad (\sigma_b - 1)(\sigma_c - 1)\omega = -1.$$

(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 $\epsilon \in F^\times_{a,c}$, $\nu \in F^\times_{b,d}$, $x,y,e \in F^\times$ and $\omega \in F^\times_{b,c}$ such that $N_{a,c}(\epsilon) = x^2$, $N_{b,d}(\nu) = y^2$, $N_a(\epsilon)N_d(\nu) = e\omega^2$, 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 $\epsilon_a \in F^\times_a$, $\epsilon_c \in F^\times_c$ and $\epsilon_{ac} \in F^\times_{ac}$ such that $\epsilon = \epsilon_a\epsilon_c\epsilon_{ac}$, as well as $\nu_b \in F^\times_b$, $\nu_d \in F^\times_d$ and $\nu_{bd} \in F^\times_{bd}$ such that $\nu = \nu_b\nu_d\nu_{bd}$.

We have

$$N_a(\epsilon) = N_a(\epsilon_a)N_{ac}(\epsilon_{ac})\epsilon_c^2, \qquad N_d(\nu) = N_d(\nu_d)N_{bd}(\nu_{bd})\nu_b^2.$$

Define $\omega_1 := \omega/(\epsilon_c\nu_b) \in F^\times_{b,c}$. Then $N_a(\epsilon)N_d(\nu) = e\omega^2$ may be rewritten as

$$N_a(\epsilon_a)N_{ac}(\epsilon_{ac})N_d(\nu_d)N_{bd}(\nu_{bd}) = e\omega_1^2. \tag{3.4}$$

In particular, ω_1^2 belongs to $F^\times$, hence ω_1 belongs to at least one of $F^\times_b$, $F^\times_c$ and $F^\times_{bc}$. 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 $b = (-d)\cdot(-bd)\cdot d^{-2} \in N_dN_{bd}$ and $c = (-a)\cdot(-ac)\cdot c^{-2} \in N_aN_{ac}$, we deduce that $\omega_1^2 \in N_aN_{ac}N_dN_{bd}$. Now (3.4) implies that $e \in N_aN_{ac}N_dN_{bd}$, as desired.

For the converse, suppose that $e = N_a(\epsilon_a)N_{ac}(\epsilon_{ac})N_d(\nu_d)N_{bd}(\nu_{bd})$, where $\epsilon_a \in F^\times_a$, $\epsilon_{ac} \in F^\times_{ac}$, $\nu_d \in F^\times_d$ and $\nu_{bd} \in F^\times_{bd}$. Set $\epsilon = \epsilon_a\epsilon_{ac}$, $\nu = \nu_d\nu_{bd}$ and $\omega = 1$. Then $N_{a,c}(\epsilon) \in F^{\times 2}$, $N_{b,d}(\nu) \in F^{\times 2}$, $N_a(\epsilon)N_d(\nu) = e\omega^2$ 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

$$V(K) \neq \emptyset \iff \langle a_1,\dots,a_n\rangle \text{ vanishes over } K. \tag{3.5}$$

In the literature, a variety V satisfying (3.5) 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 [HW15] constructed a splitting variety for $n = 3$: it is a torsor under a torus. When $n = 4$, a splitting variety was obtained in [GMT18]. Pál and Schlank [PS22] constructed splitting varieties for all n: their examples are homogeneous spaces under SL_n with finite supersolvable stabilizers. These varieties were exploited by [HW19] 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

$$S \coloneqq R_{a,c}(\mathbb{G}_\mathrm{m}) \times R_{b,d}(\mathbb{G}_\mathrm{m}) \times \mathbb{G}_\mathrm{m}^2 \times R_{b,c}(\mathbb{G}_\mathrm{m}),$$

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

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

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

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

We now show that X satisfies a variant of (3.5), where "vanishes" is replaced by "is defined."

