J. Eur. Math. Soc. 19, 255–284

DOI 10.4171/JEMS/665

Ján Mináč · Nguyễn Duy Tân

Triple Massey products and Galois theory

Dedicated to Hélène Esnault

Received January 12, 2014 and in revised form September 18, 2014

Abstract. We show that any triple Massey product with respect to prime 2 contains 0 whenever it is defined over any field. This extends the theorem of M. J. Hopkins and K. G. Wickelgren, from global fields to any fields. This is the first time when the vanishing of any n-Massey product for some prime p has been established for all fields. This leads to a strong restriction on the shape of relations in the maximal pro-2 quotients of absolute Galois groups, which has been out of reach until now. We also develop an extension of Serre's transgression method to detect triple commutators in relations of pro-p-groups, where we do not require that all cup products vanish. We prove that all n-Massey products, $n \geq 3$, vanish for general Demushkin groups. We formulate and provide evidence for two conjectures related to the structure of absolute Galois groups of fields. In each case when these conjectures can be verified, they have some interesting concrete Galois-theoretic consequences. They are also related to the Bloch–Kato conjecture.

Keywords. Massey products, Galois theory, unipotent representations, Zassenhaus filtration

1. Introduction

A major problem in Galois theory is the characterization of profinite groups which are realizable as absolute Galois groups of fields. This is a difficult problem, and in general little is known. In our paper we provide a definite contribution valid for all fields.

In 1967 A. Weil [Wei] describing Artin's first result in the theory of real fields says "Even now, this is an altogether isolated result of great depth, whose significance for the future is not to be assessed lightly." In the classical papers [AS1, AS2] published in 1927, E. Artin and O. Schreier went on with developing a theory of real fields and showed in particular that the only non-trivial finite subgroups of absolute Galois groups are cyclic groups of order 2. In [Be], E. Becker developed some parts of Artin–Schreier theory by replacing separable closures of fields by maximal p-extensions of fields. Here and below, p is a prime number. The notions of projective profinite fields and pseudo algebraically closed (PAC) fields are now basic notions in Galois theory. (See [FJ, Chapter 11] and also

J. Mináč: Department of Mathematics, Western University, London, Ontario, Canada N6A 5B7; e-mail: minac@uwo.ca

N. D. Tân: Department of Mathematics, Western University, London, Ontario, Canada N6A 5B7, and Institute of Mathematics, Vietnam Academy of Science and Technology,
18 Hoang Quoc Viet, 10307, Hanoi, Vietnam; e-mail: duytan@math.ac.vn

Mathematics Subject Classification (2010): Primary 12G05, 12F10; Secondary 55S30

the definition after Conjecture 1.6 and the beginning of Section 4 below.) In [Ax] it was proved that if a field F is PAC then its absolute Galois group is projective. However the actual name PAC was introduced only later by G. Frey [Frey] following a suggestion of M. Jarden. A nice proof due to D. Haran is presented in [FJ, Theorem 11.6.2]. In fact A. Lubotzky and L. van den Dries [LvdD] proved that for any given projective group G there exists a PAC field whose absolute Galois group is isomorphic to G. See also [FJ, Corollary 23.1.2]. Further, Y. L. Ershov [Er] showed that if finitely many profinite groups are absolute Galois groups, so is their free product. (See also I. Efrat and D. Haran's related result in [EH] concerning pro-p-groups as absolute Galois groups.)

The results above concerning projective groups and free products were generalized in a far-reaching way to "profinite groups that are relatively projective with respect to appropriate subsets of closed subgroups" in [Koe2] and [HJP]. In the remarkable 2001 paper [Koe1], J. Koenigsmann provided a classification of solvable absolute Galois groups. In [MS1] it was shown that orderings of fields can be detected already by much smaller Galois 2-extensions than maximal 2-extensions. In 1996, using Villegas' [Vi] results Mináč and Spira [MS2] provided a structural result on the quotient of absolute Galois groups by the third 2-descending series. These results were extended to analogous results for p-descending series and p-Zassenhaus series in [EM1, EM2]. These are a few fundamental results on the structure of absolute Galois groups of general fields.

