FOUR-FOLD MASSEY PRODUCTS IN GALOIS COHOMOLOGY

PIERRE GUILLOT, JÁN MINÁČ, AND ADAM TOPAZ
WITH AN APPENDIX BY OLIVIER WITTENBERG

Abstract. In this paper, we develop a new necessary and sufficient condition for the vanishing of 4-Massey products of elements in the mod-2 Galois cohomology of a field. This new description allows us to define a splitting variety for 4-Massey products, which is shown in the Appendix to satisfy a local-to-global principle over number fields. As a consequence, we prove that, for a number field, all such 4-Massey products vanish whenever they are defined. This provides new explicit restrictions on the structure of absolute Galois groups of number fields.

Contents

1. Introduction

Let F be a field and $\overline{F}$ a separable closure of F. The absolute Galois group of F, denoted $G_F := \mathrm{Gal}(\overline{F}/F)$ is an object of great interest in algebra and number theory. Many aspects of modern Galois theory, in one way or another, aim to understand the structural properties of G_F. Recent major results in Galois cohomology show that such absolute Galois groups are extremely rare among all profinite groups. The most notable restriction on absolute Galois groups arises from the Bloch-Kato conjecture, which is now a theorem due to Rost-Voevodsky; see [47] [38] [45] [18] [49]. In particular, if F contains a primitive p-th root of unity, then $\mathrm{H}^*(G_F, \mathbb{Z}/p)$ is a *quadratic algebra*. More explicitly, this means that $\mathrm{H}^*(G_F, \mathbb{Z}/p)$ is generated by elements of $\mathrm{H}^1(G_F, \mathbb{Z}/p)$, and the relations are generated only by those relations appearing in degree 2. This is a very strong restriction on the group-theoretical structure of G_F. Recently, other explicit structural restrictions on absolute Galois groups started to arise, based on the notion of *Massey Products* in the context of Galois cohomology.

2010 *Mathematics Subject Classification.* 55S30, 12G05.

Key words and phrases. Massey Products, Galois Cohomology, Splitting Variety, Group Cohomology.

JM is partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) grant R0370A01.

AT was partially supported by EPSRC programme grant EP/M024830/1 Symmetries and Correspondences.

We will recall the definition of Massey products below, but we briefly note that, given $x_1, \ldots, x_n \in \mathrm{H}^1(G_F, \mathbb{Z}/p)$ where p is a prime, the n-Massey product, denoted $\langle x_1, \ldots, x_n \rangle$, is a (possibly empty) subset of $\mathrm{H}^2(G_F, \mathbb{Z}/p)$. In the case $n = 2$, one has a simple description in terms of the cup-product as $\langle x_1, x_2 \rangle = \{x_1 \cup x_2\}$. Just as the cup-product $x_1 \cup x_2$ provides an obstruction to the existence of Heisenberg extensions of F (of degree p^3), the n-Massey product provides as obstruction for the existence of higher $\mathbb{Z}/p$-unipotent extensions. In this respect, we are primarily interested in situations where the n-Massey product $\langle x_1, \ldots, x_n \rangle$ contains 0. In the sequel, when $\langle x_1, \ldots, x_n \rangle$ contains 0, we will simply say that "$\langle x_1, \ldots, x_n \rangle$ vanishes."

In the breakthrough paper on the subject, Hopkins-Wickelgren [20] proved that, given $x_1, x_2, x_3 \in \mathrm{H}^1(G_F, \mathbb{Z}/p)$, the triple Massey product $\langle x_1, x_2, x_3 \rangle$ always vanishes whenever it is nonempty, in the case where F is a number field and $p = 2$. This result was later extended by Mináč-Tân to arbitrary fields and $p = 2$ [29] partially based on ideas appearing in [15], and to arbitrary primes p with F a global field [31].

The end of 2014 and early 2015 saw a surge of activity on triple Massey products of elements of $\mathrm{H}^1(G_F, \mathbb{Z}/p)$, significantly extending the results mentioned above. Matzri [23] was first to announce his proof, extending these results to all primes p and all fields F which contain μ_p. Shortly thereafter, the arguments from *loc. cit.* were refined by Efrat-Matzri, and this work was eventually published in [10]. At around the same time as when [10] was posted, Mináč-Tân [30] also released their proof that triple Massey products of elements of $\mathrm{H}^1(G_F, \mathbb{Z}/p)$ always vanish when defined, while also removing the condition that F must contain μ_p. Motivated by these results, Mináč-Tân [29] [30] [28] eventually formulated the so-called *n-Massey Vanishing Conjecture*, which states that for an arbitrary field F, the n-Massey products of elements of $\mathrm{H}^1(G_F, \mathbb{Z}/p)$ always vanish whenever they are non-empty.

The case of *number fields* has always played a particularly important role in this context, as will be outlined in the historical discussion below. In this respect, the present paper presents the first significant result concerning vanishing of 4-Massey products in Galois cohomology. Namely, this paper proves the following result.

Main Theorem – *Let F be a number field, and let $x_1, x_2, x_3, x_4 \in \mathrm{H}^1(G_F, \mathbb{Z}/2)$ be given. If the Massey product $\langle x_1, x_2, x_3, x_4 \rangle$ is non-empty, then it vanishes.*

To achieve this, we construct a "splitting variety" for the problem at hand, which works over *any field* of characteristic $\neq 2$, and which is compatible with base-change. More precisely, given a field F of characteristic $\neq 2$ and $x_1, x_2, x_3, x_4 \in \mathrm{H}^1(G_F, \mathbb{Z}/2)$, we construct an F-variety $\mathscr{X}_F$ such that the following are equivalent:

(1) The set of F-rational points $\mathscr{X}_F(F)$ is non-empty.
(2) The 4-Massey product $\langle x_1, x_2, x_3, x_4 \rangle$ vanishes.

Furthermore, this construction is compatible with base-change, in the sense that for all L/F, one has $\mathscr{X}_F \otimes_F L = \mathscr{X}_L$.

The study of the geometry and arithmetic of this variety falls within the reach of the recent results in [19]. Hence, when F is a number field, it turns out to be possible to prove that (a variant of) $\mathscr{X}_F$ satisfies a local-to-global principle for the existence of rational points, as soon as the corresponding Brauer-Manin obstruction vanishes. In the proof of Theorem 6.1, we arrange the existence of local points satisfying certain additional conditions which force the corresponding Brauer-Manin obstruction to vanish; this proves the mod-2 case of the 4-Massey vanishing conjecture over number fields. Moreover, it turns out that the Brauer-Manin obstruction *always vanishes* in "generic" situations, which allows us to prove a stronger version of our result in such cases (see Theorem C).

The overall strategy we take in this paper is similar to the approach taken by Wickelgren-Hopkins [20], primarily because of the fact that we use splitting varieties. However, their methods are highly specialized to the case of triple Massey products. Indeed, working with n-Massey products for $n \geq 4$ is substantially harder, especially with respect to their definability and indeterminacy (see the discussion below). Moreover, there is a technical, yet fundamental difference between the two approaches arising from the additional conditions one must arrange for the local points of the splitting variety. The details and new tools we develop here are therefore completely different and more technically involved than those in *loc. cit.*

⋆ ⋆ ⋆

We want to say more about the context, and the history of the subject. Massey products were first introduced in the context of algebraic topology by W. Massey [22], as a collection of "higher-order cohomology operations" defined in terms of the cochain algebra. For example, Massey products of elements of H^1 play a central role in (rational) homotopy theory, as being the most basic obstruction to 1-formality of manifolds – see the work of Deligne, Griffiths, Morgan, and Sullivan [7] [44] [32] [33]. Massey products in Galois cohomology were first systematically considered over *number fields* by Morishita [34] [35], Vogel [48] and Sharifi [41]. These papers were primarily focused on Galois groups of extensions with restricted ramification over number fields, where Massey products have interesting connections with topics from Iwasawa theory, Milnor invariants, and Rédei symbols. Understanding Massey products in the Galois cohomology of number fields is particularly important, as they also show up in the context of Grothendieck's *section conjecture* – see Wickelgren [50] [52] [51]. More generally, Massey products in Galois cohomology play an important role in understanding the structure of nilpotent quotients of absolute Galois groups. Therefore, a detailed understanding of Massey products in Galois cohomology could lead to significant generalizations of results in [12] [25] from the two-step nilpotent setting to more general settings.

The investigation of Massey products in Galois cohomology of arbitrary fields has recently started progressing very rapidly. This surge started with the work of Hopkins-Wickelgren [20], and further progressed by Mináč-Tân [27] [29] [30] [26] and Efrat-Matzri [11] [10] [9] [23]. In fact, ideas related to vanishing of mod-2 triple Massey products already appeared in 2003 by Gao-Leep-Mináč-Smith [15], albeit using different terminology. However, it is important to note that all of the results mentioned above were restricted to studying *triple Massey products.*

Until now, the cases of the n-Massey vanishing conjecture for $n \geq 4$ have remained completely open. Already in the case $n = 4$, having a *non-empty* 4-Massey product forces the vanishing of a new invariant defined by Isaksen [21]. In particular, prior to the present paper there was not even a strategy for approaching the 4-Massey vanishing conjecture.

⋆ ⋆ ⋆

We now introduce the basic concepts, and the precise notation, needed to state the main results of the paper.

1.1. **Basic Notation.** Throughout the paper, F will denote a field of characteristic $\neq 2$. We will use the usual notation $\mathrm{H}^*(F, A) := \mathrm{H}^*(G_F, A)$ for the Galois cohomology of F with coefficients in the G_F-module A.

Recall that Kummer theory yields a canonical isomorphism

$$F^\times/F^{\times 2} \xrightarrow{\cong} \mathrm{H}^1(F, \mathbb{F}_2).$$

For an element $x \in F^\times$, we write $[x]$ for its class in $F^\times/F^{\times 2}$, and $\chi_x \in \mathrm{H}^1(F, \mathbb{F}_2)$ for the image of $[x]$ under the Kummer isomorphism. We will usually consider χ_x as a (continuous) homomorphism

$$\chi_x : G_F \to \mathbb{F}_2$$

via the canonical identification $\mathrm{H}^1(F, \mathbb{F}_2) = \mathrm{Hom}^{\mathrm{cont}}(G_F, \mathbb{F}_2)$.

Given $a, b \in F^\times$, we will usually write $(a, b)_F$ (or (a, b) when F is understood) for the cup-product $\chi_a \cup \chi_b \in \mathrm{H}^2(F, \mathbb{F}_2)$. This notation borrows from the fact that $\mathrm{H}^2(F, \mathbb{F}_2)$ is canonically isomorphic to the 2-torsion of $\mathrm{Br}(F)$, and that the class of the quaternion algebra $(a, b)_F$ corresponds to $\chi_a \cup \chi_b$ via this identification.

1.2. **The Groups $\mathbb{U}_n(\mathbb{F}_2)$.** The group $\mathbb{U}_n(\mathbb{F}_2)$, for $n \geq 2$, is comprised of the $n \times n$ upper-triangular matrices with entries in $\mathbb{F}_2$ with 1's along the diagonal. The group $\mathbb{U}_n(\mathbb{F}_2)$ is endowed with $n - 1$ homomorphisms

$$s_1, \ldots, s_{n-1} : \mathbb{U}_n(\mathbb{F}_2) \to \mathbb{F}_2$$

defined as $s_i(g) = g_{i,i+1}$ (the i-th near-diagonal component of g).

The center $\mathcal{Z}(\mathbb{U}_n(\mathbb{F}_2))$ of $\mathbb{U}_n(\mathbb{F}_2)$ consists of those matrices whose only possibly non-zero coefficient above the diagonal is in the top-right corner. In particular, the map $g \mapsto g_{1,n}$ induces an isomorphism $\mathcal{Z}(\mathbb{U}_n(\mathbb{F}_2)) \cong \mathbb{F}_2$. We write $\overline{\mathbb{U}}_n(\mathbb{F}_2) := \mathbb{U}_n(\mathbb{F}_2)/\mathcal{Z}(\mathbb{U}_n(\mathbb{F}_2))$, and consider $\mathbb{U}_n(\mathbb{F}_2)$ as an extension of $\overline{\mathbb{U}}_n(\mathbb{F}_2)$ by $\mathbb{F}_2$. Furthermore, we denote by ξ_n the element of $\mathrm{H}^2(\overline{\mathbb{U}}_n(\mathbb{F}_2), \mathbb{F}_2)$ associated to this extension.

1.3. **Massey Products.** Let Γ be a profinite group, and let $x_1, \ldots, x_n \in \mathrm{H}^1(\Gamma, \mathbb{F}_2)$ be given. In this context, we say that the n-Massey product $\langle x_1, \ldots, x_n \rangle$ is **defined** provided that there exists a homomorphism $\varphi : \Gamma \to \overline{\mathbb{U}}_{n+1}(\mathbb{F}_2)$ such that $x_i = s_i \circ \varphi$ for $i = 1, \ldots, n$. Furthermore, in this case we say that φ is a **defining system** for the n-Massey product $\langle x_1, \ldots, x_n \rangle$.

The **n-Massey product** associated to the defining system φ, denoted by $\langle x_1, \ldots, x_n \rangle_\varphi$, is defined to be $\varphi^* \xi_{n+1} \in \mathrm{H}^2(\Gamma, \mathbb{F}_2)$, the pull-back of ξ_{n+1} along φ. Note that one has $\langle x_1, \ldots, x_n \rangle_\varphi = 0$ if and only if the map $\varphi : \Gamma \to \overline{\mathbb{U}}_{n+1}(\mathbb{F}_2)$ lifts to a homomorphism $\widetilde{\varphi} : \Gamma \to \mathbb{U}_{n+1}(\mathbb{F}_2)$.

Finally, the **n-Massey product** $\langle x_1, \ldots, x_n \rangle$ is defined as the set

$$\langle x_1, \ldots, x_n \rangle := \{\langle x_1, \ldots, x_n \rangle_\varphi\}$$

where φ varies over all defining systems for $\langle x_1, \ldots, x_n \rangle$. In particular, the n-Massey product $\langle x_1, \ldots, x_n \rangle$ is non-empty if and only if it is defined. As mentioned above we will be primarily interested in situations where the n-Massey product $\langle x_1, \ldots, x_n \rangle$ contains 0, and we say that "$\langle x_1, \ldots, x_n \rangle$ vanishes" in such situations. Note that, when we say "$\langle x_1, \ldots, x_n \rangle$ vanishes" we are also implying that $\langle x_1, \ldots, x_n \rangle$ is defined (as $\langle x_1, \ldots, x_n \rangle$ is non-empty).

Remark. We have presented the definition of defining systems and Massey products in the context of group-cohomology from the point of view of *embedding problems*. This is nevertheless equivalent to the classical (highly technical) definitions, by the work of Dwyer [8]. For our purposes, Massey products are defined as above.

We will simplify the notation somewhat in the context of Galois cohomology. Namely, given $a_1, \ldots, a_n \in F^\times$, we write $\langle a_1, \ldots, a_n \rangle$ instead of $\langle \chi_{a_1}, \ldots, \chi_{a_n} \rangle$. We will follow this convention when talking about defining systems as well as Massey products themselves.

1.4. **Main Results.** We are now prepared to state our main theorems which characterize the vanishing of 4-Massey products in mod-2 Galois cohomology.

Theorem A – *Let F be a field of characteristic $\neq 2$. Let $a, b, c, d \in F^\times$ be given, choose square roots $\sqrt{a}$ resp. $\sqrt{d}$ of a resp. d in an algebraic closure of F, and put $E := F[\sqrt{a}, \sqrt{d}]$. Then the following are equivalent:*

1. *The 4-Massey product $\langle a, b, c, d\rangle$ vanishes (i.e., it is defined and contains 0).*
2. *There exist $B \in F[\sqrt{a}]$, $C \in F[\sqrt{d}]$ and $z_1, z_2 \in F^\times$ such that the following conditions hold:*
   (a) *One has $\mathrm{N}_{F[\sqrt{a}]/F}(B) = b \cdot z_1^2$ and $\mathrm{N}_{F[\sqrt{d}]/F}(C) = c \cdot z_2^2$.*
   (b) *One has $(B, C)_E = 0$, $(B, c)_{F[\sqrt{a}]} = 0$, $(b, C)_{F[\sqrt{d}]} = 0$ and $(b, c)_F = 0$.*
3. *There exist $B \in F[\sqrt{a}]$, $C \in F[\sqrt{d}]$ and $z_1, z_2 \in F^\times$ such that the following conditions hold:*
   (a) *One has $\mathrm{N}_{F[\sqrt{a}]/F}(B) = b \cdot z_1^2$ and $\mathrm{N}_{F[\sqrt{d}]/F}(C) = c \cdot z_2^2$.*
   (b) *One has $(B, C)_E = (B, c)_E = (b, C)_E = (b, c)_E = 0$.*

Note that condition (2) of Theorem A can be readily described in terms of polynomial equations over F, hence defining an (affine) F-variety. Theorem A then shows that this variety has an F-point if and only if $\langle a, b, c, d\rangle$ vanishes. Note, however, that these equations *depend* on whether a, d, and/or ad are squares in F (the definition involves a Weil-restriction from $F[\sqrt{a}, \sqrt{d}]$ to F); in other words, the variety is not compatible with base-change to extensions of F. This is undesirable, as compatibility with base-change will be an important property towards the end of the paper. With some additional work, we are able to obtain the following characterization theorem which provides us with our desired uniform polynomial equations.

Theorem B – *Let F be a field of characteristic $\neq 2$ and let $a, b, c, d \in F^\times$ be given. Consider the finite étale F-algebra*

$$\mathcal{E} := F[X, Y]/(X^2 - a, Y^2 - d).$$

Then the following are equivalent:

1. *The 4-Massey product $\langle a, b, c, d\rangle$ vanishes.*
2. *There exist $x_1, y_1, x_2, y_2 \in F$, $z_1, z_2 \in F^\times$ and $u, v \in \mathcal{E}$ such that the following equations are satisfied:*
   (a) *One has $x_1^2 - y_1^2 \cdot a = b \cdot z_1^2$ and $x_2^2 - y_2^2 \cdot d = c \cdot z_2^2$.*
   (b) *One has $u^2 - \widetilde{B}v^2 = \widetilde{C}$ in $\mathcal{E}$, where $\widetilde{B} = x_1 + y_1 \cdot X \in \mathcal{E}$ and $\widetilde{C} = x_2 + y_2 \cdot Y \in \mathcal{E}$.*

Note that the polynomial equations described by condition (2) of Theorem B actually have the same shape over any field which contains a, b, c, d. The F-variety defined by these equations is what we will eventually call **the splitting variety for** $\langle a, b, c, d\rangle$.

It is important to note that both Theorems A and B will play a key role in this paper. Indeed, condition (2) of Theorem A has an immediate and direct formulation involving cup-products in mod-2 Galois cohomology (we exhibit some direct applications, over any field, in §4). On the other hand, condition (2) of Theorem B defines a splitting variety whose geometry is remarkably simple. In generic situations, it satisfies the Hasse principle for the existence of rational points; in all cases, the local-to-global principle is governed by the Brauer-Manin obstruction, which takes a simple form here. See Theorem A.1 in the Appendix for a detailed statement. We thereby obtain a more precise version of the Theorem announced above:

Theorem C – *Let F be a number field, and let $a, b, c, d \in F^\times$ be given. Then the following are equivalent:*

(1) *The 4-Massey product $\langle a, b, c, d\rangle$ vanishes.*
(2) *The 4-Massey product $\langle a, b, c, d\rangle$ is defined.*

If furthermore ad, ab, cd are all non-squares in F, then the above conditions are further equivalent to:

(3) *One has $(a, b)_F = (b, c)_F = (c, d)_F = 0$.*

Theorem C will be proved in Theorems 6.1, 6.2 below. It is natural to ask whether the implication (3) $\implies$ (1) holds in general. It turns out that this implication *fails in general*, even over number fields. See Remark 6.3, Example A.15, and the surrounding discussions for more details.