Proposition 3.8. *For all field extensions K/F, we have $X(K) \neq \emptyset$ 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 $(\epsilon, \nu, x, y, \omega) \in X(F)$, then $N_{a,c}(\epsilon) = bx^2$, $N_{b,d}(\nu) = cy^2$ and $(\sigma_b - 1)(\sigma_c - 1)\omega = (\sigma_b - 1)(x\sqrt{b}/N_a(\epsilon)) = -1$, 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 $\epsilon \in F_{a,c}^\times$, $\nu \in F_{b,d}^\times$ and $\omega \in F_{b,c}^\times$ such that

$$N_a(\epsilon)N_d(\nu) = \omega^2, \qquad (\sigma_b - 1)(\sigma_c - 1)\omega = -1.$$

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

$$x \coloneqq \frac{(\sigma_b - 1)\omega \cdot N_d(\nu)}{\sqrt{c}}, \qquad y \coloneqq \frac{(\sigma_c - 1)\omega \cdot N_a(\epsilon)}{\sqrt{b}}.$$

Then

$$(\sigma_c - 1)x = (\sigma_c - 1)(\sigma_b - 1)\omega \cdot (\sigma_c - 1)(N_d(\nu)) \cdot (1 - \sigma_c)\sqrt{c} = (-1) \cdot 1 \cdot (-1) = 1.$$

Moreover, since $N_a(\epsilon) \in F_c^\times$, we have $(\sigma_b - 1)(N_d(\nu)) = (\sigma_b - 1)(\omega^2)$, therefore

$$(\sigma_b - 1)x = (\sigma_b - 1)^2(\omega) \cdot (\sigma_b - 1)(N_d(\nu)) = (2 - 2\sigma_b)(\omega) \cdot (\sigma_b - 1)(\omega^2) = 1.$$

It follows that $x \in F^\times$. Similar calculations show that $y \in F^\times$, hence $(\epsilon, \nu, x, y, \omega) \in X'(F)$. This completes the proof. $\square$

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), 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 [GMT18, 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 [GMT18, Theorem A] are closely related. In particular the short exact sequence (3.6) below has been used in the proof of [GMT18, Theorem A]; see [GMT18, §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 $\mathrm{Br}(F_{a,d})$.

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

$$1 \to P \to U_5 \to U_3 \times U_3 \to 1, \tag{3.6}$$

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

$$N \times N' \to P$$

taking a pair of matrices

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

to

$$\begin{bmatrix} 1 & 0 & 0 & f_1e_2 & f_1f_2 \\ & 1 & 0 & e_1e_2 & e_1f_2 \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix}$$

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

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

The natural projections $t : U_3 \to N$ and $t' : U_3 \to N'$ 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 (3.6) 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 $h : \Gamma_F \to U_3$ 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 $N_d(\beta) = c \in F^\times/F^{\times 2}$ and let $h' : \Gamma_F \to U_3$ be a group homomorphism corresponding to $(F_{c,d})_\delta$ via (2.1).

As in the proof of Proposition 3.2, the Γ_F-module N, where Γ_F acts via h, is the induced module $\mathrm{Ind}_{F_a}^F(\mathbb{Z}/2\mathbb{Z})$. 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 α. 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 δ.

Note that

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

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

Consider the commutative diagram

$$\begin{array}{ccc}
H^1(U_3, N) \otimes H^1(U_3, N') & \xrightarrow{\ \cup\ } & H^2(U_3 \times U_3, P) \\
\big\downarrow{\scriptstyle h^* \otimes (h')^*} & & \big\downarrow{\scriptstyle (h, h')^*} \\
H^1(F, N) \otimes H^1(F, N') & \xrightarrow{\ \cup\ } & H^2(F, P) \\
\| & & \| \\
H^1(F_a, \mathbb{Z}/2\mathbb{Z}) \otimes H^1(F_d, \mathbb{Z}/2\mathbb{Z}) & \xrightarrow{\ \cup\ } & H^2(F_{a,d}, \mathbb{Z}/2\mathbb{Z}).
\end{array}$$

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

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

is equal to the cup-product (α, δ). By (3.6), the homomorphism $(h, h') : \Gamma_F \to U_3 \times U_3$ lifts to a homomorphism $\Gamma_F \to U_5$ if and only if the pullback of the exact sequence (3.6) 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 $(\alpha, \delta) \in H^2(F_{a,d}, \mathbb{Z}/2\mathbb{Z}) \subset \mathrm{Br}(F_{a,d})$, this and Theorem 2.4 imply the conclusion. □

The following result is a reformulation of [GMT18, Theorem A].