In a recent spectacular development, the Bloch–Kato conjecture was proved by M. Rost and V. Voevodsky (see [Voe]). These are very strong restrictions on the structure of absolute Galois groups but these results do not give directly structural results on absolute Galois groups. In [MS2, EM1, EM2], the previous results by A. Merkurjev and A. Suslin [MeSu] on the Bloch–Kato conjecture in degree 2 were used. It is a challenging important problem both for the structure of absolute Galois groups as well as for a better understanding of the Bloch–Kato conjecture, to provide a direct precise translation of the Bloch–Kato conjecture into the group-theoretical properties of absolute Galois groups. Building on the work of a number of mathematicians [Dwy, DGMS, Ef2, GLMS, EM1, EM2, HW, MS2, MeSu, Vi, Voe] we formulate here two other fundamental and strong conjectures which we call the "Vanishing n-Massey Conjecture" and the "Kernel n-Unipotent Conjecture".

The main objective of this paper is to prove the Vanishing 3-Massey Conjecture for prime 2 for all fields and to derive strong consequences for the structure of relations in absolute Galois groups of all fields or their maximal pro-2 quotients. Let us first recall briefly the notion of triple Massey products (see Section 2 for more details). Let $\mathcal{C}^\bullet$ be a differential graded algebra with differential $\partial\colon C^\bullet \to C^{\bullet+1}$ and homology $H^\bullet$. Suppose that $a, b, c \in H^1$ such that $ab = bc = 0$. We can choose A, B, C in $\mathcal{C}^1$ representing a, b, c respectively. Since $ab = 0$, there is E_{ab} such that $\partial E_{ab} = AB$, similarly there is E_{bc} such that $\partial E_{bc} = BC$. Note that $\partial(E_{ab}C + AE_{bc}) = 0$, hence $E_{ab}C + AE_{bc}$ represents an element of H^2. The set of all $E_{ab}C + AE_{bc}$ obtained in this manner is defined to be the *triple Massey product* $\langle a, b, c\rangle \subset H^2$. We say that the triple Massey product *vanishes* if it contains 0.

Now let F be a field of characteristic $\neq 2$ and let $G = G_F(2)$ be the maximal pro-2 quotient of the absolute Galois group G_F of F. Let $\mathcal{C}^\bullet = (\mathcal{C}^\bullet(G, \mathbb{F}_2), \partial)$ denote the differential graded algebra of $\mathbb{F}_2$-inhomogeneous cochains in the continuous group cohomology of G (see the first paragraph in Section 3 for more details). For any $a \in F^* = F \setminus \{0\}$, let χ_a denote the corresponding character via the Kummer map $F^* \to H^1(G, \mathbb{F}_2)$. In the work of M. J. Hopkins and K. G. Wickelgren [HW], the following result was proved.

Theorem 1.1 ([HW, Theorem 1.2]). *Let F be a global field of characteristic $\neq 2$ and $a, b, c \in F^*$. Then the triple Massey product $\langle \chi_a, \chi_b, \chi_c \rangle$ contains 0 whenever it is defined.*

In our paper we show that triple Massey products with respect to prime 2 vanish over any field F. It follows from Example 4.1 and from Witt's Theorem (see [Wi], [Ko2, Theorem 9.1]) that n-fold Massey products vanish with respect to 2 if $\operatorname{char}(F) = 2$. So we can assume that the characteristic of F is not 2.

Theorem 1.2. *Let F be an arbitrary field of characteristic $\neq 2$ and $a, b, c \in F^*$. Then the triple Massey product $\langle \chi_a, \chi_b, \chi_c \rangle$ contains 0 whenever it is defined.*

This has remarkable consequences for the structures of absolute Galois groups G_F and their maximal pro-2 quotients $G_F(2)$. We state our results for finitely generated pro-2-groups but our methods can also be used in the case of infinitely generated pro-2-groups with several relations. In Section 7 we also consider pro-p-groups for p possibly not equal to 2. The reason for our restriction in the remainder of the paper to consider $p = 2$ is that we do not yet have complete results for triple Massey products for $p > 2$. This is work in progress (see [GMTT]). The results on the shape of relations of finitely generated pro-2-groups of the form $G_F(2)$ for some field F are fundamental results extending the classical results of S. P. Demushkin, K. Iwasawa, U. Jannsen, H. Koch, J. Labute, J.-P. Serre, I. Shafarevich and K. Wingberg (see e.g. [De1, De2, I, JaWi, Ko1, Ko2, La, Se1, Sha]). Thus we provide strong restrictions on the structure of groups $G_F(2)$.