⋆ ⋆ ⋆

Organization of the paper. After some preliminaries in the next section, we prove Theorem A in §3. In section 4, we give some first applications of Theorem A by proving a few cases of the 4-Massey vanishing conjecture by hand, over arbitrary fields. Then in §5 we introduce the splitting variety $\mathscr{X}_F$, as well as a variant X_F which will simplify some calculations. The next section, that is §6, gives a proof of Theorem C. Finally in §7 we make some of our constructions explicit, and explain concretely how to get a Galois extension with group $\mathbb{U}_5(\mathbb{F}_2)$ when $\langle a, b, c, d\rangle$ vanishes and a, b, c, d are linearly independent modulo squares; incidentally, this gives an alternative, more pedestrian proof for the implication (3) $\implies$ (1) in Theorem A in this case.

An Appendix by Wittenberg shows that the variety X_F satisfies the local-to-global principle alluded to above, which is of course a crucial ingredient for Theorem C.

Ackowledgements. First and foremost, we have been in touch very frequently with Olivier Wittenberg while writing this paper. We thank him warmly for writing the Appendix, and for various suggestions. We also thank Adriano Marmora for suggesting us to contact Olivier in the first place. Moreover, we warmly thank Nguyễn Duy Tân for his interest and insight, and for his extremely inspiring collaboration with the second author. It is a great pleasure to also thank B. I. Chetard, I. Efrat, Ch. Kapulkin, E. Matzri, C. McLeman, D. Neftin, M. Palaisti, C. Quadrelli and K. Wickelgren for inspiring discussions. Finally, we thank the referee for helpful comments regarding the exposition.

2. Preliminaries

2.1. **The groups $\mathbb{U}_3(\mathbb{F}_2)$ and $\mathbb{U}_5(\mathbb{F}_2)$.** We shall need special notation for these two groups. First note that we *define* the dihedral group of order 8 to be $\mathbb{U}_3(\mathbb{F}_2)$, and we may write $D_4 = \mathbb{U}_3(\mathbb{F}_2)$. An element $g \in D_4$ is a matrix of the form

$$g = \begin{pmatrix} 1 & s_1(g) & t(g) \\ 0 & 1 & s_2(g) \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus D_4 is equipped with maps $s_1, s_2, t\colon D_4 \to \mathbb{F}_2$. (The letter t is for “top”.) Note that the first two are group homomorphisms, but t is not. Our favourite generators are the involutions σ_1 and σ_2, with $s_i(\sigma_i) = 1$ and $s_j(\sigma_i) = t(\sigma_i) = 0$ for $j \neq i$.

Similarly, an element $g \in \mathbb{U}_5(\mathbb{F}_2)$ will be written

$$\begin{pmatrix} 1 & s_1(g) & t_1(g) & u_1(g) & z(g) \\ 0 & 1 & s_2(g) & u_3(g) & u_2(g) \\ 0 & 0 & 1 & s_3(g) & t_2(g) \\ 0 & 0 & 0 & 1 & s_4(g) \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} .$$

This endows $\mathbb{U}_5(\mathbb{F}_2)$ with maps $s_1, \ldots, z \colon \mathbb{U}_5(\mathbb{F}_2) \to \mathbb{F}_2$, and s_i is a group homomorphism for $1 \leq i \leq 4$.

More generally the group $\mathbb{U}_n(\mathbb{F}_2)$ has homomorphisms $s_i \colon \mathbb{U}_n(\mathbb{F}_2) \to \mathbb{F}_2$ for $1 \leq i \leq n-1$, already mentioned in the Introduction, obtained by looking at the entries on what we call the near-diagonal. If we define elements σ_i by requiring $s_i(\sigma_i) = 1$ while all the other entries of σ_i above the diagonal are 0, then each σ_i is an involution, and these generate $\mathbb{U}_n(\mathbb{F}_2)$.

We note that $\mathbb{U}_n(\mathbb{F}_2)$ has an automorphism which exchanges σ_i with σ_{n-i}. Most of our considerations respect this symmetry, and this motivates the notation above for $\mathbb{U}_5(\mathbb{F}_2)$. (The automorphism is given by "the transpose but along the other diagonal", followed by $g \mapsto g^{-1}$.)

2.2. **Around the group D_4.** We write $s = (s_1, s_2) \colon D_4 \to C_2 \times C_2$, where we have identified $\mathbb{F}_2$ with the cyclic group of order 2 in multiplicative notation, written C_2. There is an exact sequence

$$1 \longrightarrow \mathbb{F}_2 \longrightarrow D_4 \xrightarrow{s} C_2 \times C_2 \longrightarrow 1 ,$$

the kernel of s being generated by $[\sigma_1, \sigma_2]$ (which is the element g with $t(g) = 1$ and $s_i(g) = 0$, $i = 1, 2$).

The quotient group $C_2 \times C_2$ is generated by the images of σ_1, σ_2, written $\overline{\sigma}_1, \overline{\sigma}_2$. The cohomology group $\mathrm{H}^1(C_2^2, \mathbb{F}_2) = \mathrm{Hom}(C_2^2, \mathbb{F}_2)$ is endowed with the dual basis $\overline{s}_1, \overline{s}_2$. The next Lemma is very well-known:

Lemma 2.1 – *The cohomology class of the above extension is $\overline{s}_1 \overline{s}_2 \in \mathrm{H}^2(C_2^2, \mathbb{F}_2)$.* □

We introduce the two elementary abelian subgroups E_1, E_2, where E_1 is the kernel of s_2 and E_2 is the kernel of s_1 (the switch is justified by the next Lemma). A very useful observation is that t, when restricted to either of these, is a group homomorphism.

Lemma 2.2 – *The corestriction*

$$\mathrm{cores} \colon \mathrm{H}^1(E_i, \mathbb{F}_2) \longrightarrow \mathrm{H}^1(D_4, \mathbb{F}_2)$$

carries $t|_{E_i}$ to s_i, for $i = 1, 2$. More generally if Γ is any profinite group with a continuous homomorphism $\varphi \colon \Gamma \to D_4$, and if $H = \varphi^{-1}(E_i)$ is assumed to have index 2 in Γ, then the corestriction

$$\mathrm{cores} \colon \mathrm{H}^1(H, \mathbb{F}_2) \longrightarrow \mathrm{H}^1(\Gamma, \mathbb{F}_2)$$

carries $t \circ \varphi$ to $s_i \circ \varphi$, for $i = 1, 2$.

Proof. We recall some properties of the corestriction

$$\mathrm{cores} \colon \mathrm{H}^i(N, M) \longrightarrow \mathrm{H}^i(G, M)$$

where N is a subgroup of finite index of the profinite group G, and M is a G-module. In fact, we only need to consider the case when M has a trivial action, N is closed of index 2 (and thus is normal) in G, and $i = 1$, so that

$$\mathrm{cores} \colon \mathrm{Hom}(N, M) \longrightarrow \mathrm{Hom}(G, M) .$$

Here if $f\colon N \to M$, then the map $\operatorname{cores}(f)\colon G \to M$ is characterized as follows. Pick $\tau \in G \smallsetminus N$. Then (i) $\operatorname{cores}(f)(n) = f(n) + f(\tau^{-1}n\tau)$ for $n \in N$, and (ii) $\operatorname{cores}(f)(\tau) = f(\tau^2)$. This follows from the material in [46], §2, for example.

Let us use this for $N = E_1$ and $G = D_4$. If

$$n = \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & c & d \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

then

$$\tau^{-1}n\tau = \begin{pmatrix} 1 & a & a+b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Moreover

$$\tau^2 = \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus $t(n) + t(\tau^{-1}n\tau) = b + a + b = a = s_1(n)$, and $t(\tau^2) = c = s_1(\tau)$. Hence the first statement of the lemma for $i = 1$. The other cases are treated similarly. □

2.3. D_4-extensions of fields.

We proceed to apply the above observations in a Galois-theoretic context, but a couple of comments are in order. First, the group D_4 has an automorphism exchanging σ_1 and σ_2, but the Proposition below is not "symmetric" in this way – it involves the subgroup E_2 and not E_1, for example (so that one could get a new Proposition by exchanging the roles of various players). Second, when asked for a basis for E_2, the reader would probably offer $[\sigma_1, \sigma_2], \sigma_2$; however, later considerations with $\mathbb{U}_5(\mathbb{F}_2)$ compel us to work with $\sigma_2[\sigma_1, \sigma_2], \sigma_2$ instead (specifically, we want Lemma 2.5 to have the simple form given below). This is reflected in the Proposition below, since the dual basis of $\mathrm{H}^1(E_2, \mathbb{F}_2)$ is $t, s_2 + t$ (or, in more complete notation, $t|_{E_2}, s_2|_{E_2} + t|_{E_2}$).

Proposition 2.3 – *Let F be a field of characteristic $\neq 2$ and let $a, b \in F^\times$ be given. Then the following are equivalent:*

(1) $(a, b)_F = 0$.
(2) *There exists a continuous homomorphism $\varphi\colon G_F \longrightarrow D_4$ such that $s_1 \circ \varphi = \chi_a$ and $s_2 \circ \varphi = \chi_b$.*
(3) *There exist $x, y, z \in F$ such that $x^2 - ay^2 = bz^2$, with $z \neq 0$.*

When the equivalent conditions hold and $B := x + y\sqrt{a}$, we will say that φ from (2) and x, y, z from (3) are consistent, *provided that $\chi_{bB} = t \circ \varphi$ and $\chi_B = (s_2 + t) \circ \varphi$ as elements of $\mathrm{H}^1(F[\sqrt{a}], \mathbb{F}_2)$. Then given any φ as in (2), we can choose x, y, z as in (3) which are consistent with φ. Conversely, given any x, y, z as in (3), we can choose φ as in (2) which is consistent with x, y, z.*

Again, this is essentially known, but we need the precise version given here. Note that it is necessary to deal with the cases when either a or b is a square, and that the proof below gives more concrete information in some situations. Also note that, as promised, the elements $t, s_2 + t$, related to E_2, make an uncanny appearance.

Proof. We can combine χ_a and χ_b into a homomorphism $G_F \to C_2 \times C_2$. The obstruction to lifting it to D_4 is the cohomology class of the extension, so that Lemma 2.1 gives immediately the equivalence of (1) and (2).

We first conduct the rest of the proof under the following

Assumption. Assume for the moment that a is not a square in F.

Suppose (2) holds. Note that $\varphi^{-1}(E_2) = G_{F[\sqrt{a}]}$. Let $B' = x' + y'\sqrt{a} \in F[\sqrt{a}]$ be such that $\chi_{B'} = t \circ \varphi|_{G_{F[\sqrt{a}]}}$. Since a is not a square in F, the subgroup $G_{F[\sqrt{a}]}$ has index 2 in G_F. Lemma 2.2 shows then that $\mathrm{cores}(\chi_{B'}) = s_2 \circ \varphi = \chi_b$. Now recall that under the identifications of $\mathrm{H}^1(F, \mathbb{F}_2)$ with $F^\times/F^{\times 2}$ and of $\mathrm{H}^1(F[\sqrt{a}], \mathbb{F}_2)$ with $F[\sqrt{a}]^\times/F[\sqrt{a}]^{\times 2}$, the corestriction becomes the usual norm $N_{F[\sqrt{a}]/F}$. It follows that

$$N_{F[\sqrt{a}]/F}(B') = (x')^2 - a(y')^2 = b \text{ mod squares}\,.$$

This gives (3), clearly, but we need to modify B' to get the consistency statement. And indeed, we put $B = bB'$, so that $B' = bB$ modulo squares, and the result follows.

Next, we must prove that (3) implies (2), or equivalently (1). We may as well suppose that a and b are both not squares, for (1) holds trivially otherwise. The assumption is that b is a norm from $F[\sqrt{a}]$, or in more cohomological terms, that χ_b is the corestriction of an element from the subgroup $G_{F[\sqrt{a}]}$. That the cup product $\chi_a\chi_b = 0$ then follows from the Arason exact sequence [1].

However, to prove the claimed consistency, a more explicit argument is needed. Assume b is not a square. The element $B = x + y\sqrt{a}$, where x, y are as in (3), is fixed up to squares by $\mathrm{Gal}(F[\sqrt{a}, \sqrt{b}]/F)$, as is readily checked. It follows that $K = F[\sqrt{a}, \sqrt{b}, \sqrt{B}]$ is Galois over F (by equivariant Kummer theory, if you will).

We distinguish two cases, and assume first that a and b are not equal modulo squares. We now introduce elements $\sigma_1, \sigma_2 \in \mathrm{Gal}(K/F)$ which are dual to $\sqrt{a}, \sqrt{b}$ in the obvious sense. Direct computation shows that $\sigma_1^2 = \sigma_2^2 = 1$, and that $[\sigma_1, \sigma_2](\sqrt{B}) = -\sqrt{B}$, so that $[\sigma_1, \sigma_2] \neq 1$. From this one draws readily that $\mathrm{Gal}(K/F) \cong D_4$ and (again!) that (2) holds. Also, one computes that $\sigma_2(\sqrt{B}) = \pm\sqrt{B}$. We want to ensure that $\sigma_2(\sqrt{B}) = -\sqrt{B}$, and to achieve this we replace σ_2 by $\sigma_2[\sigma_1, \sigma_2]$ if needed. Having done this, the elements $\sqrt{B}$, $\sqrt{bB}$ are dual to σ_2, $\sigma_2[\sigma_1, \sigma_2]$, and one checks that the corresponding map $\varphi\colon G_F \to D_4$ has precisely the required consistency.

If $a = b$ modulo squares, one sees that $\mathrm{Gal}(K/F)$ has order 4, so is abelian, and if σ is the non-trivial element of $\mathrm{Gal}(F[\sqrt{a}]/F)$ extended to $\mathrm{Gal}(K/F)$, another direct calculation shows that σ does not have order 2. So $\mathrm{Gal}(K/F) \cong C_4$ can be identified with the subgroup of D_4 generated by $\sigma_1\sigma_2$, and (2) follows. Consistency is automatic.

Finally, if b is a square in F, we use the same extension $K = F[\sqrt{a}, \sqrt{B}]$ of F, but compute that $\mathrm{Gal}(K/F) \cong C_2^2$. We identify this group with E_1 appropriately, yielding a consistent φ.

The case when a is a square.

In this situation (1) holds trivially, and thus (2) also holds. As for (3), if $a = u^2$ then put

$$x_0 = \frac{b+1}{2} \quad \text{and} \quad y_0 = \frac{1-b}{2u}$$

and compute that $x_0^2 - ay_0^2 = b$.

Let us see how we can adjust φ from x, y, z. Put $B = x + y\sqrt{a} \in F$, and consider the characters χ_{bB} and χ_b, together defining a homomorphism $G_F \to C_2 \times C_2$. Identifying Klein's group with E_2 sitting in D_4 appropriately, we obtain $\varphi\colon G_F \to D_4$ satisfying our requirements.

Our very last step is to see how one can adjust x, y, z from φ. First put $B_0 = x_0 + y_0\sqrt{a} \in F$ where x_0 and y_0 are as above, which is a non-zero element since $B_0(x - y\sqrt{a}) = b \neq 0$. For $f \in F$, put $x = \frac{f}{B_0}x_0$ and $y = \frac{f}{B_0}y_0$, so that $x^2 - ay^2 = bz^2$ for some $z \in F^\times$, while $B = x + y\sqrt{a} = f$, an arbitrary element of F. Of course φ lands in the subgroup E_2, so we only need to pick f so that $\chi_f = (s_2 + t) \circ \varphi = \chi_B$; we have then (2) and (3) simultaneously and consistently. □

2.4. **The group $\mathbb{U}_5(\mathbb{F}_2)$ and its subquotients.** Let S (for "square") be the subgroup of matrices of the form

$$\begin{pmatrix} 1 & 0 & 0 & y_1 & y_2 \\ 0 & 1 & 0 & y_3 & y_4 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} .$$

Then $S \cong C_2^4$, and our favourite $\mathbb{F}_2$-basis, denoted e_1, e_2, e_3, e_4, will be given by

$$e_1 = e = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} , \; e_2 = \sigma_1 e \sigma_1^{-1} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} ,$$

$$e_3 = \sigma_4 e \sigma_4^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} , \; e_4 = (\sigma_1\sigma_4) e (\sigma_1\sigma_4)^{-1} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} .$$

The centralizer of S in $\mathbb{U}_5(\mathbb{F}_2)$, which we denote by $\mathscr{C}(S)$, is easily seen to be comprised of the elements g for which $s_1(g) = s_4(g) = 0$, that is $\mathscr{C}(S) = \ker s_1 \cap \ker s_4$. In particular σ_2 and σ_3 centralize S, and from the formulae above we see that S is normal in $\mathbb{U}_5(\mathbb{F}_2)$. We shall write $G = \mathbb{U}_5(\mathbb{F}_2)/S$, which we identify with $D_4 \times D_4$, as we visibly may. The image of $\mathscr{C}(S)$ in G, that is $\mathscr{C}(S)/S$, will be denoted by N, a normal subgroup of G.

One has $G/N = \mathbb{U}_5(\mathbb{F}_2)/\mathscr{C}(S) = \langle \sigma_1, \sigma_4 \rangle \cong C_2^2$ (we shall often write σ_i for the image of this element in various quotients, whenever no confusion can arise). The next observation is now clear, but it is crucial:

Lemma 2.4 – *The action of G/N on S, induced by conjugation, turns it into a free $\mathbb{F}_2[G/N]$-module of rank 1. A specific isomorphism $\mathbb{F}_2[G/N] \to S$ is given by $1 \mapsto e$, for example.* □

The group N itself also has a simple structure: one has $N \cong C_2^4$, a basis being

$$\sigma_2[\sigma_1, \sigma_2], \; \sigma_2, \; \sigma_3, \; \sigma_3[\sigma_4, \sigma_3].$$

(A choice which respects the ambient "symmetry" already alluded to.) The corresponding dual basis of $\mathrm{H}^1(N, \mathbb{F}_2)$ will be denoted x_1, x_2, x_3, x_4. To bridge the notation with that of the previous sections, we regard N as sitting in $D_4 \times D_4$, which itself possesses six maps $s_1, s_2, t_1, s_3, s_4, t_2$ to $\mathbb{F}_2$, using names adapted from §2.1. With this notation, one has $x_1 = t_1$, $x_2 = s_2 + t_1$, $x_3 = s_3 + t_2$, and $x_4 = t_2$ (where restrictions to N are implicit).

Next we introduce some subgroups of S, and use them to produce extensions of N. These extensions turn out to control the entire situation, as will be explained. So we let

$$S_1 := \langle e_2, e_3, e_4 \rangle \, , \; S_2 := \langle e_1, e_3, e_4 \rangle, \; S_3 := \langle e_1, e_2, e_4 \rangle \, .$$

(The group S_4 which could be defined using the same logic will not play any role, as it happens. Also note that among these three, only S_1 respects the ambient "symmetry".)

Lemma 2.5 – *Using the notation above, the following hold:*

(1) *The cohomology class of the extension*

$$0 \longrightarrow S/S_1 \cong \mathbb{F}_2 \longrightarrow \mathscr{C}(S)/S_1 \longrightarrow N \longrightarrow 1$$

is x_2x_3.

(2) *The cohomology class of the extension*

$$0 \longrightarrow S/S_2 \cong \mathbb{F}_2 \longrightarrow \mathscr{C}(S)/S_2 \longrightarrow N \longrightarrow 1$$

is x_1x_3.

(3) *The cohomology class of the extension*

$$0 \longrightarrow S/S_3 \cong \mathbb{F}_2 \longrightarrow \mathscr{C}(S)/S_3 \longrightarrow N \longrightarrow 1$$

is x_2x_4.