Corollary 3.12. *Let $a, b, c, d \in F^\times$ be such that $(a, b) = (c, d) = 0$ in $\mathrm{Br}(F)$. 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 $\langle a, b, c, d\rangle$ is trivial if and only if there exist $x, y \in F^\times$ such that $(\alpha x, \delta y) = 0$ in $\mathrm{Br}(F_{a,d})$.*

Proof. Recall that α and δ exist by Lemma 2.1. Suppose $(\alpha x, \delta y) = 0$ in $\mathrm{Br}(F_{a,d})$ 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 $\langle a, b, c, d\rangle$ is defined by Proposition 3.11.

Conversely, if $\langle a,b,c,d\rangle$ is defined, 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 $\mathrm{Br}(F_{a,d})$. There exist $x\in F^\times$ such that $N_a(\alpha)=N_a(\alpha')$. Now Hilbert 90 implies the existence of $\eta_a\in F_a^\times$ such that $\alpha'=\alpha\cdot(\sigma_a-1)\eta_a=\alpha N_a(\eta_a)\eta_a^{-2}$. Similarly, there exists $\eta_d\in F_d^\times$ such that $\delta'=\delta N_d(\eta_d)\eta_d^{-2}$. Set $x\coloneqq N_a(\eta_a)\in F^\times$ and $y\coloneqq N_d(\eta_d)\in F^\times$. Then

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

as desired. □

Corollary 3.13. *Let $a,b,c\in F^\times$ be such that $(a,b)=(c,a)=0$ in $\mathrm{Br}(F)$. 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 $\mathrm{Br}(F_a)$.*

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

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

If $\pi=\pi_1+\pi_2v_a+\pi_3w_a+\pi_4v_aw_a\in F_{a,d}$, then

$$\varphi(\pi)=(\pi_1+a\pi_4+(\pi_2+\pi_3)u_a,\pi_1-a\pi_4+(\pi_2-\pi_3)u_a). \tag{3.7}$$

Let $x,y\in F^\times$. Since α is in the F-span of 1 and v_a, and δ is in the F-span of 1 and w_a, by (3.7) we have $\varphi(\alpha x)=(\alpha x,\alpha x)$ and $\varphi(\delta y)=(\delta y,\sigma_a(\delta)y)$. It follows that the isomorphism

$$\mathrm{Br}(F_{a,a})\xrightarrow{\sim}\mathrm{Br}(F_a)\times\mathrm{Br}(F_a)$$

induced by φ sends $(\alpha x,\delta y)$ to $((\alpha x,\delta y),(\alpha x,\sigma_a(\delta)y))$. Since

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

we deduce that $(\alpha x,\delta y)=0$ in $\mathrm{Br}(F_{a,a})$ if and only if $(\alpha x,\delta y)=(\alpha x,c)=0$ in $\mathrm{Br}(F_a)$. 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 $\mathrm{Br}(F)$.

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

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

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 $r\in N_aN_{ab}N_{ac}$.

(b) The Massey product $\langle a,b,c,a\rangle$ vanishes over F if and only if $t\in N_cN_{ac}N_{bc}$.

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

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

4.1. **Proof of Proposition 4.1(a).** We maintain the notations and assumptions of the beginning of Section 4. By Proposition 3.3, there exist $\epsilon \in F_{a,c}^\times$ and $\nu \in F_{b,d}^\times$ such that $K_1 = (F_{a,b,c})_{N_c(\epsilon),N_a(\epsilon),\epsilon}$ and $K_2 = (F_{b,c,d})_{N_d(\nu),N_b(\nu),\nu}$ 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

$$N_a(\epsilon)N_d(\nu) = e\omega^2, \qquad (\sigma_b - 1)(\sigma_c - 1)\omega = -1.$$

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

$$\epsilon := \alpha + \gamma \in F_{a,c}^\times, \qquad \nu := \beta + \delta \in F_{b,d}^\times.$$

By Lemma A.4(1), we have

$$N_a(\epsilon) = \gamma x, \qquad N_d(\nu) = \beta y,$$

where

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

In particular

$$N_{a,c}(\epsilon) = bx^2, \qquad N_{b,d}(\nu) = cy^2.$$

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

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

Thus $N_a(\epsilon)N_d(\nu) = r\omega^2$. We conclude from Proposition 3.7(b) that $e = r$ in $N_aN_{ac}N_dN_{bd}$. □