Before stating the results we illustrate them with an example. Examining the classification of Demushkin groups by Labute [La] one sees that $G_F(p)$ always has a presentation where the generating relation is a product of commutators between generators and p-powers of generators. (If $G_F(p)$ for a local field is not a Demushkin group, then it is free pro-p.) Already in [CEM, Section 9], it was shown that $G := S/\langle [[x_1, x_2], x_3] \rangle$, where S is a free pro-2-group on generators $x_1, \ldots, x_n$, $n \geq 3$, cannot be the absolute Galois group of any field. (In this paper, for $r \in S$, we denote by $\langle r \rangle$ the closed normal subgroup of S generated by r.) One can also deduce, for example, that G as above cannot be isomorphic to $G_F(2)$ for any field F. However, relations where simple commutators are combined with triple ones like $r = [x_4, x_5][[x_2, x_3], x_1]$ are much harder to exclude, and until this work one has not been able to show that $G = S/\langle r \rangle$, S a free pro-2-group on n generators $x_1, \ldots, x_n$ with $n \geq 5$, is not isomorphic to $G_F(2)$ for any field F. In Examples 7.2 and 7.3, we deal with this group in a detailed way, and in particular we show that $G \not\simeq G_F(2)$ for any field F. Theorems 1.3 and 1.4 below are a vast generalization of this example.

That some conditions are necessary can be seen from the following example. Consider a free pro-2-group S on generators x_1, x_2, x_3 and

$$G = S/\langle r \rangle, \quad r = [x_1, x_3].$$

Now consider three new generators, $y_1 = x_1x_2^{-1}$, $y_2 = x_2$, $y_3 = x_3$ of S. Then

$$\begin{aligned} r &= [y_1y_2, y_3] = [y_1, y_3]\cdot[[y_1, y_3], y_2]\cdot[y_2, y_3] \\ &= [y_1, y_3]\cdot[y_2, y_3]\cdot[[y_1, y_3], y_2]\cdot r', \end{aligned}$$

where r' is an element in the 4th term $S_{(4)}$ in the 2-Zassenhaus filtration of S defined in Section 3 after the proof of Lemma 3.7. Observe now first that the group

$$G_1 = S_1/\langle[x_1, x_3]\rangle,$$

where S_1 is a free pro-2-group on generators x_1, x_3, is realizable as $G_{F_1}(2)$ over the field $\mathbb{C}((X_1))((X_2))$ of iterated power series (see [Wa, Corollary 3.9(2)]). Also $G_2 := S_2$, the free pro-2-group on x_2, is realizable as $G_{F_2}(2)$ where $F_2 = \mathbb{C}((X_2))$. By [JW, Theorem 3.6], we see that their free product in the category of pro-2-groups,

$$G = G_1 * G_2,$$

is also realizable as $G_F(2)$ for some field F. Hence

$$G = S/\langle[y_1, y_3]\cdot[y_2, y_3]\cdot[[y_1, y_3], y_2]\cdot r'\rangle,$$

where S is a free pro-2-group on generators y_1, y_2, y_3, is of the form $G_F(2)$. Hence we see that some conditions as in our Theorems 1.3 and 1.4 are necessary to guarantee the truth of these theorems. Therefore these conditions look like natural conditions. It is clear that they are very strong conditions and they extend some results on the shape of relations of $G_F(2)$ from local fields to all fields.

In the theorems below we use the following notation. Let $(I, <)$ be a well-ordered set. Let S be a free pro-2-group on a set of generators x_i, $i \in I$ (see [NSW, Definition 3.5.14]). Let $S_{(i)}$, $i = 1, 2, \ldots$, be the 2-Zassenhaus filtration of S (see Section 3 for definition). Then any element r in $S_{(2)}$ may be uniquely written as

$$r = \prod_{i\in I} x_i^{2a_i} \prod_{i<j}[x_i, x_j]^{b_{ij}} \prod_{i<j,\, k\le j} [[x_i, x_j], x_k]^{c_{ijk}} r', \tag{1}$$

where $a_i, b_{ij}, c_{ijk} \in \{0, 1\}$ and $r' \in S_{(4)}$. For convenience we call (1) the *canonical decomposition of r modulo $S_{(4)}$* (with respect to the basis (x_i)) and we also set $u_{ij} = b_{ij}$ if $i < j$, and $u_{ij} = b_{ji}$ if $j < i$.

Theorem 1.3. *Let $\mathcal{R}$ be a set of elements in $S_{(2)}$. Assume that there exists an element r in $\mathcal{R}$ and distinct indices i, j, k with $i, k < j$ such that:*

(i) *in the canonical decomposition (1) of r modulo $S_{(4)}$, $a_k = a_j = u_{ij} = u_{kj} = u_{ki} = u_{kl} = u_{jl} = 0$ for all $l \neq i, j, k$, and $c_{ijk} \neq 0$; and*
(ii) *for every $s \in \mathcal{R}$ different from r, the factors $[x_k, x_i]$, $[x_i, x_k]$ and $[x_i, x_j]$ do not occur in the canonical decomposition of s modulo $S_{(4)}$.*

Then $G = S/\langle\mathcal{R}\rangle$ is not realizable as $G_F(2)$ for any field F.