Proof. An element of $\mathscr{C}(S)$ has the form

$$g = \begin{pmatrix} 1 & 0 & t_1(g) & u_1(g) & z(g) \\ 0 & 1 & s_2(g) & u_3(g) & u_2(g) \\ 0 & 0 & 1 & s_3(g) & t_2(g) \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let us multiply two of these, say g and g', using the shorthand $s_2 = s_2(g)$ and $s_2' = s_2(g')$, and so on:

$$(*) \qquad gg' = \begin{pmatrix} 1 & 0 & t_1 + t_1' & t_1s_3' + u_1 + u_1' & t_1t_2' + z + z' \\ 0 & 1 & s_2 + s_2' & s_2s_3' + u_3 + u_3' & s_2t_2' + u_2 + u_2' \\ 0 & 0 & 1 & s_3 + s_3' & t_2 + t_2' \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We shall use the set-theoretic section $\sec\colon N \to \mathscr{C}(S)$ given by

$$\sec(g) = \begin{pmatrix} 1 & 0 & t_1(g) & 0 & 0 \\ 0 & 1 & s_2(g) & 0 & 0 \\ 0 & 0 & 1 & s_3(g) & t_2(g) \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let us prove (1). Using the section $N \to \mathscr{C}(S)/S_1$ induced by sec, we end up with the bijection of sets $\Phi\colon S/S_1 \times N \to \mathscr{C}(S)/S_1$ given by

$$\Phi(x,g) = x\sec(g) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & x & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \times \sec(g) = \begin{pmatrix} 1 & 0 & t_1(g) & 0 & 0 \\ 0 & 1 & s_2(g) & x & 0 \\ 0 & 0 & 1 & s_3(g) & t_2(g) \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Here we have used (*) to perform the calculation. A caveat : in these expressions, we have identified S/S_1 with $\mathbb{F}_2$ (this can be done uniquely!), so that $x \in S/S_1$ can be seen as an entry (0 or 1) of a matrix. A second caveat is that the matrix displayed is understood modulo S_1 only.

From the theory of group extensions, we have $\Phi(x,g)\Phi(y,g') = \Phi(x+y+c(g,g'),gg')$, where the expression $c(g,g')$, is what we are after, that is, it is a two-cocycle representing the cohomology class of the extension under scrutiny. So we compute, from (*), that

$$\Phi(x,g)\Phi(y,g') = \begin{pmatrix} 1 & 0 & t_1+t_1' & t_1s_3' & t_1t_2' \\ 0 & 1 & s_2+s_2' & s_2s_3'+x+y & s_2t_2' \\ 0 & 0 & 1 & s_3+s_3' & t_2+t_2' \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Another useful computational remark is that, in S identified with the additive group of 2×2-matrices, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a+b+c+d)e_1+(a+b)e_2+(b+d)e_3+be_4 \equiv \begin{pmatrix} 0 & 0 \\ a+b+c+d & 0 \end{pmatrix} \bmod S_1 .$$

Thus the last matrix displayed, viewed in $\mathscr{C}(S)/S_1$, is also

$$\begin{pmatrix} 1 & 0 & t_1+t_1' & 0 & 0 \\ 0 & 1 & s_2+s_2' & x+y+s_2s_3'+t_1s_3'+s_2t_2'+t_1t_2' & 0 \\ 0 & 0 & 1 & s_3+s_3' & t_2+t_2' \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

We conclude that, as predicted, $c(g,g') = s_2(g)s_3(g') + t_1(g)s_3(g') + s_2(g)t_2(g') + t_1(g)t_2(g') = x_2(g)x_3(g')$, and c is indeed the cup-product of x_2 and x_3.

The proofs of (2) and (3) are similar. □

Remark 2.6. Note that in each case $\mathscr{C}(S)/S_i \cong C_2^2 \times D_4$.

3. The fundamental cup-products

In this section, we prove Theorem A, as stated in the Introduction. We shall see that we are led naturally to another statement first, in which the following notation is used. When $a \in F$, we put $F_a = F[X]/(X^2-a)$. When $e+fX \in F_a$, we define its *norm* to be $\mathrm{N}_{F_a/F}(e+fX) = e^2-af^2$. When a square root $\sqrt{a}$ has been chosen in some field containing F, there is a homomorphism $F_a \to F[\sqrt{a}]$ mapping X to $\sqrt{a}$. Of course when a is not a square in F, this map is an isomorphism of extensions of F, and the norm just introduced coincides with the usual norm map between fields. However, it is useful to work with F_a for those occasions when a is already a square in F.

We start by the implication (1) $\implies$ (2) from Theorem A.

3.1. Proving that the four cup-products vanish.

Theorem 3.1 – *Let F be a field of characteristic not 2, let $a,b,c,d \in F^\times$ be given and put $E := F[\sqrt{a},\sqrt{d}]$. Suppose there exist a continuous homomorphism $\overline{\varphi}\colon G_F \to \overline{\mathbb{U}}_5(\mathbb{F}_2)$ such that $\chi_a = s_1\circ\overline{\varphi}$, $\chi_b = s_2\circ\overline{\varphi}$, $\chi_c = s_3\circ\overline{\varphi}$, and $\chi_d = s_4\circ\overline{\varphi}$. (In other words, we assume that $\langle a,b,c,d\rangle$ is defined.) Then there exist $\widetilde{B} \in F_a$ and $\widetilde{C} \in F_d$ such that the following hold, where B denotes the image of $\widetilde{B}$ under $F_a \to F[\sqrt{a}]$ and C denotes the image of $\widetilde{C}$ under $F_d \to F[\sqrt{d}]$.*

1. *One has $\mathrm{N}_{F_a/F}(\widetilde{B}) = b$ modulo squares and $\mathrm{N}_{F_d/F}(\widetilde{C}) = c$ modulo squares.*
2. *One has $(B,c)_{F[\sqrt{a}]} = 0$, $(b,C)_{F[\sqrt{d}]} = 0$, and $(b,c)_F = 0$.*
3. *There is a class $u \in \mathrm{H}^2(F,\mathbb{F}_2)$ whose image under the canonical restriction map $\mathrm{H}^2(F,\mathbb{F}_2) \longrightarrow \mathrm{H}^2(E,\mathbb{F}_2)$ is $(B,C)_E$.*
4. *Suppose that $\overline{\varphi}$ can be lifted to $\varphi\colon G_F \to \mathbb{U}_5(\mathbb{F}_2)$. (In other words, assume that $\langle a,b,c,d\rangle$ vanishes.) Then one has $(B,C)_E = 0$.*

Note that the mere existence of $\widetilde{B}$ and $\widetilde{C}$ implies also that $(a,b)_F = 0$ and $(c,d)_F = 0$, by Proposition 2.3.

Proof. First we consider the composition

$$\overline{\overline{\varphi}}\colon G_F \longrightarrow \overline{U}_5(\mathbb{F}_2) \longrightarrow \overline{\mathbb{U}}_5(\mathbb{F}_2)/S = G = D_4 \times D_4\,.$$

Projecting further onto the left factor, we make a first use of Proposition 2.3. We draw the existence of $x, y, z \in F$ satisfying $x^2 - ay^2 = bz^2$, that is $\mathrm{N}_{F_a/F}(\widetilde{B}) = bz^2$, with $\widetilde{B} = x + yX \in F_a$. If $B = x + y\sqrt{a}$ is the corresponding element, then the Proposition says that we can arrange to have $\chi_{bB} = t_1 \circ \overline{\varphi} = x_1 \circ \overline{\varphi}$, $\chi_B = (s_2 + t_1) \circ \overline{\varphi} = x_2 \circ \overline{\varphi}$. (We fully use the notation from §2.4.)

Using the right factor, we find elements $\widetilde{C}$ and C similarly, such that $\chi_C = x_3 \circ \overline{\varphi}$, $\chi_{cC} = x_4 \circ \overline{\varphi}$. This also proves the first assertion.

We prove that the cup-products vanish as announced in the second assertion, starting with $(b,c)_F = 0$ (which of course does not depend on the choices for B and C). For this, consider the map

$$\mathbb{U}_5(\mathbb{F}_2) \longrightarrow \mathbb{U}_3(\mathbb{F}_2) = D_4$$

which discards the top row and the rightmost column of an element of $\mathbb{U}_5(\mathbb{F}_2)$; this factors through $\overline{U}_5(\mathbb{F}_2)$. Postcomposing $\overline{\varphi}$ with this, we draw from Proposition 2.3 that $(b,c)_F = 0$, as required.

Next we turn to the proof of $(B,c)_{F[\sqrt{a}]} = 0$, the cup-product $(b,C)_{F[\sqrt{d}]}$ being treated in a similar way. Define a group homomorphism $\pi\colon \ker(s_1) \subset \overline{\mathbb{U}}_5(\mathbb{F}_2) \to \mathbb{U}_3(\mathbb{F}_2) = D_4$ by

$$g \mapsto \begin{pmatrix} 1 & t_1(g) & u_1(g) \\ 0 & 1 & s_3(g) \\ 0 & 0 & 1 \end{pmatrix}.$$

One checks that π is well-defined. Note that $\pi \circ \overline{\varphi} : G_{F[\sqrt{a}]} \to D_4$ is a lift for $(t_1 \circ \overline{\varphi}, s_3 \circ \overline{\varphi})\colon G_{F[\sqrt{a}]} \to \mathbb{F}_2 \times \mathbb{F}_2$ (using that $G_{F[\sqrt{a}]} = \overline{\varphi}^{-1}(\ker(s_1))$). Therefore, we see from Proposition 2.3 that the cup product of $t_1 \circ \overline{\varphi}$ and $s_3 \circ \overline{\varphi}$ is zero. This means, in alternative notation, that $(Bb, c)_{F[\sqrt{a}]} = 0$, so $(B,c)_{F[\sqrt{a}]} = 0$.

We now turn to the third assertion. Let α be the cohomology class of the extension

$$0 \longrightarrow \mathbb{F}_2 \longrightarrow \mathbb{U}_5(\mathbb{F}_2) \longrightarrow \overline{\mathbb{U}}_5(\mathbb{F}_2) \longrightarrow 1\,.$$

Let us write down an explicit two-cocycle γ representing α. First, recall the functions $s_1, t_1, \ldots : \mathbb{U}_5(\mathbb{F}_2) \to \mathbb{F}_2$ introduced in §2.1. Multiplying two matrices $g, h \in \mathbb{U}_5(\mathbb{F}_2)$, the top-right coefficient must be $z(g) + z(h) + \gamma(g,h)$, and we deduce

$$\gamma(g,h) = s_1(g)u_2(h) + t_1(g)t_2(h) + u_1(g)s_4(h)\,.$$

To obtain a two-cocycle representing the pull-back $\overline{\varphi}^*(\alpha) \in \mathrm{H}^2(F, \mathbb{F}_2)$, we only need compose with $\overline{\varphi}$. Restricting to the subgroup G_E where $s_1 \circ \overline{\varphi}$ and $s_4 \circ \overline{\varphi}$ both vanish, we obtain that $\overline{\varphi}^*(\alpha)_E$ is represented by the two-cocyle

$$\sigma, \tau \mapsto (t_1 \circ \overline{\varphi}(\sigma))\,(t_2 \circ \overline{\varphi}(\tau))\,.$$

It follows that $\overline{\varphi}^*(\alpha)_E = t_1 \circ \overline{\varphi} \cup t_2 \circ \overline{\varphi}$, the cup-product of the classes $t_i \circ \overline{\varphi} \in \mathrm{H}^1(E, \mathbb{F}_2)$. Or in other words $\overline{\varphi}^*(\alpha)_E = (bB, cC)_E$.

Given that $(B,c)_{F[\sqrt{a}]} = 0$, $(b,C)_{F[\sqrt{d}]} = 0$, and $(b,c)_F = 0$, it follows that $u = \varphi^*(\alpha) \in \mathrm{H}^2(F, \mathbb{F}_2)$ satisfies $u_E = (B,C)_E$.

Finally, suppose that φ exists as in the fourth assertion. We note that $G_E = \varphi^{-1}(\mathscr{C}(S))$ (again the notation $\mathscr{C}(S)$ for the centralizer of S is from §2.4, and we had noted $\mathscr{C}(S) = \ker(s_1) \cap \ker(s_4)$). The composition

$$f \colon G_E \longrightarrow \mathscr{C}(S) \longrightarrow N$$

factors via $\mathscr{C}(S)/S_i$ (for $i = 1, 2, 3$), so from the Lemma 2.5, we must have $f^*(x_2x_3) = 0$, $f^*(x_1x_3) = 0$ and $f^*(x_2x_4) = 0$. But these translate as $(B, C)_E = 0$, which we were after, and $(bB, C)_E = 0$, $(B, cC)_E = 0$, consistently with the above. □

3.2. **Shapiro's lemma and the converse.** Let G be a finite group, let N be a subgroup, and let k be a field. For any kN-module A, we let $\mathrm{Coind}_N^G(A)$ denote $\mathrm{Hom}_N(kG, A)$, which is a (left) kG-module with action $(\sigma \cdot f)(x) = f(x\sigma)$. (We are thinking of G and N as being the groups bearing those names in the discussion above, with $k = \mathbb{F}_2$, and A having trivial action.) The well-known Shapiro's lemma states the existence of an isomorphism

$$sh \colon \mathrm{H}^2(G, \mathrm{Coind}_N^G(A)) \longrightarrow \mathrm{H}^2(N, A)\,.$$

More precisely, the map is obtained using $\mathrm{ev} \colon \mathrm{Coind}_N^G(A) \to A$ which evaluates at $1 \in G$, followed by restriction (in cohomology) to N. Note, if the class $\alpha \in \mathrm{H}^2(G, \mathrm{Coind}_N^G(A))$ describes the extension

$$0 \longrightarrow \mathrm{Coind}_N^G(A) \longrightarrow \Gamma \xrightarrow{p} G \longrightarrow 1\,,$$

then $sh(\alpha)$ corresponds to

$$0 \longrightarrow A \longrightarrow \frac{p^{-1}(N)}{\ker(\mathrm{ev})} \longrightarrow N \longrightarrow 1\,,$$

as is easily verified.

In order to recognize that a given G-module, say S, is isomorphic to $\mathrm{Coind}_N^G(A)$ for some A, let us merely consider the case where $A = k^r$ with trivial N-action, and assume that N is normal in G to boot. Then $\mathrm{Coind}_N^G(A) = (k[G/N]^*)^r$. The dual module $(k[G/N])^*$ is free of rank one, that is, it is isomorphic to $k[G/N]$. (Consider the map taking $1 \in G$ to δ_1, the Dirac delta function at 1. Thus, $\delta_1(N) = 1$ and $\delta_1(g \cdot N) = 0$ if $g \notin N$.) We conclude that S is isomorphic to $\mathrm{Coind}_N^G(k^r)$ if and only if N acts trivially and we can find a basis for S as a free $k[G/N]$ of rank r. If this basis is $\varepsilon_1, \ldots, \varepsilon_r$, then $\ker(ev)$ is the k-vector space spanned by $g\varepsilon_i$, for $g \in G$, $g \neq 1$, $i = 1, \ldots, r$.

For example, let G, N, S recover their concrete meanings as in §2.4 (all the accompanying notation will be used, too). Then Lemma 2.4 asserts that $S \cong \mathrm{Coind}_N^G(\mathbb{F}_2)$, in such a way that $\ker(ev)$ is identified with S_1. As a result, the cohomology class of

$$(*) \qquad 0 \longrightarrow S \longrightarrow \mathbb{U}_5(\mathbb{F}_2) \longrightarrow G \longrightarrow 1$$

corresponds via sh to the cohomology class of the first extension treated in Lemma 2.5, that is, x_2x_3.

But S can be regarded in another way. Consider the subgroup $G' \subset G$ of elements mapping into $\langle \sigma_1\sigma_4 \rangle$ under $G \to G/N$ (equivalently, $g \in G'$ if $s_1(g) = s_4(g)$), and view S as a G'-module. Lemma 2.4 shows that S is a free $\mathbb{F}_2[\langle \sigma_1\sigma_4 \rangle] = \mathbb{F}_2[G'/N]$-module, with basis e_1, e_2 (or alternatively e_1, e_3). Thus we also have $S \cong \mathrm{Coind}_N^{G'}(\mathbb{F}_2 \oplus \mathbb{F}_2)$, and $\ker(ev)$ is spanned by e_3, e_4 (or e_2, e_4 in the alternative). Now the cohomology class of

$$0 \longrightarrow S \longrightarrow \mathbb{U}_5(\mathbb{F}_2)' \longrightarrow G' \longrightarrow 1\,,$$

where $\mathbb{U}_5(\mathbb{F}_2)'$ is the preimage of G', is taken by Shapiro to that of the extension

$$0 \longrightarrow \mathbb{F}_2 e_1 \oplus \mathbb{F}_2 e_2 \longrightarrow \frac{\mathscr{C}(S)}{\langle e_3, e_4 \rangle} \longrightarrow N \longrightarrow 1\,.$$

This extension is described by two classes in $\mathrm{H}^2(N, \mathbb{F}_2)$, corresponding to the exact sequences obtained by factoring out e_1 and e_2 respectively. From Lemma 2.5, these are x_1x_3 and x_2x_3 respectively. With the alternative choice of basis for S, this discussion ends with x_2x_4 and x_2x_3.

There is a well-known version of Shapiro's lemma for profinite groups (cf. [37, Ch. 1 §6]), which can be deduced from the version mentioned above using a straightforward limit argument. We record this version below in the context of Galois cohomology, since we will use it later on.

Lemma 3.2 – *Let E/F be a finite Galois extension, let A be a trivial, discrete G_E-module, and consider $\mathrm{Coind}_{G_E}^{G_F}(A)$, a discrete G_F-module. Then Shapiro's map*

$$\mathrm{H}^2(F, \mathrm{Coind}_{G_E}^{G_F}(A)) \longrightarrow \mathrm{H}^2(E, A)\,,$$

defined as above, is an isomorphism. □

With the preparations above, we can now prove our primary converse to Theorem 3.1.

Theorem 3.3 – *Let F be a field of characteristic not 2, let $a, b, c, d \in F^\times$ be given, and put $E := F[\sqrt{a}, \sqrt{d}]$. Assume that there exist $\widetilde{B} \in F_a$ such that $\mathrm{N}_{F_a/F}(\widetilde{B}) = b$ modulo squares, and $\widetilde{C} \in F_d$ such that $\mathrm{N}_{F_d/F}(\widetilde{C}) = c$ modulo squares, with the following additional property: if B is the image of $\widetilde{B}$ under $F_a \to F[\sqrt{a}]$ and C is the image of $\widetilde{C}$ under $F_d \to F[\sqrt{d}]$, then $(B, C)_E = (B, c)_E = (b, C)_E = (b, c)_E = 0$.*

Then there exist a continuous homomorphism $\varphi : G_F \to \mathbb{U}_5(\mathbb{F}_2)$ such that $s_1 \circ \varphi = \chi_a$, $s_2 \circ \varphi = \chi_b$, $s_3 \circ \varphi = \chi_c$ and $s_4 \circ \varphi = \chi_d$. In other words, the Massey product $\langle a, b, c, d\rangle$ is defined and vanishes.

Proof. We start by assuming that neither a nor d is a square in F (we identify F_a and F_d with $F[\sqrt{a}]$ and $F[\sqrt{d}]$ respectively). From Proposition 2.3 (applied twice), we obtain a homomorphism

$$f\colon G_F \longrightarrow D_4 \times D_4 = G$$

such that $s_i \circ f = \chi_a, \chi_b, \chi_c, \chi_d$ according as $i = 1, 2, 3, 4$, and also $f^*(x_1) = \chi_{bB}$, $f^*(x_2) = \chi_B$, $f^*(x_3) = \chi_C$, $f^*(x_4) = \chi_{cC}$. If $\alpha \in \mathrm{H}^2(D_4 \times D_4, S)$ is the class of the extension

$$0 \longrightarrow S \longrightarrow \mathbb{U}_5(\mathbb{F}_2) \longrightarrow D_4 \times D_4 \longrightarrow 1\,,$$

then its pull-back $f^*(\alpha) \in \mathrm{H}^2(F, S)$ is represented by the fibered-product of $\mathbb{U}_5(\mathbb{F}_2)$ with G_F over $D_4 \times D_4$ (via f). To conclude the proof of the theorem, we will show that one has $f^*(\alpha) = 0$, so that this fibered-product is a split extension of G_F by S. The composition of such a splitting with the projection to $\mathbb{U}_5(\mathbb{F}_2)$ provides the necessary homomorphism φ.

Note that $G_E = f^{-1}(N)$. Suppose first that $[E : F] = 4$. The G_F-module S is isomorphic to $\mathrm{Coind}_{G_E}^{G_F}(\mathbb{F}_2)$, the trivial module of G_E (co)induced to G_F. Shapiro's lemma applies, yielding the isomorphism

$$\mathrm{H}^2(F, S) \longrightarrow \mathrm{H}^2(E, \mathbb{F}_2)\,.$$

From the comments above and the naturality of Shapiro's isomorphism, we see that $f^*(\alpha)$ is taken to $f^*(x_2x_3) = f^*(x_2)f^*(x_3) = (B, C)_E = 0$, so we are done in this case.