Proof of Proposition 4.1(a). Since $a = d$, we have $N_aN_{ac}N_dN_{bd} = N_aN_{ab}N_{ac}$. The conclusion follows from Proposition 4.3 and Proposition 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 $\mathrm{Br}(F)$. Then there exists $z \in F^\times$ such that $(\pi, \mu z) = 0$ in $\mathrm{Br}(F_a)$.*

Proof. We use the theory of Albert forms attached to biquaternion algebras; see [KMRT98, §16 A]. As explained in [KMRT98, Example (16.4)], given a biquaternion F-algebra $A \coloneqq (a_1, b_1) \otimes (a_2, b_2)$, 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 [KMRT98, Proposition (16.3)].

Let K/F be an étale algebra of degree 2, let $s\colon K \to F$ be a nonzero 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 $q : Q^0 \to K$ be the quadratic form given by squaring, and let $s_*(q)$ be the transfer of q; see [Lam05, Chapter VII, §1]. Then it follows from [KMRT98, 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 [KMRT98, Corollary (16.28)]. Thus, by Albert's theorem [KMRT98, Theorem 16.5]:

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

Now let $K = F_a$, let $s\colon F_a \to F$ 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 also 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 $\mathrm{Br}(F_a)$ and we may take $z = 1$. Otherwise $\langle \mu, -\pi\mu\rangle$ over F_a represents an element $z \in F^\times$, then μz is represented by $\langle 1, -\pi\rangle$. By Lemma 2.1, this implies that $(\pi, \mu z) = 0$ in $\mathrm{Br}(F_a)$ and completes the proof. □

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

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

By (4.1), we have

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

Corollary 4.5. *(a) If $N_a(\alpha x, \delta y) = 0$ in $\mathrm{Br}(F_a)$ 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 $\mathrm{Br}(F_a)$.

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

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

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

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

It follows that

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

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 (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 $\mathrm{Br}(F_a)$. Letting $y := n_{bc} z$, we obtain $(\alpha x, \delta y) = 0$ in $\mathrm{Br}(F_a)$, 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:

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

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

Now let $s \colon F_a \to F$ 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 $\mathrm{Br}(F_a)$, 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 $\mathrm{Br}(F_a)$. 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 $\mathrm{Br}(F_a)$ if and only if $x \in t N_c N_{ac}$.*

Proof. We have

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

and

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

Now Lemma A.4(3) implies

$$(\alpha, c) = (t, c) \qquad \text{in } \mathrm{Br}(F_a),$$

hence, adding (x, c) to both sides,

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

Thus $(\alpha x, c) = 0$ in $\mathrm{Br}(F_a)$ if and only if $(tx, c) = 0$ in $\mathrm{Br}(F_a)$. By [Ser79, Chapter XIV, Proposition 2], this is in turn equivalent to the existence of $y \in F^\times$ such that $(tx, c) = (a, y)$ in $\mathrm{Br}(F)$. By Lemma A.1, this is equivalent to $tx \in N_c N_{ac}$, that is, $x \in N_c N_{ac}$. □

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

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

By 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 $\mathrm{Br}(F)$.*

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

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

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

$$(s, b) = (s, v_2^2 + u_2^2) \qquad \text{if } v_2^2 + u_2^2 \neq 0, \tag{4.8}$$

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

$$(r, a) = (r, v_2^2 + u_2^2) \qquad \text{if } v_2^2 + u_2^2 \neq 0, \tag{4.9}$$

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

$$rst = 2v_2u_2\cdot\left(\frac{rl}{v_2u_2}\right)^2. \tag{4.10}$$

Finally,

$$(2v_2u_2, v_2^2+u_2^2)=0 \tag{4.11}$$

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)-(4.11) 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 $\mathrm{Br}(F)$, then*