We turn to the case where $a = d$ mod squares and $[E : F] = 2$; another way to phrase this is by saying that the image of f lies within G'. Now the G_F-module S is isomorphic, although not canonically, to $\mathrm{Coind}_{G_E}^{G_F}(\mathbb{F}_2 \oplus \mathbb{F}_2)$: we have at least the two possibilities given in the discussion preceding the proof, and for definiteness say we pick the basis e_1, e_2.

Now Shapiro's lemma gives an isomorphism

$$\mathrm{H}^2(F, S) \longrightarrow \mathrm{H}^2(E, \mathbb{F}_2 \oplus \mathbb{F}_2) = \mathrm{H}^2(E, \mathbb{F}_2) \oplus \mathrm{H}^2(E, \mathbb{F}_2)\,.$$

This takes $f^*(\alpha)$ to a pair of cohomology classes, and again from naturality, they are $f^*(x_2x_3) = (B, C)_E$ and $f^*(x_1x_3) = (bB, C)_E$. These are both zero by assumption, and $f^*(\alpha) = 0$ also in this case.

Finally, suppose that a is a square in F (a symmetric argument deals with the case when d is a square). A neat way to handle this is to use the Massey Vanishing Conjecture for $n = 3$, (which is now a theorem, see [23] [10] [29] [30]). First we claim that $(b, c)_F = 0$. Indeed, $(b, c)_E = 0$ by assumption; if d is also a square in F then $E = F$, and otherwise $E = F[\sqrt{d}]$ and $\mathrm{N}_{E/F}(C) = c$ mod squares, so $(b, C)_E = 0$ implies $(b, c)_F = 0$ by the projection formula in group cohomology. We also have $(c, d)_F = 0$ by Proposition 2.3. We deduce that the Massey product $\langle b, c, d\rangle$ vanishes, and so that there is a continuous $\psi\colon G_F \to \mathbb{U}_4(\mathbb{F}_2)$ compatible with b, c, d. However, if we see $\mathbb{U}_4(\mathbb{F}_2)$ as the subgroup of $\mathbb{U}_5(\mathbb{F}_2)$ consisting of those matrices whose first row is that of the identity matrix, we see that we have built $G_F \to \mathbb{U}_5(\mathbb{F}_2)$ compatible with $1, b, c, d$, as required. □

Remark 3.4. It is possible to avoid relying on the Massey Vanishing Conjecture for $n = 3$ if one wishes to do so. Here is a sketch. When d is not a square, use another argument based on Shapiro's lemma, this time replacing G' by G'', the subgroup of G of elements mapping to $\langle \sigma_d\rangle \subset G/N$. When d is a square, define f as in the first part of the proof; this time f takes values in N. The exact sequence

$$0 \longrightarrow S \longrightarrow \mathscr{C}(S) \longrightarrow N \longrightarrow 1$$

is *central*, and controlled by four cohomology classes in $\mathrm{H}^2(N, \mathbb{F}_2)$, pulling back to (B, C), (b, C), (B, c) and (b, c) in $\mathrm{H}^2(F, \mathbb{F}_2)$ under f^*.

The proof of Theorem A is now almost complete. In fact, what we have is this:

Theorem 3.5 – *Let F be a field of characteristic not 2, and let $a, b, c, d \in F^\times$ be given. Then the following statements are equivalent.*

(1) *$\langle a, b, c, d\rangle$ is defined and vanishes.*
(2) *There exist $\widetilde{B} \in F_a$ such that $\mathrm{N}_{F_a/F}(\widetilde{B}) = b$ modulo squares, and $\widetilde{C} \in F_d$ such that $\mathrm{N}_{F_d/F}(\widetilde{C}) = c$ modulo squares, with the following extra property. If B is the image of $\widetilde{B}$ under $F_a \to F[\sqrt{a}]$ and C is the image of $\widetilde{C}$ under $F_d \to F[\sqrt{d}]$, then $(B, C)_{F[\sqrt{a}, \sqrt{d}]} = 0$, $(B, c)_{F[\sqrt{a}]} = 0$, $(b, C)_{F[\sqrt{d}]} = 0$, and $(b, c)_F = 0$.*
(3) *There exist $\widetilde{B} \in F_a$ such that $\mathrm{N}_{F_a/F}(\widetilde{B}) = b$ modulo squares, and $\widetilde{C} \in F_d$ such that $\mathrm{N}_{F_d/F}(\widetilde{C}) = c$ modulo squares, with the following extra property. If B is the image of $\widetilde{B}$ under $F_a \to F[\sqrt{a}]$ and C is the image of $\widetilde{C}$ under $F_d \to F[\sqrt{d}]$, then $(B, C)_E = (B, c)_E = (b, C)_E = (b, c)_E = 0$.*

Proof. Theorem 3.1 shows the implication (1) $\implies$ (2), while (2) $\implies$ (3) is trivial, and Theorem 3.3 shows (3) $\implies$ (1). □

The only difference with Theorem A is the presence of the elements $\widetilde{B}$ and $\widetilde{C}$ instead of just B, C. Clearly, if neither a nor d is a square in F, then the two results are the same. On the other hand, when one of these two elements is a square, in fact when one of a, b, c, d is a square, things become very easy, as we proceed to show in the following subsection.

3.3. **Some trivial cases.**

Lemma 3.6 – *Let F be a field of characteristic different from 2 and let $a, b, c, d \in F^\times$ be given. Suppose that $(a, b)_F = (b, c)_F = (c, d)_F = 0$. Finally, assume that one of a, b, c, d is a square in F. Then the Massey product $\langle a, b, c, d\rangle$ is defined and vanishes.*

Proof. First assume that a is a square, or equivalently $a = 1$. Then the argument given in the last paragraph of the proof of Theorem 3.3 shows that $0 \in \langle a, b, c, d\rangle$. The case when $d = 1$ is treated similarly.

On the other hand, suppose that $b = 1$. From $(c, d)_F = 0$, we draw the existence of $G_F \to \mathbb{U}_3(\mathbb{F}_2)$ compatible with c and d, by Proposition 2.3. The element a itself defines $\chi_a \colon G_F \to \mathbb{F}_2 \cong C_2$. Since the subgroup of $\mathbb{U}_5(\mathbb{F}_2)$ generated by $\sigma_1, \sigma_3, \sigma_4$ is isomorphic to $C_2 \times \mathbb{U}_3(\mathbb{F}_2)$, we see immediately that we may combine our two homomorphisms into one of the form $G_F \to \mathbb{U}_5(\mathbb{F}_2)$, showing that $0 \in \langle a, 1, b, c\rangle$. The case when $c = 1$ is treated similarly. □

Remark 3.7. The above proof, *via* the reference to the proof of Theorem 3.3, uses the Massey Vanishing Conjecture for $n = 3$. Without this, it is still a general fact about Massey products that $\langle a, b, c, d\rangle$ vanishes when it is defined and one of them is a square ([14], Lemma 6.2.4). However, the statement just given is stronger.

We proceed to show how we can improve the statement of Theorem 3.5 to that of Theorem A from the Introduction, so that the two are in fact equivalent. We have already mentioned that this is obvious when neither a nor d is a square in F.

Let us call (1A), (2A), (3A) the conditions of Theorem A, and keep (1), (2), (3) for those of Theorem 3.5, which we know are equivalent. Note (1) = (1A).

Suppose a is a square in F, but not d. Assume condition (1A). We must show that condition (2A) holds. Indeed, from condition (2), we have the element C with $\mathrm{N}_{F[\sqrt{d}]/F}(C) = c$ mod squares, and satisfying $(b, C)_{F[\sqrt{d}]} = 0$, and moreover $(b, c)_F = 0$. Now put $B = b \in F = F[\sqrt{a}]$, so that $\mathrm{N}_{F[\sqrt{a}]/F}(B) = B = b$. Then $(B, C)_E = (b, C)_E = 0$, while $(B, c)_{F[\sqrt{a}]} = (b, c)_F = 0$. We do have condition (2A), and so also (3A).

Conversely, condition (3A) is enough to ensure that $(a, b)_F = (1, b)_F = 0$, $(b, c)_F = 0$ (apply the projection formula to $(b, C)_E = 0$) and $(c, d)_F = 0$ (merely because C exists, cf Proposition 2.3). So the last Lemma applies and shows that condition (1A) holds.

The situation when a is not a square, but d is, is clearly similar.

Now suppose a and d are both squares. Suppose condition (1A) holds, and so also (2), and we have $(a, b) = (c, d) = 0$ (because $\widetilde{B}$ and $\widetilde{C}$ exist, cf remark after Theorem 3.1) and $(b, c) = 0$. Thus condition (2A) holds with $B = b$ and $C = c$, and (2A) = (3A) here. Conversely, condition (3A) contains the statement $(b, c) = 0$, while $(a, b) = (1, b) = 0$ and $(c, d) = (c, 1) = 0$, and we see by the last Lemma that condition (1A) holds. We have therefore just proven Theorem A.

Remark 3.8. Theorem 3.5 is heavier on notation than Theorem A, so we have deemed it unfit for the Introduction. However, the extra case-by-case considerations needed to establish the latter, as just given, are perhaps an indication that it is less natural. (Also, it relies more seriously on the Massey Vanishing Conjecture for $n = 3$, see Remark 3.4.) In the sequel we shall refer to Theorem 3.5, rather than to Theorem A.

3.4. **Maps from profinite groups into $\mathbb{U}_5(\mathbb{F}_2)$.** A routine modification of the arguments given above produces the next result.

Theorem 3.9 – *Let Γ be a profinite group, and let $\chi_1, \chi_2, \chi_3, \chi_4 \in \mathrm{H}^1(\Gamma, \mathbb{F}_2)$ be given. Put $\Gamma_1 := \ker(\chi_1)$, $\Gamma_4 := \ker(\chi_4)$, and $\Gamma_{14} := \Gamma_1 \cap \Gamma_4$. The the following statements are equivalent.*

(1) *There exists a continuous homomorphism $\varphi\colon \Gamma \to \mathbb{U}_5(\mathbb{F}_2)$ such that $\chi_i = s_i \circ \varphi$ for $i = 1, 2, 3, 4$. In other words, $\langle \chi_1, \chi_2, \chi_3, \chi_4 \rangle$ is defined and vanishes.*

(2) *There exist a continuous homomorphism $\Gamma \to D_4$ given by*

$$\gamma \mapsto \begin{pmatrix} 1 & \chi_1(\gamma) & \zeta_1(\gamma) \\ 0 & 1 & \chi_2(\gamma) \\ 0 & 0 & 1 \end{pmatrix},$$

and another one given by

$$\gamma \mapsto \begin{pmatrix} 1 & \chi_3(\gamma) & \zeta_2(\gamma) \\ 0 & 1 & \chi_4(\gamma) \\ 0 & 0 & 1 \end{pmatrix},$$

such that $\zeta_1|_{\Gamma_{14}} \cup \zeta_2|_{\Gamma_{14}} = 0$, $\zeta_1|_{\Gamma_1} \cup \chi_3|_{\Gamma_1} = 0$, $\chi_2|_{\Gamma_4} \cup \zeta_2|_{\Gamma_4} = 0$, $\chi_2 \cup \chi_3 = 0$.

(3) *ζ_1 and ζ_2 exist as above and satisfy $\zeta_1|_{\Gamma_{14}} \cup \zeta_2|_{\Gamma_{14}} = \zeta_1|_{\Gamma_{14}} \cup \chi_3|_{\Gamma_{14}} = \chi_2|_{\Gamma_{14}} \cup \zeta_2|_{\Gamma_{14}} = \chi_2|_{\Gamma_{14}} \cup \chi_3|_{\Gamma_{14}} = 0$.*

We shall have no use for this Theorem in the sequel, so we leave the proof to the reader.

4. First applications

While our main objective in this paper is to prove the 4-Massey Vanishing Conjecture for number fields, there are a few cases which can be treated *over any field*. Usually, we use the following trick when working "by hand". It will have a more theoretical use below, too.

Proposition 4.1 – *Let F be a field of characteristic not 2, and let $a, b, c, d \in F^\times$. Let $\widetilde{B}_0 \in F_a$ be any initial element such that $\mathrm{N}_{F_a/F}(\widetilde{B}_0) = b$, and likewise let $\widetilde{C}_0 \in F_d$ be any initial element such that $\mathrm{N}_{F_d/F}(\widetilde{C}_0) = c$. The following statements are equivalent:*

(1) *There exist $\widetilde{B} \in F_a$ with $\mathrm{N}_{F_a/F}(\widetilde{B}) = bz_1^2$, and $\widetilde{C} \in F_d$ with $\mathrm{N}_{F_d/F}(\widetilde{C}) = cz_2^2$, for some $z_1, z_2 \in F^\times$, such that we have simultaneously $(B, C)_{F[\sqrt{a}, \sqrt{d}]} = 0$, $(B, c)_{F[\sqrt{a}]} = 0$, $(b, C)_{F[\sqrt{d}]} = 0$, $(b, c)_F = 0$, where $B \in F[\sqrt{a}]$ and $C \in F[\sqrt{d}]$ correspond to $\widetilde{B}, \widetilde{C}$ respectively.*

(2) *There exist $\beta, \gamma \in F^\times$ such that $\widetilde{B} = \beta \widetilde{B}_0$ and $\widetilde{C} = \gamma \widetilde{C}_0$ satisfy the previous condition.*

Of course, by Theorem 3.5 these conditions are also equivalent to the vanishing of $\langle a, b, c, d \rangle$, but the point of the Proposition is to show that it makes sense to start with any $\widetilde{B}_0, \widetilde{C}_0$ and then look for the "modifiers" β, γ.

Proof. It is plain that (2) implies (1), so here is the non-trivial part. Assume that $\widetilde{B}, \widetilde{C}$ exist as in the first part. We claim that we can in fact find $\beta, \gamma \in F$ and $\lambda \in F[\sqrt{a}]$, $\mu \in F[\sqrt{d}]$ such that $B = \beta B_0 \lambda^{-2}$ and $C = \gamma C_0 \mu^{-2}$, where $B_0 \in F[\sqrt{a}]$ and $C_0 \in F[\sqrt{d}]$ correspond to $\widetilde{B}_0, \widetilde{C}_0$ respectively. Clearly this will give the result.

To prove the claim, we suppose first that a is not a square in the field F, and write $\mathrm{N}_{F[\sqrt{a}]/F}(Bz_1^{-1}) = b = \mathrm{N}_{F[\sqrt{a}]/F}(B_0)$. Since we have $\mathrm{N}_{F[\sqrt{a}]/F}(Bz_1^{-1}B_0^{-1}) = 1$, by Hilbert 90 we have

$$\frac{Bz_1^{-1}}{B_0} = \frac{\sigma(\lambda)}{\lambda}$$

for some $\lambda \in F[\sqrt{a}]$, where σ is the non-trivial element of $\mathrm{Gal}(F[\sqrt{a}]/F)$. Rewrite this $B = \beta B_0 \lambda^{-2}$, with $\beta = z_1 \lambda \sigma(\lambda) \in F$, and we are done.

If on the other hand a is a square in F, then $B_0, B \in F^\times$, so we may put $\beta = \frac{B}{B_0}$ and $\lambda = 1$.

A similar argument works with C, C_0. □

We give a series of examples. These will demonstrate how, in practice, one looks for β and γ rather than B and C directly. Logically speaking, only the trivial implication of the last Proposition is used, at this point (although knowing that the converse holds gives us confidence in the whole approach).

The elements a and d are always assumed not to be squares in F, so we identify F_a and $F[\sqrt{a}]$, as well as F_d and $F[\sqrt{d}]$, and $\widetilde{B}_0 = B_0$, $\widetilde{C}_0 = C_0$. As you have guessed, the characteristic is always $\neq 2$. We will make some forward references to the results of the next section, which reduce the number of conditions to check.

Example 4.2 (The abaa case) – We show that when $(a,b) = (a,a) = 0$, the Massey product $\langle a,b,a,a\rangle$ is defined and vanishes, under the assumption that $a \neq b$ modulo squares, and that a and b are not squares.

Clearly we can find B_0 and C_0 as in the Proposition, by our assumption (and using Proposition 2.3, of course). We claim that B_0 and C_0 form a basis for $F[\sqrt{a}]$ as an F-vector space. Indeed, if we had $\beta B_0 = \gamma C_0$ for $\beta, \gamma \in F^\times$, then by taking norms to F we would find that $b = a$ modulo squares, a contradiction. Therefore there must exist $\beta, \gamma \in F$ such that

$$\beta B_0 + \gamma C_0 = 1\,.$$

This implies $(\beta B_0, \gamma C_0)_{F[\sqrt{a}]} = 0$. Moreover $(\beta B_0, a)_{F[\sqrt{a}]} = (\beta B_0, 1)_{F[\sqrt{a}]} = 0$. By Lemma 5.5 below, the other cup-products vanish automatically (the reader will also enjoy looking for a direct argument). By Theorem 3.5, the Massey product is defined and vanishes.

Example 4.3 (The aaaa case) – Now we complete the discussion of the previous example, and turn to the case when $a = b$ modulo squares (still assuming that a is not a square). We show that $(a,a) = 0$ implies that $\langle a,a,a,a\rangle$ is defined and vanishes.

Since $(a,a) = 0$, we draw the existence of B_0 with $\mathrm{N}_{F[\sqrt{a}]/F}(B_0) = a$ from Proposition 2.3. It is always true that $(a,-a) = 0$, so we have $(a,-1) = 0$, implying that a is a sum of two squares in F. We invoke the "Norm Principle" from [13]: from the fact that $\mathrm{N}_{F[\sqrt{a}]/F}(B_0)$ is the product of two elements, namely a and 1, which are each the sum of two squares in F, this principle implies that there exists $\beta \in F^\times$ such that $B = \beta B_0$ is the sum of two squares in $F[\sqrt{a}]$. In turn, this means that $(B,-1) = 0$ and so $(B,B) = 0$.

Obviously $(B,a) = (B,1) = 0$ in the cohomology of $F[\sqrt{a}]$ since a is a square there, so Theorem 3.5 applies (with $C = B$).

Example 4.4 (The abad case) – One more example in the same style. We prove that $\langle a,b,a,d\rangle$ is defined and vanishes, under the following assumptions: none of $a,b,d \in F^\times$ is a square, neither is ad, and $(a,b) = (a,d) = 0$.

Pick B_0 such that $\mathrm{N}_{F[\sqrt{a}]/F}(B_0) = b$ and C_0 such that $\mathrm{N}_{F[\sqrt{d}]/F}(C_0) = a$. Put $E = F[\sqrt{a},\sqrt{d}]$. From the fact that $\mathrm{N}_{E/F[\sqrt{a}]}(C/\sqrt{a}) = 1$, we draw *via* Hilbert 90 the existence of $x \in E^\times$ such that $Cx^2 = \mathrm{N}_{E/F[\sqrt{a}]}(x)\sqrt{a}$, and so in particular $Cx^2 \in F[\sqrt{a}]$.

Two cases can occur. First, assume that B_0 and C_0x^2 are linearly independent in $F[\sqrt{a}]$ over F. Then there exist $\beta, \gamma \in F$ such that

$$\beta B_0 + \gamma C_0 x^2 = 1\,.$$

We can see easily that β and γ are both non-zero, for supposing otherwise would lead us to conclude, upon taking norms, that b or a is a square in F. Thus

$$(\beta B_0, \gamma C_0 x^2)_E = (\beta B_0, \gamma C_0)_E = 0\,.$$

Let us check that we can come to the same conclusion if we assume, alternatively, that $B_0 = hC_0x^2$ for some $h \in F^\times$. Indeed, put $\beta = 1$ and $\gamma = -h$ and we do have

$$(\beta B_0, \gamma C_0) = (B_0, -hC_0) = (B_0, -hC_0x^2) = (B_0, -B_0) = 0\,.$$

In either case, if we put $B = \beta B_0$ and $C = \gamma C_0$, then $(B, C)_E = 0$. The other hypotheses required to apply Theorem 3.5 are redundant here, from Lemma 5.2 below (essentially because of the projection formula).