$$a'\in N_aN_{ab}N_{ac} \iff b'\in N_bN_{ab}N_{bc} \iff c'\in N_cN_{ac}N_{bc}.$$

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

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

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

Proof of Proposition 4.2. Immediate from Lemma 4.8 and Lemma 4.9. □

4.4. **Proof of Theorem 1.3.** As anticipated, Theorem 1.3 will follow from Proposition 4.1 and Proposition 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 $(a,b)=(b,c)=(c,d)=0$ in $\mathrm{Br}(F)$. 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 $(\mathbb{A}^2_F)^2$ with coordinates (v_1,v_2,u_1,u_2), and let $Y\subset(\mathbb{A}^2_F)^2$ be the locally-closed subvariety given by (4.1). Since $(a,b)=(a,c)=0$ in $\mathrm{Br}(F)$ 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 $r\in N_aN_{ab}N_{ac}$. It follows from Proposition 4.2 that $t\in N_cN_{ac}N_{bc}$. 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 $(\mathbb{A}^2_F)^2$ with coordinates (v_1, v_2, u_1, u_2), and let $Z \subset (\mathbb{A}^2_F)^2$ be the smooth variety given by the first two equalities of (4.1). Then the restrictions to Z of the coordinate functions of $(\mathbb{A}^2_F)^2$ 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 Proposition 4.1 and Proposition 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 $b, c \in F^\times$ such that $b + c = 1$. In particular $(b, c) = 0$ in $\mathrm{Br}(F)$. Suppose further that $(bc, b) = (bc, c) = 0$. This is equivalent to $(b, -1) = (c, -1) = 0$, that is, by Lemma 2.1, $-1 \in N_b \cap N_c$.

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

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

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

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

We have

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

We may also write

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

Finally, define

$$f \coloneqq \mathrm{Tr}_{bc}(\alpha) + \mathrm{Tr}_c(lv_2(1+\sqrt{c})) = 2lv_1 + 2lv_2.$$

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

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

Proof. By Lemma A.4(2) applied to $\rho = \alpha$ and $\mu = lv_2(1+\sqrt{c})$, we have that $b(lv_2)^2 f^2 \in N_{b,c}$. Thus, in order to prove that $-f^2 \in N_{b,c}$, 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 $N_b(v/\sqrt{b}) = -c = N_c(\sqrt{c})$, 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 $a = d = bc$ and $b + c = 1$. By Theorem 1.3, we know that (1) is equivalent to (2).

We now prove that (2) is equivalent (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 $(\mathbb{A}^2_F)^2$ with coordinates (v_1, v_2, u_1, u_2), and let $Y \subset (\mathbb{A}^2_F)^2$ 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 $\mathrm{Br}(F_{bc})$. By Corollary 4.5(a) and Lemma 4.7, these equalities are equivalent to $N_c N_{bc} \cap f N_b N_c \neq \emptyset$. The latter is equivalent to $f \in N_b N_c N_{bc}$, which by Lemma A.3(2) is equivalent to $f^2 \in N_{b,c}$. 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 [GMT18, 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 $\mathrm{Gal}(K/F)$ 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 $K \otimes_F F_v \to \prod_{i=1}^m K_{w_i}$ is an isomorphism (see e.g. [CF67, 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 $K \coloneqq \mathbb{Q}(\sqrt{2}, \sqrt{17})$. It is not difficult to prove that the local degree of $K/\mathbb{Q}$ at v is either 1 or 2. For all $c \in \mathbb{Q}^\times$, define

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

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 $\mathrm{Br}(\mathbb{Q}_v)$. 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 [CF67, Exercise 5.2] or [Hür86, Lemma p. 114].

Note that 3 does not belong to S_1 while 17 belongs to S_1. Moreover, 3 is not square modulo 17, hence $\omega(3) = (17, 3)_{17} = -1$. By the aforementioned result of Serre and Tate, 3 is not in $N_2 N_{17} N_{34}$, which by Lemma A.3(2) implies that 9 does not belong to $N_{2,17}$. On the other hand,

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

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

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

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 we 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, and consider the norm map*

$$N_a\colon \operatorname{Div}(X_{F_a})\to \operatorname{Div}(X).$$

Let $\sum m_x x$ be a divisor in the image of N_a. 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 $\sum m_x x$ be in the image of N_a, and let $x\in X$ be a closed point. Note that $\deg(x)\coloneqq [F(x):F]$ is a power of 2, and it is different from 1 since $X(F)=\emptyset$. If $m_x\deg(x)$ is divisible by 4, then either $\deg(x)$ is divisible by 4, or $\deg(x)=2$ and $F(x)\neq F_a$, that is, $F(x)$ and F_a are linearly disjoint. Since $\sum m_x\deg(x)=0$, the sum of $m_x\deg(x)=2m_x$ over all closed points $x\in X$ such that $F(x)\simeq F_a$ is divisible by 4. □

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

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

Let X be the smooth projective conic over E corresponding to (a,b), and set $F\coloneqq E(X)$. Then $(a,b)=(a,c)=(b,c)=0$ in $\operatorname{Br}(F)$ 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 $\operatorname{Br}(F)$ because $b+c=1$ and every quaternion algebra splits over the function field of the corresponding conic.