5. Splitting varieties

5.1. **The fundamental equation.** Proposition 2.3 gives a necessary and sufficient condition for a cup-product to vanish in Galois cohomology, in terms of a simple polynomial equation. We shall see that the four cup-products of Theorem 3.5 are likewise controlled by a single polynomial equation, taking place in a certain finite étale F-algebra, namely

$$\mathscr{E} = F[X, Y]/(X^2 - a, Y^2 - d) \cong F_a \otimes_F F_d.$$

More precisely, we establish the following.

Proposition 5.1 – *Let $a, b, c, d \in F^\times$. Let $\widetilde{B} \in F_a \subset \mathscr{E}$ satisfy $\mathrm{N}_{F_a/F}(\widetilde{B}) = bz_1^2$, and let $\widetilde{C} \in F_d \subset \mathscr{E}$ satisfy $\mathrm{N}_{F_d/F}(\widetilde{C}) = cz_2^2$, for some $z_1, z_2 \in F^\times$. Let $B \in F[\sqrt{a}]$ and $C \in F[\sqrt{d}]$ be the corresponding elements. Then the equation*

$$u^2 - \widetilde{B}v^2 = \widetilde{C}$$

has a solution with $u, v \in \mathscr{E}$ if and only if we have simultaneously $(B, C)_{F[\sqrt{a},\sqrt{d}]} = 0$, $(B, c)_{F[\sqrt{a}]} = 0$, $(b, C)_{F[\sqrt{d}]} = 0$, $(b, c)_F = 0$. Alternatively, the same holds with the equation

$$u^2\widetilde{B} + v^2\widetilde{C} = 1\,.$$

The proof will be done in a case-by-case manner (each time getting a slightly more precise statement than that in the Proposition). A quick remark about the equivalence of the two equations, though: it is not a completely general fact, as for example the equation $u^2 + 2v^2 = 1$ has four solutions over $\mathbb{Z}/4\mathbb{Z}$ while $u^2 - v^2 = 2$ has no solution over the same ring. When working over a field of characteristic different from 2 however, the two problems are equivalent, as elementary computations reveal; since $\mathscr{E}$ is a direct sum of such fields, we may indeed use either equation. The second is symmetric in $\widetilde{B}$ and $\widetilde{C}$, and will be used in the sequel, but the proofs in the remainder of this section will be dealing with the first.

In the "generic case" first, that is when a and d are linearly independent in $F^\times/F^{\times 2}$, we can and we do identify $\mathscr{E}$ with $E = F[\sqrt{a}, \sqrt{d}]$. Moreover, we have the following simple situation.

Lemma 5.2 – *Let $\widetilde{B}, B, \widetilde{C}, C$ be as in the Proposition. Suppose that $(B, C)_E = 0$.*

(i) *If neither d nor ad is a square in F, then we have $(B, c)_{F[\sqrt{a}]} = 0$. If neither a nor ad is a square in F, we have $(b, C)_{F[\sqrt{d}]} = 0$.*

(ii) *If $(B, c)_{F[\sqrt{a}]} = 0$ and a is not a square in F, we have $(b, c)_F = 0$. Likewise, if $(b, C)_{F[\sqrt{d}]} = 0$ and d is not a square in F, we also conclude that $(b, c)_F = 0$.*

In particular, when $[E : F] = 4$, the four cup-products from Theorem 3.5 vanish precisely when there are $u, v \in E$ satisfying

$$u^2 - v^2 B = C \, .$$

Proof. If we suppose that a is not a square in F, then $\mathrm{N}_{F[\sqrt{a}]/F}(B) = bz_1^2$; if ad is not a square either, than we can also write $\mathrm{N}_{E/F[\sqrt{d}]}(B) = bz_1^2$. Thus we can use the projection formula from group cohomology, asserting that

$$\mathrm{cores}((B, C)_E) = (b, C)_{F[\sqrt{d}]} \, ,$$

where cores: $\mathrm{H}^2(E, \mathbb{F}_2) \to \mathrm{H}^2(F[\sqrt{d}], \mathbb{F}_2)$ is the corestriction. Thus $(B, C)_E = 0$ does imply $(b, C)_{F[\sqrt{d}]} = 0$. The other case is treated similarly.

One also proves (ii) using the projection formula.

For the last statement, we invoke Proposition 2.3 which states that the proposed equation has a solution if and only if $(B, C)_E = 0$. By the first part, this implies that the other three cup-products also vanish. □

Now suppose that a and d are both squares in F. Then we have four F-homomorphisms $p_i\colon \mathscr{E} \to F$, for $i = 1, 2, 3, 4$, mapping X to $\pm\sqrt{a}$ and Y to $\pm\sqrt{d}$. Together they induce an isomorphism $\mathscr{E} \cong F \times F \times F \times F$, by the Chinese Remainder Theorem. (Note that the map $F \to \mathscr{E}$ which turns $\mathscr{E}$ naturally into an F-algebra is the diagonal embedding of F in F^4, under this isomorphism.)

Lemma 5.3 – *Suppose a and d are both squares in F. Let $\widetilde{B}, B, \widetilde{C}, C$ be as in the Proposition. Then*

$$u^2 - \widetilde{B} v^2 = \widetilde{C}$$

has a solution with $u, v \in \mathscr{E}$ if and only if we have simultaneously $(B, C)_F = (B, c)_F = (b, C)_F = (b, c)_F = 0$.

Proof. Applying p_i with $i = 1, 2, 3, 4$, the equation becomes equivalent to the four equations

$$u_i^2 - p_i(\widetilde{B}) v_i^2 = p_i(\widetilde{C})$$

with unknowns $u_i, v_i \in F$. This is possible if and only if $(p_i(\widetilde{B}), p_i(\widetilde{C})) = 0$ for $i = 1, 2, 3, 4$. (Note that the calculations to follow will establish that $p_i(B) \neq 0$, $p_i(C) \neq 0$ for all i, so that the cup-products make sense.)

We need some notation. Let $B = x + y\sqrt{a}$ and $C = x' + y'\sqrt{d}$, and introduce $B' = x - y\sqrt{a}$ and $C' = x' - y'\sqrt{d}$, so that $BB' = bz_1^2 \neq 0$, and likewise $CC' = cz_2^2 \neq 0$. To fix our ideas, we assume that the numbering of the homomorphisms p_i has been made such that

$$p_1(\widetilde{B}) = p_3(\widetilde{B}) = B \, , \qquad p_2(\widetilde{B}) = p_4(\widetilde{B}) = B' \, ,$$
$$p_1(\widetilde{C}) = p_2(\widetilde{C}) = C \, , \qquad p_3(\widetilde{C}) = p_4(\widetilde{C}) = C' \, .$$

The four cup-products we consider are then (B, C), (B', C), (B, C') and (B', C') for $i = 1, 2, 3, 4$ respectively, all in the cohomology of F. However

$$(b, C) = (BB', C) = (B, C) + (B', C) = 0 \, ,$$

and similarly we draw $(B, c) = 0$ and $(b, c) = 0$. One can also work backwards, clearly. □

When a is a square in F, but d is not, we view $\mathscr{E}$ as $F[\sqrt{d}][X]/(X^2 - a) \cong F[\sqrt{d}] \times F[\sqrt{d}]$ with its two $F[\sqrt{d}]$-homomorphisms $p_1, p_2\colon \mathscr{E} \to F[\sqrt{d}]$. The elements Y and $\sqrt{d}$ are identified. A reasoning similar to the above yields:

LEMMA 5.4 – *Suppose that a is a square in F, and that d is not. Let $\widetilde{B}, B, \widetilde{C}, C$ be as in the Proposition. Then the equation*

$$u^2 - \widetilde{B}v^2 = \widetilde{C}$$

has a solution with $u, v \in \mathscr{E}$ if and only if we have simultaneously $(B, C)_{F[\sqrt{d}]} = (b, C)_{F[\sqrt{d}]} = 0$. When this is the case, we have automatically $(B, c)_F = (b, c)_F = 0$ from Lemma 5.2. □

Of course a similar result holds with the roles of a and d exchanged.

Finally we turn to the case when neither a nor d is a square in F, but ad is. This is in fact similar to the previous case, except that we now have a choice. Namely, we can produce two $F[\sqrt{d}]$-homomorphisms $p_1, p_2 \colon \mathscr{E} \to F[\sqrt{d}]$ giving an isomorphism $\mathscr{E} \cong F[\sqrt{d}] \times F[\sqrt{d}]$, identifying $\sqrt{d}$ with Y all along; or, we can alternatively find two $F[\sqrt{a}]$-homomorphisms $p_1', p_2' \colon \mathscr{E} \to F[\sqrt{a}]$, giving an isomorphism $\mathscr{E} \cong F[\sqrt{a}] \times F[\sqrt{a}]$, identifying X with $\sqrt{a}$ all along. These two isomorphisms are distinct, even if $a = d$. Using one and then the other, we get:

LEMMA 5.5 – *Suppose that neither a nor d is a square in F, but that ad is. Let $\widetilde{B}, B, \widetilde{C}, C$ be as in the Proposition. Then the equation*

$$u^2 - \widetilde{B}v^2 = \widetilde{C}$$

has a solution with $u, v \in \mathscr{E}$ if and only if we have simultaneously $(B, C)_{F[\sqrt{d}]} = (b, C)_{F[\sqrt{d}]} = 0$, if and only if we have simultaneously $(B, C)_{F[\sqrt{a}]} = (B, c)_{F[\sqrt{a}]} = 0$. When this is the case, we have automatically $(b, c)_F = 0$ from Lemma 5.2. □

This concludes the proof of the Proposition. Given that the existence of $\widetilde{B}$ and $\widetilde{C}$ is itself controlled by an simple polynomial equation, as in Proposition 2.3, the situation is now entirely rewritten in terms of the existence of a rational point on an algebraic variety.

5.2. **Splitting varieties.** We proceed to translate our results into the language of algebraic geometry.

As ever, let F be a field of characteristic not 2, let $a, b, c, d \in F^\times$, and put $\mathscr{E} = F[X, Y]/(X^2 - a, Y^2 - d)$. Together, Theorem 3.5, Proposition 2.3 and Proposition 5.1 show that the vanishing of the Massey product $\langle a, b, c, d\rangle$ is equivalent to the existence of a solution to the following system of equations, with unknowns $x_1, y_1, z_1, x_2, y_2, y_3 \in F$, $u, v \in \mathscr{E}$:

(1) $x_1^2 - ay_1^2 = bz_1^2$,
(2) $x_2^2 - dy_2^2 = cz_2^2$,
(3) $u^2\widetilde{B} + v^2\widetilde{C} = 1$, where $\widetilde{B} = x_1 + y_1X \in \mathscr{E}$ and $\widetilde{C} = x_2 + y_2Y \in \mathscr{E}$.

There is also the condition $z_1 \neq 0$, $z_2 \neq 0$. Here $u = u_1 + u_2X + u_3Y + u_4XY$, and likewise for v, so that equation (3) can be written as four equations over F (carrying out the expansion in practice does not seem to clarify things).

For technical reasons, related to Proposition 4.1, we change coordinates and work with the equations:

(i) $x_1^2 - ay_1^2 = b$,
(ii) $x_2^2 - dy_2^2 = c$,
(iii) $u^2\beta\widetilde{B} + v^2\gamma\widetilde{C} = 1$, where $\widetilde{B} = x_1 + y_1X \in \mathscr{E}$ and $\widetilde{C} = x_2 + y_2Y \in \mathscr{E}$.

Here $\beta, \gamma \in F^\times$ are two new unknowns, and z_1, z_2 have disappeared.

Equations (i), (ii), (iii) define an affine subvariety of $\mathbf{A}_F^{14}$, the affine space of dimension 14 over F; we consider its intersection with the open subset defined by $\beta \neq 0$, $\gamma \neq 0$, and call it $\mathscr{X}_F$. Also, note that equation (i) implies that $\widetilde{B}$ is a *unit* of $F_a := F[X]/(X^2 - a)$, and similarly equation (ii) implies that $\widetilde{C}$ is a *unit* of $F_d := F[Y]/(Y^2 - d)$. In particular, we can describe $\mathscr{X}_F$ in a more conceptual way using the Weil-restriction functors $R_{\mathscr{E}|F}$, $R_{F_a|F}$ and $R_{F_d|F}$. Namely, consider the F-variety:

$$\mathscr{Y} := \mathbf{G}_{\mathrm{m}} \times \mathbf{G}_{\mathrm{m}} \times R_{\mathscr{E}/F}\mathbf{A}^2_{\mathscr{E}} \times R_{F_a/F}\mathbf{G}_{\mathrm{m}} \times R_{F_d/F}\mathbf{G}_{\mathrm{m}}\,.$$

We view an F-point of $\mathscr{Y}$ as a tuple $(\beta, \gamma, u, v, \widetilde{B}, \widetilde{C})$, with $\beta, \gamma \in F^\times$, $u, v \in \mathscr{E}$, $\widetilde{B} \in F_a^\times$ and $\widetilde{C} \in F_d^\times$. Then $\mathscr{X}_F$ is the closed subvariety of $\mathscr{Y}$ defined by the three equations:

$$\mathrm{N}_{F_a/F}(\widetilde{B}) = b,\ \mathrm{N}_{F_d/F}(\widetilde{C}) = c,\ u^2\beta\widetilde{B} + v^2\gamma\widetilde{C} = 1\,.$$

We have the following trivial, yet crucial property: for an extension L/F, we have

$$\mathscr{X}_F \times_{\mathrm{Spec}(F)} \mathrm{Spec}(L) = \mathscr{X}_L\,.$$

In particular, we have $\mathscr{X}_F(L) = \mathscr{X}_L(L)$ (using the standard notation for the set of rational points). As already noted, the set $\mathscr{X}_F(F)$ is non-empty if and only if the Massey product $\langle a, b, c, d\rangle$ is defined and vanishes in the cohomology of F. Now, it is obviously also true, but nicer, that for any field extension L/F, the set $\mathscr{X}_F(L)$ is non-empty if and only if the Massey product $\langle a, b, c, d\rangle$ is defined and vanishes in the cohomology of L. This is a property which is expected of a "splitting variety" for the problem of the vanishing of $\langle a, b, c, d\rangle$.

As it turns out, we can introduce a second splitting variety X_F. It will depend on choices, and so is not canonically associated with the problem alone; on the other hand, the local-global principle is established in the Appendix for X_F rather than $\mathscr{X}_F$. The construction will echo Proposition 4.1 rather precisely. Let Z_F be the subvariety of $R_{F_a/F}\mathbf{G}_{\mathrm{m}} \times R_{F_d/F}\mathbf{G}_{\mathrm{m}}$, defined over F be the equations

$$\mathrm{N}_{F_a/F}(\widetilde{B}) = b,\ \mathrm{N}_{F_d/F}(\widetilde{C}) = c\,.$$

There is an obvious morphism $\pi\colon \mathscr{X}_F \to Z_F$ (forgetting β, γ, u, v), and we will define X_F to be a fibre of π above an F-rational point of Z_F. That is, we suppose from now on that $(a, b)_F = (c, d)_F = 0$, and using Proposition 2.3 twice, we select $\widetilde{B}_0 \in F_a$ and $\widetilde{C}_0 \in F_d$ whose norms are b and c respectively; then we put $X_F = \pi^{-1}(\widetilde{B}_0, \widetilde{C}_0)$. The variety X_F is thus defined by the equation

$$u^2\beta\widetilde{B}_0 + v^2\gamma\widetilde{C}_0 = 1\,.$$

Note that our construction of X_F depends on the choice of $\widetilde{B}_0$ and $\widetilde{C}_0$ as above. In the sequel, this choice will always be clear from context, so we omit the $\widetilde{B}_0$, $\widetilde{C}_0$ from the notation.

It is clear that X_F is also compatible with base-change, just like $\mathscr{X}_F$ is. That it is also a splitting variety is part of the next Theorem.

Theorem 5.6 – *Let the notation be as above (in particular, $\widetilde{B}_0$ and $\widetilde{C}_0$ have been chosen). Let L/F be any field extension. The following statements are equivalent.*

(1) *The Massey product $\langle a, b, c, d\rangle$ is defined and vanishes in the cohomology of L.*
(2) *The variety $\mathscr{X}_F$ has an L-rational point.*
(3) *The variety X_F has an L-rational point.*

Moreover, let $\beta, \gamma \in L$. Then there is a rational point $(\beta, \gamma, u, v) \in X_F(L)$ if and only if we have $(\beta B_0, \gamma C_0)_{L[\sqrt{a},\sqrt{d}]} = 0$, $(\beta B_0, c)_{L[\sqrt{a}]} = 0$, $(b, \gamma C_0)_{L[\sqrt{d}]} = 0$ and $(b, c)_L = 0$ simultaneously, where $B_0 \in L[\sqrt{a}]$ corresponds to $\widetilde{B}_0$ under the natural map $F_a \to L[\sqrt{a}]$, and likewise for $C_0 \in L[\sqrt{d}]$.

Proof. Since $\mathscr{X}_F(L) = \mathscr{X}_L(L)$, and similarly for X_F, we may as well (and we do) assume that $L = F$. Then the equivalence is a mere reformulation of earlier material. To wit, Theorem 3.5 together with Proposition 5.1 shows the equivalence of (1) and (2), the variety $\mathscr{X}_F$ being defined just for this purpose. The implication (3) $\implies$ (2) is trivial. On the other hand, Proposition 4.1 gives (2) $\implies$ (3) readily.

The "moreover" statement is obtained by another application of Proposition 5.1. □

Having such a statement dealing with field extensions is necessary for us, as we intend to apply a local-global principle to prove the existence of rational points, and this requires an understanding of $X_F(F_v)$ where F_v is a completion of F.

6. The 4-Massey Vanishing Conjecture for number fields

In this section we finally prove:

Theorem 6.1 – *Let F be a number field, and let $a, b, c, d \in F^\times$ be such that the Massey product $\langle a, b, c, d\rangle$ is defined. Then $\langle a, b, c, d\rangle$ vanishes. In other words, the 4-Massey Vanishing Conjecture is true for number fields.*

Proof. Since the Massey product is defined, we can apply Theorem 3.1, but some simplifying remarks are in order. First, we have $(a, b) = (b, c) = (c, d) = 0$, and so Lemma 3.6 takes care of the case when one of a, b, c, d is a square in F; now we assume that none of them is a square, and in particular, we identify F_a and $F[\sqrt{a}]$, and we identify F_d and $F[\sqrt{d}]$. We do not distinguish between $\widetilde{B}$ and B, or between $\widetilde{C}$ and C, in the notation of Theorem 3.1. A second point is that we may replace once and for all b by bz_1^2 for $z_1 \in F^\times$ if we wish, as the class $\chi_b \in \mathrm{H}^1(F, \mathbb{F}_2)$ is not affected by this, and neither is the Massey product $\langle a, b, c, d\rangle$. Likewise with c.

With these precautions, the result of our application of Theorem 3.1 is this. We can find $B_0 \in F[\sqrt{a}]$ and $C_0 \in F[\sqrt{d}]$ such that $\mathrm{N}_{F\sqrt{a}]/F}(B_0) = b$ and $\mathrm{N}_{F[\sqrt{d}]/F}(C_0) = c$, while $(B_0, c)_{F[\sqrt{a}]} = 0$ and $(b, C_0)_{F[\sqrt{d}]} = 0$. Finally, we can find $u \in \mathrm{H}^2(F, \mathbb{F}_2)$ whose restriction to E is (B_0, C_0).

We select this B_0 and this C_0 in order to construct the splitting variety X_F, and we proceed to prove that $X_F(F)$ is non-empty (by Theorem 5.6, we will then be done). From Theorem A.1, we see that it suffices to show that for each place v of F, we can find a rational point $(\beta_v, \gamma_v, u_v, v_v)$ in $X_F(F_v)$, in such a way that our various choices satisfy

$$\sum_v \mathrm{inv}_v\left((\beta_v, c)_{F_v}\right) = 0\,, \qquad \sum_v \mathrm{inv}_v\left((b, \gamma_v)_{F_v}\right) = 0\,.$$

Here inv_v is the unique isomorphism between $\mathrm{H}^2(F_v, \mathbb{F}_2)$ and $\mathbb{F}_2$. We turn to this, and in fact we shall arrange to have $\mathrm{inv}_v\left((\beta_v, c)_{F_v}\right) = 0$ and $\mathrm{inv}_v\left((b, \gamma_v)_{F_v}\right) = 0$ at each place.