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

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

Define

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

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

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

Since $(a,b)\neq 0$ in $\operatorname{Br}(E)$, the field E must be infinite. Thus, as $(a,c)=0$ in $\operatorname{Br}(E)$, 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

$$2(u_1+u_2)u_2f=2(v_1+v_2)(u_1+u_2)v_2u_2v_2^{-2}\in N_aN_{ab}N_{ac}.$$

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

$$f=f_0n_an_{ab}n_{ac}$$

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 $\mathrm{div}(f_0) = 0$, we conclude that

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

We write $\mathrm{div}(n_a) = \sum m_x x$, $\mathrm{div}(n_{ab}) = \sum m'_x x$ and $\mathrm{div}(n_{ac}) = \sum m''_x x$. 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 $X_{ab} \to X$ and $X_{ac} \to X$ 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 $C^\cdot(F, \mathbb{Z}/2\mathbb{Z})$ is formal if it is quasi-isomorphic to its cohomology algebra $H^\cdot(F, \mathbb{Z}/2\mathbb{Z})$, viewed as a DGA with zero differential. If $C^\cdot(F, \mathbb{Z}/2\mathbb{Z})$ is formal, then by [Pos17, Proposition 2.1] for all $n \geq 3$ and all $a_1, \dots, a_n \in F^\times$ such that $a_1 \cup a_2 = a_2 \cup a_3 = \cdots = a_{n-1} \cup a_n = 0$, 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 $\mathrm{Br}(F)$ but the Massey product $\langle a, b, c, a\rangle$ is not defined.

(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 $\mathrm{Br}(F)$ but the Massey product $\langle a, b, c, d\rangle$ is not defined.

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 $(a, c) \in \mathrm{Br}(F_1)$, let $F_2 := F_1(C)$ and F_3 be a 2-closure of F_2, that is, the subfield of $(F_2)_{\mathrm{sep}}$ fixed by a 2-Sylow subgroup of Γ_{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

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

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 $\mathrm{Br}(F_2)$ because C is the conic corresponding to (a, c), hence $(a, c) = 0$ in $\mathrm{Br}(F_3)$. Suppose that $(a, b) = 0$ in $\mathrm{Br}(F_3)$. Then there exists a finite extension L/F_2 of odd degree such that $(a, b) = 0$ in $\mathrm{Br}(L)$. Since $[L : F_2]$ is odd, a restriction-corestriction argument shows that the restriction map $\mathrm{Br}(F_2) \to \mathrm{Br}(L)$ is injective, hence $(a, b) = 0$ in $\mathrm{Br}(F_2)$. By [CTS21, Proposition 7.2.4(b)], the kernel of the restriction map $\mathrm{Br}(F_1) \to \mathrm{Br}(F_2)$ is generated by (a, c), hence

either $(a,b)=0$ or $(a,b)=(a,c)$ (that is, $(a,b(1-b))=0$) in $\mathrm{Br}(F_1)$. 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 $\mathrm{Br}(F)$, 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 $\mathrm{Br}(L)$ 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 Theorem 1.3 and Theorem 1.4. They are all consequences of Hilbert 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

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

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

Proof. It follows from Lemma 2.1 that $(a,n_an_{ab})=(b,n_bn_{ab})$ 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 [Lam05, 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 [DMSS07, Theorem 4]. Let $T\subset R_{a,b}(\mathbb{G}_\mathrm{m})$ be the torus image of the multiplication map

$$\mu\colon R_a(\mathbb{G}_\mathrm{m})\times R_b(\mathbb{G}_\mathrm{m})\to R_{a,b}(\mathbb{G}_\mathrm{m}).$$