Let v be a place. We see B_0 and C_0, chosen above, as elements of $F_v[\sqrt{a}]$ and $F_v[\sqrt{d}]$ respectively, and we wish rely on the "moreover" statement of Theorem 5.6 with $L = F_v$.

First we treat the case when one of a or d is not a square in the completion F_v: either way, the field $F_v[\sqrt{a}, \sqrt{d}]$ is strictly larger than F_v. However, it is a well-known fact from the theory of local fields that the restriction map $\mathrm{H}^2(F_v, \mathbb{F}_2) \to \mathrm{H}^2(F_v[\sqrt{a}, \sqrt{d}], \mathbb{F}_2)$ is then the zero map. Since $(B_0, C_0)_{F_v[\sqrt{a}, \sqrt{d}]}$ is the image of $u_{F_v} \in \mathrm{H}^2(F_v, \mathbb{F}_2)$ (in the above notation), we have in fact $(B_0, C_0)_{F_v[\sqrt{a}, \sqrt{d}]} = 0$. For such a place, we take $\beta_v = \gamma_v = 1$. The four cup-products in (3) of Theorem 5.6 then vanish, so we have a rational point in $X_F(F_v)$. In this case $(\beta_v, c)_{F_v} = 0$ and $(b, \gamma_v)_{F_v} = 0$, as promised.

Now suppose alternatively that a and d are both squares in F_v. Suppose our element B_0 was of the form $B_0 = x + y\sqrt{a} \in F[\sqrt{a}] \subset F_v$, and let $\beta_v = x - y\sqrt{a} \in F_v$, so that $\beta_v B_0 = b$.

Likewise, write $C_0 = x' + y'\sqrt{d}$ and let $\gamma_v = x' - y'\sqrt{d} \in F_v$, so $\gamma_v C_0 = c$. The four cup-products mentioned in (3) of Theorem 5.6 are equal to $(b, c)_{F_v}$, so they all vanish, and there is an F_v-rational point. Moreover, we have

$$0 = (\beta_v B_0, c)_{F_v} = (\beta_v, c)_{F_v} + (B_0, c)_{F_v} = (\beta_v, c)_{F_v} \,,$$

as $(B_0, c)_{F[\sqrt{a}]} = 0$. Similarly we draw $(b, \gamma_v)_{F_v} = 0$. □

The argument given in this proof establishes, in particular, that fourfold Massey products always vanish in the cohomology of local fields, when they are defined. This was of course known (we quote a strong version of this in the next proof), but here everything stays fairly concrete.

In many cases, we obtain an improved version of the conjecture:

Theorem 6.2 – *Let F be a number field, and let $a, b, c, d \in F^\times$ be given. Suppose that none of ad, ab, cd is a square. Then the following are equivalent:*

(1) *The 4-Massey product $\langle a, b, c, d\rangle$ vanishes.*
(2) *The 4-Massey product $\langle a, b, c, d\rangle$ is defined.*
(3) *One has $(a, b)_F = (b, c)_F = (c, d)_F = 0$.*

Proof. The definitions are so arranged that (1) $\implies$ (2) is a tautology, while (2) $\implies$ (3) is (a very small) part of Theorem 3.1 (and following remark). The non-trivial portion of the proof is (3) $\implies$ (1).

Assume (3). From Theorem 5.6, we must prove that $X_F(F)$ is non-empty. By Theorem A.1 in the Appendix, it suffices to show that for each place v of F, we have $X_F(F_v) \neq \varnothing$. Applying Theorem 5.6 yet again, we now see that we must prove that the Massey product $\langle a, b, c, d\rangle$ is defined and vanishes in the cohomology of F_v. However, for a local field such as F_v, it is known (see [27], Proposition 4.1) that the conditions $(a, b)_{F_v} = (b, c)_{F_v} = (c, d)_{F_v} = 0$ (which hold here by restriction of the analogous identities over F) are enough to imply this. □

Remark 6.3. The implication (3) $\implies$ (1) from Theorem 6.2 fails in general, if one removes the additional assumptions on ad, ab, cd. More precisely, Proposition A.12 and Remark A.14 provide necessary and sufficient conditions for the classes (β, c), (γ, b) and/or $(\beta, c) + (\gamma, b)$, over the function field of X_F, to be unramified over F (see the notation in §5.2). When these conditions hold for one of these classes, a Brauer-Manin obstruction to the implication (3) $\implies$ (1) may arise. See Example A.15, suggested by Y. Harpaz, for a concrete situation where (3) holds, so the variety X_F has local points everywhere, but no F-rational point exists – that is, (1) fails. By Theorem 6.1, (2) also fails to hold. (In this case (β, c) is unramified.) As we see from Theorem 6.2, this cannot happen in *non-degenerate* situations, where $[F(\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d}) : F] = 2^4$.

7. Explicit constructions

Suppose $a, b, c, d \in F^\times$ are linearly independent in $F^\times/F^{\times 2}$. When the Massey product $\langle a, b, c, d\rangle$ vanishes, there is a certain map $\varphi\colon G_F \to \mathbb{U}_5(\mathbb{F}_2)$ which is surjective when composed with $\mathbb{U}_5(\mathbb{F}_2) \to \mathbb{U}_5(\mathbb{F}_2)/\Phi(\mathbb{U}_5(\mathbb{F}_2))$, the quotient modulo the Frattini subgroup, as follows from examining the notation (note that $\Phi(\mathbb{U}_5(\mathbb{F}_2))$ is the intersection of the kernels of the four maps s_i, $i = 1, 2, 3, 4$). If follows that φ is itself surjective, and therefore, there exists an extension L/F such that $\mathrm{Gal}(L/F) \cong \mathbb{U}_5(\mathbb{F}_2)$. The compatibility with a, b, c, d means that $F[\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d}]$ must be contained in L, corresponding to the Frattini quotient via the Galois correspondence.

This section is about constructing L explicitly, under the condition that our usual four cup-products vanish – or equivalently, from Lemma 5.2, under the condition $(B, C)_E = 0$. As it turns out, we end up giving an alternative, more explicit proof for Theorem 3.3, restricted to the “non-degenerate case”.

Theorem 7.1 – *Let F be a field of characteristic $\neq 2$, and let $a, b, c, d \in F^\times$ be elements such that $[a], [b], [c], [d]$ are linearly independent in $F^\times / F^{\times 2}$.*

Assume that we can find $x, y \in F$ such that

$$x^2 - ay^2 = b\,, \tag{1}$$

and likewise assume that we can find $x', y' \in F$ such that

$$(x')^2 - d(y')^2 = c\,. \tag{2}$$

Finally, put $B = x + y\sqrt{a}$ and $C = x' + y'\sqrt{d}$, and assume that we can find $u, v \in F[\sqrt{a}, \sqrt{d}]$ such that

$$u^2 - Bv^2 = C\,. \tag{3}$$

Under these assumptions, if we put $w = u + v\sqrt{B}$, then the Galois closure L of

$$F[\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d}, \sqrt{B}, \sqrt{C}, \sqrt{w}]$$

verifies $\mathrm{Gal}(L/F) \cong \mathbb{U}_5(\mathbb{F}_2)$.

The rest of this section is devoted to the proof. The argument is self-contained, but assumes the notation from §2 and §3, and uses Shapiro’s lemma.

Lemma 7.2 – *Put $K = F[\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d}, \sqrt{B}, \sqrt{C}]$. Then K/F is Galois with*

$$\mathrm{Gal}(K/F) \cong D_4 \times D_4\,.$$

More precisely, the isomorphism can be chosen such that the standard generating involutions $\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in D_4 \times D_4$, when viewed in $\mathrm{Gal}(K/F)$, act on the elements of K as follows:

	$\sqrt{a}$	$\sqrt{b}$	$\sqrt{B}$
σ_1	$-\sqrt{a}$	$\sqrt{b}$	$\star$
σ_2	$\sqrt{a}$	$-\sqrt{b}$	$-\sqrt{B}$
$[\sigma_1, \sigma_2]$	$\sqrt{a}$	$\sqrt{b}$	$-\sqrt{B}$

and

	$\sqrt{d}$	$\sqrt{c}$	$\sqrt{C}$
σ_4	$-\sqrt{d}$	$\sqrt{c}$	$\star$
σ_3	$\sqrt{d}$	$-\sqrt{c}$	$-\sqrt{C}$
$[\sigma_4, \sigma_3]$	$\sqrt{d}$	$\sqrt{c}$	$-\sqrt{C}$

Finally, σ_1 and σ_2 fix $\sqrt{c}, \sqrt{d}, \sqrt{C}$, and vice-versa.

The $\star$ means that we do not insist on a value. One may show, for example, that $\sigma_1(\sqrt{B}) = \pm\frac{\sqrt{b}}{\sqrt{B}}$, but the particular sign will not be relevant.

Proof. Let $K_1 = F[\sqrt{a}, \sqrt{b}, \sqrt{B}]$ and $K_2 = F[\sqrt{c}, \sqrt{d}, \sqrt{C}]$. Then K_i is a D_4-extension of F, for $i = 1, 2$, and the actions are as announced, for some choices of generating involutions for the dihedral groups : simply argue as in the proof of Proposition 2.3.

In order to show that $K = K_1 K_2$ is a $D_4 \times D_4$-extension, it suffices to show that $K_1 \cap K_2 = F$.

The extension of F which corresponds to the Frattini quotient of $\mathrm{Gal}(K_1/F)$ resp. $\mathrm{Gal}(K_2/F)$ is $F[\sqrt{a}, \sqrt{b}]$, resp. $F[\sqrt{c}, \sqrt{d}]$, so $K_1 \neq K_2$. Thus $K_1 \cap K_2$ corresponds to a non-trivial normal subgroup of $\mathrm{Gal}(K_i/F)$, for $i = 1, 2$. Looking at the normal subgroups of D_4, we see that $K_1 \cap K_2 \subset F[\sqrt{a}, \sqrt{b}] \cap F[\sqrt{c}, \sqrt{d}] = F$, which concludes the proof. □

From now on we write G for the group $D_4 \times D_4$, which we have just identified explicitly with $\mathrm{Gal}(K/F)$. As above, we will write N for the subgroup of $\mathrm{Gal}(K/F)$ generated by $\sigma_2, [\sigma_1, \sigma_2], \sigma_3, [\sigma_4, \sigma_3]$.

Lemma 7.3 – *The fixed field of N within K is $E = F[\sqrt{a}, \sqrt{d}]$.* □

Consider now $w = u + v\sqrt{B}$ as above, with $u, v \in F[\sqrt{a}, \sqrt{d}]$, and let us study its class $[w] \in K^\times/K^{\times 2}$. Note that w is clearly non-zero, since $w(u - v\sqrt{B}) = C \neq 0$.

Lemma 7.4 – *The element $[w]$ is fixed by N.*

Proof. The element w is itself fixed by σ_3 and $[\sigma_4, \sigma_3]$, as we see immediately from the tables. On the other hand $\sigma_2(w) = u - v\sqrt{B}$, and things have thus been arranged so that

$$\sigma_2(w) = \frac{w\sigma_2(w)}{w} = \frac{C}{w} = w\left(\frac{\sqrt{C}}{w}\right)^2 .$$

As a result $\sigma_2([w]) = [w]$. The element $[\sigma_1, \sigma_2]$ has the same effect on w as σ_2, so the same argument applies. □

We now let W denote the G-module spanned by $[w]$ within $K^\times/K^{\times 2}$. By the Lemma this can be seen as a G/N-module, and indeed it is the image of

$$\pi \colon \mathbb{F}_2[G/N] \longrightarrow W$$

mapping $1 \in G/N$ to $[w]$. We put $L = K[\sqrt{W}]$, which is indeed the L introduced in the Theorem. Equivariant Kummer theory states that L/F is Galois, and that $\mathrm{Gal}(L/K) \cong W^*$ *via* the Kummer pairing. For future reference, let us recall that $\tau \in \mathrm{Gal}(L/K)$ is viewed as an element of W^* via

$$\tau(w) = \frac{\tau(\sqrt{w})}{\sqrt{w}} \in \{\pm 1\} \cong \mathbb{F}_2 .$$

So we have an exact sequence

$$0 \longrightarrow W^* \longrightarrow \mathrm{Gal}(L/F) \xrightarrow{q} G \longrightarrow 1 ,$$

and we let $\alpha \in \mathrm{H}^2(G, W^*)$ denote the corresponding cohomology class. Consider the following commutative diagram.

$$\begin{tikzcd}
\mathrm{H}^2(G, W^*) \arrow[r, "\pi^*"] \arrow[d, "\widetilde{sh}"'] & \mathrm{H}^2(G, \mathbb{F}_2[G/N]^*) \arrow[d, "sh"] \\
\mathrm{H}^2(N, \frac{W^*}{[w]^\perp}) \arrow[r, "="] & \mathrm{H}^2(N, \mathbb{F}_2) .
\end{tikzcd}$$

Here is a word of explanation about the notation. First, $[w]^\perp = \{f \in W^* : f([w]) = 0\}$. The map sh is Shapiro's isomorphism; the map π^* is the injection which is dual to the surjection $\pi \colon \mathbb{F}_2[G/N] \to W$; the map $\widetilde{sh}$ is Shapiro-like, defined by using the projection $W^* \to \frac{W^*}{[w]^\perp}$ and restriction to N; and the bottom map is seen as the identity, since $\frac{W^*}{[w]^\perp}$ can be identified with $\mathbb{F}_2$ in a unique way (just like any group of order 2). Commutativity is clear.

The cohomology class $\widetilde{sh}(\alpha)$ corresponds to the extension

$$(\dagger) \qquad 0 \longrightarrow \frac{W^*}{[w]^\perp} \longrightarrow \frac{q^{-1}(N)}{[w]^\perp} \longrightarrow N \longrightarrow 1 .$$

Let us elucidate a few things. First we have

$$q^{-1}(N) = \mathrm{Gal}(L/E)\,.$$

Further,

$$\begin{aligned}[w]^\perp &= \{f \in W^* : f([w]) = 0\} \\ &\cong \{\tau \in \mathrm{Gal}(L/K) : \tau(\sqrt{w}) = \sqrt{w}\}\,.\end{aligned}$$

It follows that, if we put $L' = K[\sqrt{w}]$, then $\mathrm{Gal}(L/L') \cong [w]^\perp$, and

$$\frac{q^{-1}(N)}{[w]^\perp} = \mathrm{Gal}(L'/E)\,.$$

Lemma 7.5 – *The Galois group* $\mathrm{Gal}(L'/E)$ *is isomorphic to* $C_2^2 \times D_4$.

Proof. The element $w \in E[\sqrt{B}]$ satisfies $N_{E[\sqrt{B}]/E}(w) = C$, and it follows that

$$M = E[\sqrt{B}, \sqrt{C}, \sqrt{w}]$$

is a D_4-extension of E. (Here we do use the fact that $E[\sqrt{B}, \sqrt{C}]$ is a C_2^2-extension of E, which we know from $\mathrm{Gal}(K/E) = N$.)

Of course K/E is Galois with group $N \cong C_2^4$, so that $L' = KM$ is Galois with group

$$\mathrm{Gal}(KM/E) = \mathrm{Gal}(K/E) \times_{\mathrm{Gal}(K\cap M/E)} \mathrm{Gal}(M/E)\,.$$

Certainly we have $E[\sqrt{B}, \sqrt{C}] \subset K \cap M$, and the intersection $K \cap M$ cannot in fact be larger, for (by counting dimensions, say) if it were we would have $K \cap M = M$; so $M \subset K$, a non-abelian extension contained in an abelian one, contradiction. So $K \cap M = E[\sqrt{B}, \sqrt{C}]$.

Thus $\mathrm{Gal}(L'/E)$ is of the form $C_2^4 \times_{C_2^2} D_4$. Since the map $C_2^4 \to C_2^2$ is split, we see that this fibre product is in fact isomorphic to $C_2^2 \times D_4$. □

From this last Lemma, and its proof, it follows that (†) can be identified with the first exact sequence in Lemma 2.5, which implies that $\widetilde{sh}(\alpha) = x_2x_3$. As a consequence, from the commutativity of the diagram above and the injectivity of Shapiro's map, we see that $\pi^*(\alpha)$ describes the extension

$$0 \longrightarrow S \cong \mathbb{F}_2[G/N]^* \longrightarrow \mathbb{U}_5(\mathbb{F}_2) \longrightarrow G \longrightarrow 1\,.$$

We conclude that $\mathrm{Gal}(L/F)$ is a subgroup of $\mathbb{U}_5(\mathbb{F}_2)$ which maps onto the Frattini quotient $\mathrm{Gal}(F[\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d}]/F)$. Thus $\mathrm{Gal}(L/F) = \mathbb{U}_5(\mathbb{F}_2)$.

Example 7.6 – Let us take $F = \mathbb{Q}$ and $a = 11$, $b = 5$, $c = 79$, $d = 13$. Let us try to look for solutions to (1)-(2)-(3). A little calculation with Hilbert symbols reveals that $(a, b) = (b, c) = (c, d) = 0$, and so Theorem 6.1 guarantees that such solutions do exist.

In practice though, the quickest way to look for $x, y, z \in \mathbb{Q}$ such that

$$x^2 - 11y^2 = 5z^2$$

is to pick random integers y and z until $11y^2 + 5z^2$ is a square. Let us fix an initial solution, say $x_0 = 4$, $y_0 = z_0 = 1$, and put $B_0 = 4 + \sqrt{11}$. Likewise $C_0 = 14 + 3\sqrt{13}$ is an initial solution to equation (2).

With these random values, there will likely be no solution to (3), since $(B_0, C_0) \neq 0$ in general. The next step is to pick random integers $f, g \in \mathbb{Z}$ and check whether $(fB_0, gC_0) = 0$. Again, Proposition 4.1 justifies the existence of these – but there would be no harm in trying even if we did not know that. The most efficient method seems to be to compute the conductor of (fB_0, gC_0), that is, the product of those prime ideals in the ring of integers of $E = \mathbb{Q}[\sqrt{11}, \sqrt{13}]$ such that the cup product (fB_0, gC_0) maps to a non-zero class in the corresponding non-archimedean completion: this is an operation done quickly by the software PARI (which we have used through Sagemath). If the conductor is trivial, we use the more time-consuming methods of PARI to find a rational point on the conic defined by (3).

Having found f, g, we put $B = fB_0$ and $C = gC_0$ (but also in principle $x = fx_0, y = fy_0, z = fz_0$, and so on, thus changing our solutions to (1), (2), although these do not show up themselves in the statement of Theorem 7.1).

In the case at hand, one search of the type just described has yielded the solutions

$$B = \frac{1}{7}\sqrt{11} + \frac{16}{7}\,, \qquad C = \frac{9}{2}\sqrt{13} + \frac{37}{2}$$

which verify $(B, C) = 0$. Indeed, equation (3) is solved by $w = u + v\sqrt{B}$ with

$$\begin{aligned} u = {} & \frac{2}{57319}\sqrt{13}\big(40730430348570235670\sqrt{11} - 28385007947179978688 1\big) \\ & - \frac{64212249821826705848 4}{57319}\sqrt{11} + \frac{14376070991394580931 3}{7396}\,, \\ v = {} & \frac{4}{286595}\sqrt{13}\big(27413052840094197823\sqrt{11} - 19104137033965287353 6\big) \\ & - \frac{17286866674703839900 8}{57319}\sqrt{11} + \frac{19351231516412297413 1}{36980}\,. \end{aligned}$$

Appendix A. Local-global principles and the splitting varieties

by Olivier Wittenberg[1]

The goal of this Appendix is to establish a local-global principle, when F is a number field, for the existence of a rational point on the variety X_F appearing in Theorem 5.6 of the paper (see Theorem A.1 below). I am indebted to the authors for sharing drafts of their paper with me, to Pierre Guillot for numerous discussions on 4-Massey products, and to Yonatan Harpaz for suggesting Example A.15.

A.1. **Statements.** Let F be a field of characteristic zero. For $q, q' \in F$, we set $F_q = F[t]/(t^2 - q)$ and $F_{q,q'} = F[t,t']/(t^2 - q, t'^2 - q')$. Let us fix $a, b, c, d \in F^*$ and $B \in F_a^*$, $C \in F_d^*$ such that $N_{F_a/F}(B) = b$ and $N_{F_d/F}(C) = c$, and consider the closed subvariety

$$X \subset \mathbf{G}_{\mathrm{m}}^2 \times R_{F_{a,d}/F}\mathbf{A}^2_{F_{a,d}}$$

defined by the equation $\beta Bx^2 + \gamma Cy^2 = 1$, where $R_{F_{a,d}/F}$ denotes the Weil restriction functor and β, γ are the coordinates of $\mathbf{G}_{\mathrm{m}}^2$ while x, y are those of $R_{F_{a,d}/F}\mathbf{A}^2_{F_{a,d}}$. (In the body of the paper, this variety is denoted by X_F rather than X, and our B, C play the rôle of the elements called B_0, C_0 there.)

When F is a number field, we denote by Ω the set of its places, by F_v the completion of F at $v \in \Omega$, and by $(x, y) \in \{-1, 1\}$ the Hilbert symbol of $x, y \in F_v^*/F_v^{*2}$ (see [36, Ch. V, §3]).

[1] Département de mathématiques et applications, École normale supérieure, 45 rue d'Ulm, 75230 Paris Cedex 05, France. wittenberg@dma.ens.fr

Theorem A.1 – *Assume that F is a number field. If none of ad, ab, cd is a square in F, then X satisfies the Hasse principle: $X(F) \neq \varnothing$ if and only if $X(F_v) \neq \varnothing$ for all $v \in \Omega$. In any case, the existence of a rational point on X is equivalent to the existence of an element of $\prod_{v\in\Omega} X(F_v)$ whose β and γ coordinates $\beta_v, \gamma_v \in F_v^*$ satisfy*

$$\prod_{v\in\Omega}(\beta_v, c) = \prod_{v\in\Omega}(\gamma_v, b) = 1.$$

In addition, if $X(F) \neq \varnothing$, then $X(F)$ is dense in X for the Zariski topology.

It is not hard to see that X is smooth, irreducible, and geometrically rational. When F is a number field, the existence of a rational point on X is therefore conjectured to be controlled by the Brauer–Manin obstruction (see [3, §4]). To establish Theorem A.1, we shall first deduce the validity of this conjecture, in the case of X, by an application of the fibration method (specifically, of [19, Th. 9.31]). We shall then prove, in Theorem A.2 below, that the unramified Brauer group of X consists of constant classes, except when ad, ab, or cd is a square, in which case the classes of the quaternion algebras (β, c) and (γ, b) over $F(X)$ may come into play. The combination of these two facts yields Theorem A.1. We note that Theorem A.2 is a purely algebraic statement: it holds over an arbitrary field F of characteristic zero.

Theorem A.2 – *The natural map $\mathrm{Br}(F) \to \mathrm{Br}_{\mathrm{nr}}(F(X)/F)$ is surjective if none of ad, ab, cd is a square in F. In any case, its cokernel is killed by 2 and is contained in the subgroup of $\mathrm{Coker}\big(\mathrm{Br}(F) \to \mathrm{Br}(F(X))\big)$ generated by the classes of the quaternion algebras (β, c) and (γ, b) over $F(X)$.*

We recall that the unramified Brauer group $\mathrm{Br}_{\mathrm{nr}}(K/F)$ of a finitely generated field extension K/F is the intersection of the subgroups $\mathrm{Im}\big(\mathrm{Br}(A) \to \mathrm{Br}(K)\big)$ where A ranges over the discrete valuation rings $F \subset A \subset K$ with quotient field K. If F has characteristic zero and $K = F(S)$ for a smooth irreducible variety S, the group $\mathrm{Br}(S) = \mathrm{H}^2_{\text{ét}}(S, \mathbf{G}_\mathrm{m})$ can be identified with the intersection of the subgroups $\mathrm{Im}\big(\mathrm{Br}(\mathscr{O}_{S,\xi}) \to \mathrm{Br}(K)\big)$ where ξ ranges over the codimension 1 points of S; if S is proper, then $\mathrm{Br}(S) = \mathrm{Br}_{\mathrm{nr}}(K/F)$. See [17, III, §6], [5, §5].

Remark A.3. It is only for simplicity that we assume that F has characteristic zero in the statement of Theorem A.2: it allows us to refer to a smooth compactification of X. When F has characteristic $p > 2$, the definition of X still makes sense and Theorem A.2 remains true. Indeed, on the one hand, the proof given below easily adapts to show that the cokernel of $\mathrm{Br}(F) \to \mathrm{Br}_{\mathrm{nr}}(F(X)/F)$ satisfies the desired statement modulo its p-primary torsion subgroup, and on the other hand, this cokernel is killed by a power of 2 since X becomes rational over $F(\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d})$ (see [39, Prop. 1.7]). Presumably, the proof of Theorem A.1 should also work over a global field of characteristic $p > 2$; however, the results we use from [19] have not been written down in this setting.

A.2. **Geometry.** Following [42], we shall say that a scheme of finite type over a field is *split* if it possesses an irreducible component of multiplicity 1 which is geometrically irreducible. In this preliminary section, we compactify X to the total space of a fibration, over a proper base, with very few non-split fibres in codimension 1. This fibration will play a crucial rôle both in the proof of Theorem A.1 and in that of Theorem A.2. We then proceed to make further observations concerning its fibres (Proposition A.4 below), for use in the proof of Theorem A.2.

Let $X'' \subset \mathbf{G}^2_\mathrm{m} \times R_{F_{a,d}/F}\mathbf{P}^2_{F_{a,d}}$ denote the closed subvariety defined by $\beta B x^2 + \gamma C y^2 = z^2$, where β, γ are the coordinates of $\mathbf{G}^2_\mathrm{m}$ and x, y, z now denote the homogeneous coordinates of $R_{F_{a,d}/F}\mathbf{P}^2_{F_{a,d}}$. Clearly X'' is smooth and contains X as a dense open subset. Let us fix once and for all a smooth compactification $X'' \subset X'$ such that the map $\varphi : X'' \to \mathbf{G}^2_{\mathrm{m}}$ defined by $\varphi(\beta, \gamma, [x : y : z]) = (\beta, \gamma)$ extends to a morphism $\varphi' : X' \to \mathbf{P}^1_F \times \mathbf{P}^1_F$. (We view $\mathbf{G}^2_{\mathrm{m}}$ as an open subset of $\mathbf{P}^1_F \times \mathbf{P}^1_F$.) For $w \in F^*$, let $\nu_{\gamma=w}, \nu_{\beta=w\gamma} \in \mathbf{G}^2_{\mathrm{m}}$ denote the generic points of the subvarieties of $\mathbf{G}^2_{\mathrm{m}}$ defined by $\gamma = w$ and by $\beta = w\gamma$, respectively. The next proposition lists sufficient conditions for the fibre of φ (or, equivalently, of φ') above these points to contain a rational point (*i.e.*, an $F(\mathbf{G}_{\mathrm{m}})$-point) for some w.

Proposition A.4 – *The following statements hold:*

(1) *If c is a square in F or if d and ac are squares in F, then there exists $w \in F^*$ such that $\varphi^{-1}(\nu_{\gamma=w})$, $\varphi^{-1}(\nu_{\gamma=aw})$, and $\varphi^{-1}(\nu_{\gamma=dw})$ contain a rational point.*
(2) *If $a = b = c = d$ in F^*/F^{*2}, then there exists $w \in F^*$ such that $\varphi^{-1}(\nu_{\beta=w\gamma})$ and $\varphi^{-1}(\nu_{\beta=aw\gamma})$ contain a rational point.*
(3) *In the case where d and ac are squares in F, one can take $w = C_1$ (or $w = C_2$) in (1), where $C = (C_1, C_2)$ denotes the image of C by the isomorphism $F_d = F \times F$ induced by the choice of a square root of d.*

Proof. We first assume that c is a square in F and prove (1) in this case. As $N_{F_d/F}(C) = c$ is a square in F, it follows from Hilbert's Theorem 90 that there exists $w \in F^*$ such that wC is a square in F_d. Evaluating the function γC at any $\nu \in \{\nu_{\gamma=w}, \nu_{\gamma=aw}, \nu_{\gamma=dw}\}$ yields an element of $F(\nu) \otimes_F F_d$ which becomes a square in $F(\nu) \otimes_F F_{a,d}$, hence the claim.

Let us now assume that d and ac are squares in F, and prove (1) and (3) simultaneously. In this case, following the notation of (3), we have $C_1 C \in F^{*2}_{a,d}$ as c is a square in F_a and as the decomposition $F_{a,d} = F_a \times F_a$ maps $C_1 C$ to (C_1^2, c). Hence, with $w = C_1$, the value of γC at any $\nu \in \{\nu_{\gamma=w}, \nu_{\gamma=aw}, \nu_{\gamma=dw}\}$ is again a square in $F(\nu) \otimes_F F_{a,d}$.

Finally, let us assume that $a = b = c = d$ in F^*/F^{*2} and turn to (2). The choice of a square root of ad determines isomorphisms $\iota : F_d \xrightarrow{\sim} F_a$ and $F_{a,d} = F_a \times F_a$. As $N_{F_a/F}(B\iota(C)) = bc$ is a square in F, Hilbert's Theorem 90 ensures the existence of $w \in F^*$ such that $-wB\iota(C)$ is a square in F_a. As c is a square in F_a, it follows that $-wBC$ is a square in $F_{a,d}$ and hence that the value of the function $-\gamma C\beta B$ at any $\nu \in \{\nu_{\beta=w\gamma}, \nu_{\beta=aw\gamma}\}$ is a square in $F(\nu) \otimes_F F_{a,d}$. Hence, writing $(\beta B, \gamma C)$ for the class in $\mathrm{Br}(F(\nu) \otimes_F F_{a,d})$ of the corresponding quaternion algebra, we have $(\beta B, \gamma C) = (-\gamma C \beta B, \gamma C) = 0$ for any such ν, or equivalently $\varphi^{-1}(\nu)$ possesses a rational point. □

A.3. **Arithmetic.** Let us deduce Theorem A.1 from Theorem A.2. The relevant arithmetic input is the following statement.

Theorem A.5 – *Let Z be a smooth, proper, and irreducible variety over a number field F. Let $n \geq 1$ be an integer and $f : Z \to (\mathbf{P}^1_F)^n$ be a dominant morphism. Assume that the geometric generic fibre of f is rationally connected and that the fibre of f above any codimension 1 point of $(\mathbf{P}^1_F \setminus \{0, \infty\})^n$ is split. Assume, in addition, that for any rational point t of a dense open subset of $(\mathbf{P}^1_F)^n$, the set $Z_t(F)$ is dense in $Z_t(\mathbf{A}_F)^{\mathrm{Br}(Z_t)}$, where $Z_t = f^{-1}(t)$. Then $Z(F)$ is dense in $Z(\mathbf{A}_F)^{\mathrm{Br}(Z)}$.*

For $n = 1$, this is [19, Th. 9.31]. In view of [16, Cor. 1.3], Theorem A.5 for any n follows from the $n = 1$ case by a straightforward induction.

To prove Theorem A.1, we apply Theorem A.5 to φ', with $n = 2$. By our choice of X'', the fibres of φ' above $(\mathbf{P}^1_F \setminus \{0, \infty\})^2$ are Weil restrictions of smooth projective conics. In particular, the geometric generic fibre of φ' is rational, hence rationally connected, and the codimension 1 fibres of φ' above $(\mathbf{P}^1_F \setminus \{0, \infty\})^2$ are smooth and geometrically irreducible, hence split. To verify the arithmetic hypothesis on the closed fibres of φ', we note that if Z_t is a Weil restriction, by a finite extension of number fields, of a smooth projective conic, and if $Z_t(\mathbf{A}_F) \neq \varnothing$, then the Hasse–Minkowski theorem implies that $Z_t(F) \neq \varnothing$, from which it follows that the variety Z_t is rational over F and hence that $Z_t(F)$ is dense in $Z_t(\mathbf{A}_F)$. All in all, we conclude that $X'(F)$ is dense in $X'(\mathbf{A}_F)^{\mathrm{Br}(X')}$. Therefore $X(F) \neq \varnothing$ if and only if $X'(\mathbf{A}_F)^{\mathrm{Br}(X')} \cap \prod_{v\in\Omega} X(F_v) \neq \varnothing$. By Theorem A.2, the latter condition is implied by the one which appears in the statement of Theorem A.1, which, in view of the quadratic reciprocity law, is itself implied by the existence of a rational point on X. Thus the proof of Theorem A.1 is complete.

A.4. **Brauer groups.** In the remainder of this appendix, we prove Theorem A.2. Hereafter F denotes a field of characteristic zero. We start with two general remarks about the Brauer group of Weil restrictions of conics and of trivial 2-dimensional tori.

Proposition A.6 – *Let k'/k be a finite separable extension of fields. Let C be a smooth, projective conic over k'. If $R_{k'/k}C$ denotes the Weil restriction of C from k' to k, the pull-back map $\mathrm{Br}(k) \to \mathrm{Br}(R_{k'/k}C)$ is surjective.*

Proof. Let $\bar{k}$ be a separable closure of k. The choice of a $(k'\otimes_k \bar{k})$-point of C determines an isomorphism between $(R_{k'/k}C)\otimes_k \bar{k}$ and the product of $[k':k]$ copies of $\mathbf{P}^1_{\bar{k}}$ indexed by the finite set $\mathrm{Spec}(k'\otimes_k \bar{k})$. It follows that $\mathrm{Br}((R_{k'/k}C)\otimes_k \bar{k}) = 0$ and that $\mathrm{Pic}((R_{k'/k}C)\otimes_k \bar{k})$ is isomorphic, as a Galois module, to $\mathbf{Z}^{\mathrm{Spec}(k'\otimes_k\bar{k})}$. Hence, by Shapiro's lemma, the terms $E_2^{0,2}$ and $E_2^{1,1}$ of the Hochschild–Serre spectral sequence

$$E_2^{p,q} = \mathrm{H}^p(k, \mathrm{H}^q_{\text{ét}}((R_{k'/k}C)\otimes_k \bar{k}, \mathbf{G}_\mathrm{m})) \Rightarrow \mathrm{H}^{p+q}_{\text{ét}}(R_{k'/k}C, \mathbf{G}_\mathrm{m})$$

vanish (see [24, Ch. III, Prop. 4.9]). We conclude that $E_2^{2,0} = \mathrm{Br}(k)$ surjects onto $\mathrm{H}^2_{\text{ét}}(R_{k'/k}C, \mathbf{G}_\mathrm{m}) = \mathrm{Br}(R_{k'/k}C)$. □

Given a field k of characteristic different from 2 (typically $k = F(\beta,\gamma)$ or $k = F(X)$) and two elements $x, y \in k^*$, we denote by (x,y) the class, in $\mathrm{Br}(k)$, of the corresponding quaternion algebra over k.

Proposition A.7 – *Any 2-torsion element of $\mathrm{Br}((\mathbf{P}^1_F \setminus \{0,\infty\})^2)$ can be written as*

$$(\beta, r) + (\gamma, s) + \varepsilon(\beta,\gamma) + \delta$$

for some $r, s \in F^*$, some $\varepsilon \in \{0,1\}$, and some $\delta \in \mathrm{Im}\Big(\mathrm{Br}(F) \to \mathrm{Br}(F(\beta,\gamma))\Big)$.

Proof. Let $D_1 = \mathbf{A}^1_F \times \{0\}$, $D_2 = \{0\}\times \mathbf{A}^1_F$, $D_{12} = D_1 \cap D_2$, and $D_i^0 = D_i \setminus D_{12}$. By purity for étale cohomology, we have $\mathrm{H}^q_{\text{ét},D_{12}}(\mathbf{A}^2_F, \mathbf{Z}/2\mathbf{Z}) = \mathrm{H}^{q-4}_{\text{ét}}(D_{12}, \mathbf{Z}/2\mathbf{Z}) = \mathrm{H}^{q-4}(F, \mathbf{Z}/2\mathbf{Z})$ for any q, and $\mathrm{H}^3_{\text{ét},D_1^0\cup D_2^0}(\mathbf{A}^2_F \setminus D_{12}, \mathbf{Z}/2\mathbf{Z}) = \mathrm{H}^1_{\text{ét}}(D_1^0, \mathbf{Z}/2\mathbf{Z}) \oplus \mathrm{H}^1_{\text{ét}}(D_2^0, \mathbf{Z}/2\mathbf{Z})$ (see [24, Ch. VI, §5]). The long exact sequence of a triple therefore yields an exact sequence

$$0 \to \mathrm{H}^3_{\text{ét},D_1\cup D_2}(\mathbf{A}^2_F, \mathbf{Z}/2\mathbf{Z}) \to \mathrm{H}^1_{\text{ét}}(D_1^0, \mathbf{Z}/2\mathbf{Z}) \oplus \mathrm{H}^1_{\text{ét}}(D_2^0, \mathbf{Z}/2\mathbf{Z}) \to \mathbf{Z}/2\mathbf{Z},$$

where the rightmost map is the sum of the residues at 0 (*op. cit.*, Ch. III, Rem. 1.26). Finally, let us consider the localisation exact sequence

$$\mathrm{H}^2_{\text{ét}}(\mathbf{A}^2_F, \mathbf{Z}/2\mathbf{Z}) \to \mathrm{H}^2_{\text{ét}}(\mathbf{A}^2_F \setminus (D_1\cup D_2), \mathbf{Z}/2\mathbf{Z}) \to \mathrm{H}^3_{\text{ét},D_1\cup D_2}(\mathbf{A}^2_F, \mathbf{Z}/2\mathbf{Z})$$

(*loc. cit.*, Prop. 1.25). As any 2-torsion element of $\mathrm{Br}((\mathbf{P}^1_F \setminus \{0,\infty\})^2)$ can be lifted to $\mathrm{H}^2_{\text{ét}}(\mathbf{A}^2_F \setminus (D_1\cup D_2), \mathbf{Z}/2\mathbf{Z})$ and as $H^1(D_i^0, \mathbf{Z}/2\mathbf{Z}) \subset H^1(F(D_i), \mathbf{Z}/2\mathbf{Z}) = F(D_i)^*/F(D_i)^{*2}$ is generated by F^*/F^{*2} and by the class of β (resp. γ) if $i=1$ (resp. $i=2$), we deduce from these two exact sequences that for an arbitrary 2-torsion class $\alpha \in \mathrm{Br}((\mathbf{P}^1_F \setminus \{0,\infty\})^2)$, the residues of α at the generic points of D_1 and D_2, viewed as elements of $F(D_i)^*/F(D_i)^{*2}$, are represented by elements of $F(D_i)^*$ of the shape $\beta^\varepsilon s$ and $\gamma^\varepsilon r$, respectively, for some

$r, s \in F^*$ and some $\varepsilon \in \{0,1\}$. The class $(\beta, r) + (\gamma, s) + \varepsilon(\beta, \gamma)$ has the same residues as α at these two points. As $\mathrm{H}^2_{\text{ét}}(\mathbf{A}^2_F, \mathbf{Z}/2\mathbf{Z}) = \mathrm{H}^2(F, \mathbf{Z}/2\mathbf{Z})$ (*op. cit.*, Ch. VI, Cor. 4.20), these two classes differ by a constant class, in view of the localisation exact sequence. □

The following is a simple consequence of Proposition A.6 and Proposition A.7.

Proposition A.8 – *The cokernel of the natural map* $\mathrm{Br}(F) \to \mathrm{Br}_{\mathrm{nr}}(F(X)/F)$ *is killed by* 2. *Its elements are represented by classes of the shape*

$$(\beta, r) + (\gamma, s) + \varepsilon(\beta, \gamma)$$

for $r, s \in F^*$ *and* $\varepsilon \in \{0,1\}$.