A character lattice computation shows that the torus T is defined by the equation $(\sigma_a-1)(\sigma_b-1)\omega=1$ inside $R_{a,b}(\mathbb{G}_\mathrm{m})$. 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

$$1\to\mathbb{G}_\mathrm{m}\to R_a(\mathbb{G}_\mathrm{m})\times R_b(\mathbb{G}_\mathrm{m})\xrightarrow{\mu}T\to 1.$$

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 $u\in N_aN_bN_{ab}$ 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

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

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

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

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

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

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

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

hence

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

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 [CF67, 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 $-1 \in N_aN_bN_{ab}$, hence $u \in N_aN_bN_{ab}$ 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 $d \coloneqq \mathrm{Tr}_a(\rho) + \mathrm{Tr}_b(\mu)$. 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 $\mathrm{Br}(F_b)$.

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 $(\mu d, a) = 0$, 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 $\epsilon \in F_{a,b}^\times$ and $v \in F^\times$ be such that $u = N_{a,b}(\epsilon)v^2$. Then $u = N_a(N_b(\epsilon)v) \in N_a$, and $u = N_b(N_a(\epsilon)v) \in N_b$, 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 ρ by $-\rho$ if necessary, we may suppose that $d \coloneqq \mathrm{Tr}_a(\rho) + \mathrm{Tr}_b(\mu)$ is non-zero. By Lemma A.4(2), we have $ud^2 \in N_{a,b}$, as desired. □

Acknowledgements

We are grateful to Olivier Wittenberg for many helpful comments on an earlier version of this paper.

References

[CF67] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*. Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967. 25, 29

[CTS21] Jean-Louis Colliot-Thélène and Alexei N. Skorobogatov. *The Brauer-Grothendieck group*, volume 71 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer, Cham, 2021. 27

[DMSS07] Roman Dwilewicz, Jan Minac, Andrew Schultz, and John Swallow. Hilbert 90 for biquadratic extensions. *The American Mathematical Monthly*, 114(7):577–587, 2007. 28

[Dwy75] William G. Dwyer. Homology, Massey products and maps between groups. *J. Pure Appl. Algebra*, 6(2):177–190, 1975. 3, 7

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

[GMT18] Pierre Guillot, Ján Mináč, and Adam Topaz. Four-fold Massey products in Galois cohomology. *Compos. Math.*, 154(9):1921–1959, 2018. With an appendix by Olivier Wittenberg. 2, 4, 5, 15, 16, 17, 25

[GS17] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. Second edition of [MR2266528]. 6

[Hür86] W. Hürlimann. H^3 and rational points on biquadratic bicyclic norm forms. *Arch. Math. (Basel)*, 47(2):113–116, 1986. 25

[HW15] Michael J. Hopkins and Kirsten G. Wickelgren. Splitting varieties for triple Massey products. *J. Pure Appl. Algebra*, 219(5):1304–1319, 2015. 1, 3, 13, 15

[HW19] Yonatan Harpaz and Olivier Wittenberg. The Massey vanishing conjecture for number fields. *arXiv:1904.06512*, 2019. 2, 7, 15

[KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The book of involutions*, volume 44 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1998. With a preface in French by J. Tits. 5, 20

[Lam05] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005. 20, 28

[Mat14] Eliyahu Matzri. Triple Massey products in Galois cohomology. *arXiv:1411.4146*, 2014. 2

[MT15a] Ján Mináč and Nguyen Duy Tân. The kernel unipotent conjecture and the vanishing of Massey products for odd rigid fields. *Adv. Math.*, 273:242–270, 2015. 1

[MT15b] Ján Mináč and Nguyen Duy Tân. Triple Massey products over global fields. *Doc. Math.*, 20:1467–1480, 2015. 13

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

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

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

[PS22] Ambrus Pál and Tomer M. Schlank. Brauer-Manin obstruction to the local-global principle for the embedding problem. *Int. J. Number Theory*, 18 (2022), no. 7, 1535–1565. 15

[Pos17] Leonid Positselski. Koszulity of cohomology = $K(\pi, 1)$-ness + quasi-formality. *J. Algebra*, 483:188–229, 2017. 3, 27

[Qua22] Claudio Quadrelli. Massey products in Galois cohomology and the Elementary Type Conjecture. *arXiv:2203.16232*, 2022. 3

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. 6, 22

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

Email address: merkurjev@math.ucla.edu

Email address: scavia@math.ubc.ca