Proof. The generic fibre of $\varphi' : X' \to \mathbf{P}^1_F \times \mathbf{P}^1_F$ is a Weil restriction of a smooth projective conic. Applying Proposition A.6 to it, we see that any element of $\mathrm{Br}_{\mathrm{nr}}(F(X)/F) = \mathrm{Br}(X')$ can be written as $\varphi'^*\alpha$ for some $\alpha \in \mathrm{Br}(F(\mathbf{P}^1_F \times \mathbf{P}^1_F))$. As $\varphi'^*\alpha$ is unramified on X' and as the fibres of φ' above $(\mathbf{P}^1_F \setminus \{0, \infty\})^2$ are split, the class α belongs to the subgroup $\mathrm{Br}((\mathbf{P}^1_F \setminus \{0,\infty\})^2) \subset \mathrm{Br}(F(\mathbf{P}^1_F \times \mathbf{P}^1_F))$ (see [6, Prop. 1.1.1]). After adding a constant class to α, we may assume that the value of α at the point $(1,1)$ vanishes in $\mathrm{Br}(F)$. The next lemma then implies that $2\alpha = 0$ (*op. cit.*, Prop. 1.3.3). Applying Proposition A.7 now concludes the proof of Proposition A.8. □

Lemma A.9 – *Let* $i \in \{1,2\}$, $t \in \{0, \infty\}$. *Let* $\xi \in \mathbf{P}^1_F \times \mathbf{P}^1_F$ *be the generic point of the fibre, above* t, *of the* i*th projection* $\mathbf{P}^1_F \times \mathbf{P}^1_F \to \mathbf{P}^1_F$. *The residue of* α *at* ξ *is killed by* 2.

Proof. Let $K = F(\mathbf{P}^1_F \times \mathbf{P}^1_F) = F(\beta, \gamma)$ and $\mathscr{O}_K \subset K$ denote the local ring of $\mathbf{P}^1_F \times \mathbf{P}^1_F$ at ξ. Let K'/K be the quadratic extension obtained by adjoining a square root of β if $i = 1$, or of γ if $i = 2$. Let $\mathscr{O}_{K'}$ denote the integral closure of $\mathscr{O}_K$ in K'. To prove the lemma, it suffices to check that the image of $\alpha \in \mathrm{Br}(K)$ in $\mathrm{Br}(K')$ belongs to the subgroup $\mathrm{Br}(\mathscr{O}_{K'}) \subset \mathrm{Br}(K')$ (see [6, Prop. 1.1.2]). For this, as $\varphi'^*\alpha$ is unramified over X', it suffices to check that the K'-variety $X' \times_{\mathbf{P}^1_F \times \mathbf{P}^1_F} \mathrm{Spec}(K')$ admits a proper regular model over $\mathscr{O}_{K'}$ whose special fibre is split (*loc. cit.*, Prop. 1.1.1; this property does not depend on the choice of the model [42, Cor. 1.2]). A look at the equations which define X'' shows that $X' \times_{\mathbf{P}^1_F \times \mathbf{P}^1_F} \mathrm{Spec}(K')$ even has good reduction over $\mathscr{O}_{K'}$ as it descends to a variety over $F(\gamma) \subset \mathscr{O}_{K'}$ if $i = 1$, or over $F(\beta) \subset \mathscr{O}_{K'}$ if $i = 2$. □

To exploit the hypothesis that the classes under consideration are unramified, we shall repeatedly use the following tool.

Proposition A.10 – *Let* $r, s \in F^*$ *and* $\varepsilon \in \{0,1\}$ *be such that* $(\beta, r) + (\gamma, s) + \varepsilon(\beta, \gamma) \in \mathrm{Br}_{\mathrm{nr}}(F(X)/F)$. *Let* $w \in F^*$.

(1) *If* $\varphi^{-1}(\nu_{\gamma=w})$ *contains a rational point, then* rw^ε *is a square in* F.
(2) *If* $\varphi^{-1}(\nu_{\beta=w\gamma})$ *contains a rational point, then* $rs(-w)^\varepsilon$ *is a square in* F.

Proof. Let $\nu \in \{\nu_{\gamma=w}, \nu_{\beta=w\gamma}\}$. Let $\overline{\nu}$ denote the Zariski closure of ν in $\mathbf{P}^1_F \times \mathbf{P}^1_F$. Suppose that $\varphi^{-1}(\nu)$ contains a rational point. The inclusion $\overline{\nu} \hookrightarrow \mathbf{P}^1_F \times \mathbf{P}^1_F$ then factors through φ'. As $(\beta, r) + (\gamma, s) + \varepsilon(\beta, \gamma) \in \mathrm{Br}((\mathbf{P}^1_F \setminus \{0, \infty\})^2)$ becomes, by assumption, unramified over X' when pulled back to X'', its value at ν must therefore belong to the subgroup $\mathrm{Br}(\overline{\nu}) \subset \mathrm{Br}(\nu)$. Letting t denote the coordinate of $\mathbf{P}^1_F$, this means that when $\nu = \nu_{\gamma=w}$ (resp., $\nu = \nu_{\beta=w\gamma}$), the class $(t, r) + (w, s) + \varepsilon(t, w)$ (resp., $(wt, r) + (t, s) + \varepsilon(wt, t)$) in $\mathrm{Br}(\mathbf{P}^1_F \setminus \{0, \infty\})$ must be unramified over $\mathbf{P}^1_F$; hence the proposition. □

The next three propositions complete the proof of Theorem A.2.

Proposition A.11 – *Let* $r, s \in F^*$. *If the class* $(\beta, r) + (\gamma, s) + (\beta, \gamma) \in \mathrm{Br}(F(X))$ *belongs to* $\mathrm{Br}_{\mathrm{nr}}(F(X)/F)$, *then it belongs to the image of the natural map* $\mathrm{Br}(F) \to \mathrm{Br}(F(X))$.

Proof. We proceed in several steps.

Step 1: we claim that ad is a square in F.

Suppose that ad is not a square in F. Then a and d are not both squares; by symmetry, we may assume that a is not a square in F; after replacing F by $F(\sqrt{d})$, we may then assume that d is a square in F. As a is not a square in F, it cannot be a square in $F(\sqrt{c})$ and in $F(\sqrt{ac})$ at the same time. After replacing F by one of these two extensions, we may therefore assume that c or ac is a square. The hypotheses of Proposition A.4 (1) are now met. By Proposition A.10 (1) applied twice, we deduce that rw and raw are squares in F, hence a is a square in F, which is absurd.

Step 2: we claim that at least one of d and cd is a square in F.

We may assume, after replacing F with $F(\sqrt{c})$, that c is a square in F. Applying Proposition A.4 (1) and Proposition A.10 (1), we deduce that rw and rdw are squares in F; hence d is a square in F.

Step 3: we claim that at least one of a and ab is a square in F.

This follows from Step 2, by symmetry.

Step 4: if $a = b = c = d$ in F^*/F^{*2}, then $a = b = c = d = 1$ in F^*/F^{*2}.

Applying Proposition A.4 (2) and Proposition A.10 (2), we see that $-rsw$ and $-rsaw$ are squares in F, hence a is a square in F.

Putting Steps 1 to 4 together, we have now proved that a and d are squares in F. Let us write $B = (B_1, B_2)$ and $C = (C_1, C_2)$ according to the decompositions $F_a = F \times F$ and $F_d = F \times F$ induced by the choice of square roots of a and d.

Step 5: we claim that $s = B_i$ and $r = C_j$ in F^*/F^{*2} for some $i, j \in \{1, 2\}$.

By symmetry, it suffices to check that $r = C_j$ in F^*/F^{*2} for some $j \in \{1, 2\}$. To this end, as $C_1C_2 = c$, we may replace F with $F(\sqrt{c})$ and assume that c is a square in F. In this case, Proposition A.4 (3) and Proposition A.10 (1) together imply the claim.

As the equality $(\beta B_i, \gamma C_j) = 0$ holds in $\mathrm{Br}(F(X))$ by the very definition of X, Step 5 implies that $(\beta, r) + (\gamma, s) + (\beta, \gamma) = (B_i, C_j)$, which does come from $\mathrm{Br}(F)$. □

Proposition A.12 – *Let $r, s \in F^*$ be such that $(\beta, r) + (\gamma, s) \in \mathrm{Br}_{\mathrm{nr}}(F(X)/F)$. Then at least one of the following holds:*

1. *r and s are squares in F;*
2. *rc and s are squares in F, at least one of a, c, ad, cd is a square in F, and at least one of a, b, c, d, abc is a square in F;*
3. *r and sb are squares in F, at least one of b, d, ad, ab is a square in F, and at least one of a, b, c, d, bcd is a square in F;*
4. *rc and sb are squares in F, at least one of a, c, ad, cd is a square in F, and at least one of b, d, ad, ab is a square in F.*

Proof. Extending the scalars from F to $F(\sqrt{c})$ and applying Proposition A.4 (1) and Proposition A.10 (1) shows that r is a square in $F(\sqrt{c})$, hence at least one of r and rc is a square in F. By symmetry, at least one of s and sb is a square in F. The following two assertions and the symmetric assertions will now imply the proposition:

(i) if rc is a square in F, then at least one of a, c, ad, cd is a square in F;

(ii) if rc and s are squares in F, then at least one of a, b, c, d, abc is a square in F.

To prove (i), we may replace F with $F(\sqrt{ac}, \sqrt{d})$ and assume that ac and d are squares in F. Proposition A.4 (1) and Proposition A.10 (1) then imply that r is a square in F; if rc is a square in F, it follows that c is a square in F, as desired. To prove (ii), we may assume, in view of (i), that ad or cd is a square in F. We may then replace F with $F(\sqrt{ab}, \sqrt{ac})$ and assume that ab and ac are squares in F. In this case, Proposition A.4 (2) and Proposition A.10 (2) imply that c is a square in F. □

Proposition A.13 – *If a or c is a square in F, then $(\beta, c) \in \mathrm{Im}(\mathrm{Br}(F) \to \mathrm{Br}(F(X)))$. If b or d is a square in F, then $(\gamma, b) \in \mathrm{Im}(\mathrm{Br}(F) \to \mathrm{Br}(F(X)))$.*

Proof. By symmetry, we need only check the first assertion. If c is a square, it is trivial. Let us assume that a is a square in F and write $B = (B_1, B_2)$ according to the decomposition $F_a = F \times F$ induced by the choice of a square root of a. The vanishing of the class $(\beta B, \gamma C) \in \mathrm{Br}(F(X) \otimes_F F_{a,d})$, which holds by the very definition of X, is then equivalent to that of the two classes $(\beta B_i, \gamma C) \in \mathrm{Br}(F(X) \otimes_F F_d)$, $i \in \{1, 2\}$. Taking the norm down to $F(X)$ and applying the projection formula, we deduce that $(\beta B_i, c) = 0$ in $\mathrm{Br}(F(X))$ for $i \in \{1, 2\}$. Hence $(\beta, c) = (B_i, c)$, which does come from $\mathrm{Br}(F)$. □

Remark A.14. Proposition A.12 provides necessary conditions for the classes (β, c), (γ, b) and $(\beta, c) + (\gamma, b)$ to belong to $\mathrm{Br}_{\mathrm{nr}}(F(X)/F)$. It is possible to show, although we do not do it here, that these necessary conditions are in fact necessary and sufficient.

Example A.15 – Let $F = \mathbf{Q}$, $a = d = 34$, $b = 2$, $c = 17$, $B = 6 + \sqrt{34}$, $C = (17 + 2\sqrt{34})/3$. It is easy to see that X has points everywhere locally. Using the fact that at every place of $\mathbf{Q}$, at least one of 2, 17, and 34 is a square, one can check that for any place v of $\mathbf{Q}$ other than 17 (resp., for $v = 17$), if $\beta_v \in F_v^*$ denotes the β coordinate of any $\mathbf{Q}_v$-point of X, the Hilbert symbol $(\beta_v, 17)$ is trivial (resp., is nontrivial). Hence $X(\mathbf{Q}) = \varnothing$. Thus, in this case, the three classes $(a, b), (b, c), (c, d) \in \mathrm{Br}(\mathbf{Q})$ vanish, but the Massey product $\langle a, b, c, d\rangle$ is not defined, by Theorem 5.6 and Theorem 6.1. By Theorem 6.2, for such an example to exist, it is necessary that at least one of ad, ab, cd is a square.

References

[1] J. K. Arason. Cohomologische Invarianten quadratischer Formen. *J. Algebra*, 36(3):448–491, 1975.

[2] M. Auslander and O. Goldman. The Brauer group of a commutative ring. *Trans. Amer. Math. Soc.*, 97:367–409, 1960.

[3] J.-L. Colliot-Thélène. L'arithmétique des variétés rationnelles. *Ann. Fac. Sci. Toulouse Math. (6)*, 1(3):295–336, 1992.

[4] J.-L. Colliot-Thélène. Fibre spéciale des hypersurfaces de petit degré. *C. R. Math. Acad. Sci. Paris*, 346(1-2):63–65, 2008.

[5] J.-L. Colliot-Thélène and J.-J. Sansuc. The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group). In *Algebraic groups and homogeneous spaces*, Tata Inst. Fund. Res. Stud. Math., pages 113–186. Tata Inst. Fund. Res., Mumbai, 2007.

[6] J.-L. Colliot-Thélène and P. Swinnerton-Dyer. Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties. *J. reine angew. Math.*, 453:49–112, 1994.

[7] P. Deligne, P. Griffiths, J. Morgan, and D. Sullivan. Real homotopy theory of Kähler manifolds. *Invent. Math.*, 29(3):245–274, 1975.

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

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

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

[11] I. Efrat and E. Matzri. Vanishing of Massey products and Brauer groups. *Canad. Math. Bull.*, 58(4):730–740, 2015.

[12] I. Efrat and J. Mináč. On the descending central sequence of absolute Galois groups. *Amer. J. Math.*, 133(6):1503–1532, 2011.

[13] R. Elman and T. Y. Lam. Quadratic forms under algebraic extensions. *Math. Ann.*, 219(1):21–42, 1976.

[14] R. A. Fenn. *Techniques of geometric topology*, volume 57 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1983.

[15] W. Gao, D. B. Leep, J. Mináč, and T. L. Smith. Galois groups over nonrigid fields. In *Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999)*, volume 33 of *Fields Inst. Commun.*, pages 61–77. Amer. Math. Soc., Providence, RI, 2003.

[16] T. Graber, J. Harris, and J. Starr. Families of rationally connected varieties. *J. Amer. Math. Soc.*, 16(1):57–67, 2003.

[17] A. Grothendieck. Le groupe de Brauer, I, II, III. In *Dix exposés sur la cohomologie des schémas*, pages 46–188. North-Holland, Amsterdam, 1968.

[18] C. Haesemeyer and C. Weibel. Norm varieties and the chain lemma (after Markus Rost). In *Algebraic topology*, volume 4 of *Abel Symp.*, pages 95–130. Springer, Berlin, 2009.

[19] Y. Harpaz and O. Wittenberg. On the fibration method for zero-cycles and rational points. *Ann. of Math. (2)*, 183(1):229–295, 2016.

[20] M. J. Hopkins and K. G. Wickelgren. Splitting varieties for triple Massey products. *J. Pure Appl. Algebra*, 219(5):1304–1319, 2015.

[21] D. C. Isaksen. When is a fourfold Massey product defined? *Proc. Amer. Math. Soc.*, 143(5):2235–2239, 2015.

[22] W. S. Massey. Some higher order cohomology operations. In *Symposium internacional de topología algebraica International symposium on algebraic topology*, pages 145–154. Universidad Nacional Autónoma de México and UNESCO, Mexico City, 1958.

[23] E. Matzri. Triple Massey products in Galois cohomology. *Manuscript.* arXiv:1411.4146.

[24] J. S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series.* Princeton University Press, Princeton, N.J., 1980.

[25] J. Mináč and M. Spira. Witt rings and Galois groups. *Ann. of Math. (2)*, 144(1):35–60, 1996.

[26] J. Mináč and N. D. Tân. Construction of unipotent Galois extensions and Massey products. *Adv. Math.* 304:1021–1054, 2017.

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

[28] J. Mináč and N. D. Tân. The kernel unipotent conjecture and the vanishing of Massey products for odd rigid fields. *Adv. Math.* 273:242–270, 2015.

[29] J. Mináč and N. D. Tân. Triple Massey products and Galois theory. *J. Eur. Math. Soc.* 19(1):255–284, 2017.

[30] J. Mináč and N. D. Tân. Triple Massey products vanish over all fields. *J. London Math. Soc.* 94(3):909–932, 2016.

[31] J. Mináč and N. D. Tân. Triple Massey products over global fields. *Doc. Math.*, 20:1467–1480, 2015.

[32] J. W. Morgan. The algebraic topology of smooth algebraic varieties. *Inst. Hautes Études Sci. Publ. Math.*, (48):137–204, 1978.

[33] J. W. Morgan. Correction to: "The algebraic topology of smooth algebraic varieties" [Inst. Hautes Études Sci. Publ. Math. No. 48 (1978), 137–204; MR0516917 (80e:55020)]. *Inst. Hautes Études Sci. Publ. Math.*, (64):185, 1986.

[34] M. Morishita. On certain analogies between knots and primes. *J. Reine Angew. Math.*, 550:141–167, 2002.

[35] M. Morishita. Milnor invariants and Massey products for prime numbers. *Compos. Math.*, 140(1):69–83, 2004.

[36] J. Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1999.

[37] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, second edition, 2008.

[38] M. Rost. Chain lemma for splitting fields of symbols. *Preprint*, 1998.

[39] D. J. Saltman. The Brauer group and the center of generic matrices. *J. Algebra*, 97(1):53–67, 1985.

[40] J.-P. Serre. *Cohomologie galoisienne*, volume 5 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin, fifth edition, 1994.

[41] R. T. Sharifi. Massey products and ideal class groups. *J. Reine Angew. Math.*, 603:1–33, 2007.

[42] A. N. Skorobogatov. Descent on fibrations over the projective line. *Amer. J. Math.*, 118(5):905–923, 1996.

[43] A. N. Skorobogatov. Descent on toric fibrations. In *Arithmetic and geometry*, volume 420 of *London Math. Soc. Lecture Note Ser.*, pages 422–435. Cambridge Univ. Press, Cambridge, 2015.

[44] D. Sullivan. Infinitesimal computations in topology. *Inst. Hautes Études Sci. Publ. Math.*, (47):269–331 (1978), 1977.

[45] A. Suslin and S. Joukhovitski. Norm varieties. *J. Pure Appl. Algebra*, 206(1-2):245–276, 2006.

[46] J. Tate. Relations between K_2 and Galois cohomology. *Invent. Math.*, 36:257–274, 1976.

[47] V. Voevodsky. On motivic cohomology with $\mathbf{Z}/l$-coefficients. *Ann. of Math. (2)*, 174(1):401–438, 2011.

[48] D. Vogel. On the Galois group of 2-extensions with restricted ramification. *J. Reine Angew. Math.*, 581:117–150, 2005.

[49] C. Weibel. The norm residue isomorphism theorem. *J. Topol.*, 2(2):346–372, 2009.

[50] K. Wickelgren. *Lower central series obstructions to homotopy sections of curves over number fields.* PhD thesis, 2009.

[51] K. Wickelgren. n-nilpotent obstructions to π_1 sections of $\mathbb{P}^1 - \{0, 1, \infty\}$ and Massey products. In *Galois-Teichmüller theory and arithmetic geometry*, volume 63 of *Adv. Stud. Pure Math.*, pages 579–600. Math. Soc. Japan, Tokyo, 2012.

[52] K. Wickelgren. On 3-nilpotent obstructions to π_1 sections for $\mathbb{P}^1_{\mathbb{Q}} - \{0, 1, \infty\}$. In *The arithmetic of fundamental groups—PIA 2010*, volume 2 of *Contrib. Math. Comput. Sci.*, pages 281–328. Springer, Heidelberg, 2012.

Pierre Guillot, Université de Strasbourg & CNRS, Institut de Recherche Mathématique Avancée, UMR 7501, F-67000 Strasbourg, France
E-mail address: guillot@math.unistra.fr

Ján Mináč, Department of Mathematics, Western University, London, Ontario, N6A 5B7, Canada
E-mail address: minac@uwo.ca

Adam Topaz, Mathematical Institute, University of Oxford, Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, United Kingdom
E-mail address: topaz@maths.ox.ac.uk