Theorem 1.4. *Let $\mathcal{R}$ be a set of elements in $S_{(2)}$. Assume that there exists an element r in $\mathcal{R}$ and indices $i < j$ such that:*

(i) *in the canonical decomposition (1) of r modulo $S_{(4)}$, $a_i = a_j = u_{ij} = u_{il} = u_{jl} = 0$ for all $l \neq i, j$ and $c_{iji} \neq 0$ (respectively, $c_{ijj} \neq 0$); and*

(ii) *for every $s \in \mathcal{R}$ different from r, the factors $[x_i, x_j]$ and x_i^2 (respectively, $[x_i, x_j]$ and x_j^2) do not occur in the canonical decomposition of s modulo $S_{(4)}$.*

Then $G = S/\langle\mathcal{R}\rangle$ is not realizable as $G_F(2)$ for any field F.

Theorem 1.3 (respectively Theorem 1.4) follows immediately from Theorem 1.2 and Theorem 7.8 (respectively Theorem 7.12).

Remarks 1.5. 1) Notice that any pro-2-group which is realizable as G_F for some field F, is also realizable as $G_F(2)$. Hence the above two theorems also provide pro-2-groups which cannot be realizable as the absolute Galois group of any field F.

2) One can also use Theorems 1.3 and 1.4 to obtain *profinite* groups which are not realizable as the absolute Galois group of any field F. For simplicity we consider only the following example. Let S be a free profinite group on five generators $x_1, \ldots, x_5$ and let $r = [x_4, x_5][[x_2, x_3], x_1]$. Then $G := S/\langle r\rangle$ cannot be realizable as G_F for any field F. In fact, one can check that the pro-2 quotient $G(2)$ of G has a presentation $G(2) = S'/\langle r'\rangle$, where S' is a free pro-2-group on five generators $y_1, \ldots, y_5$ and $r' = [y_4, y_5][[y_2, y_3], y_1]$. By Theorem 1.3, $G(2)$ cannot be of the form $G_F(2)$ for any field F. Therefore G is not realizable as G_F.

Motivated by the theorems above, we formulate the Vanishing n-Massey Conjecture for $n \geq 3$. See Definition 3.3 for the definition of the vanishing n-fold Massey product property.

Conjecture 1.6. *Let p be a prime number and $n \geq 3$ an integer. Let F be a field which contains a primitive pth root of unity if* $\operatorname{char}(F) \neq p$. *Then the absolute Galois group G_F of F has the vanishing n-fold Massey product property with respect to $\mathbb{F}_p$.*

A family of fields which satisfy the Vanishing n-Massey Conjecture for any $n \geq 3$ (and any p) are PAC fields. (Recall that a field F is called PAC if each non-empty variety defined over F has an F-rational point; see [FJ, Chapter 11, p. 192].) This follows from the result, mentioned earlier in the Introduction, that the absolute Galois groups of PAC fields are projective, and from Example 4.2.

In this paper, Theorem 1.2, more precisely Theorem 6.2, shows that Conjecture 1.6 holds true for $n = 3$, $p = 2$ and for any field F. In [MTE], we show that the conjecture is true for any $n \geq 3$, $p > 2$ and for any p-rigid field F. In [MT1], the conjecture is verified for $n = 3$, $p > 2$ and F an algebraic number field. Note also that Theorem 4.3 shows that the conjecture is true for any $n \geq 3$, any prime number p and any local field F. Further results related to Conjecture 1.6 are Propositions 4.5 and 4.6 as well as additional results in [MTE]. In Section 8, we also formulate a related conjecture, the Kernel n-Unipotent Conjecture (Conjecture 8.3).

As will be explained in Section 8, the Kernel n-Unipotent Conjecture evolved over a number of years through work contained in [Vi], [MS2], [GLMS], [EM1], [EM2] and [Ef2]. This conjecture has significant value because it describes specific pro-p-groups which are images of unipotent representations of absolute Galois groups as building blocks of quotients of absolute Galois groups by various terms in their p-Zassenhaus filtrations.

The Vanishing n-Massey Conjecture can be used to construct these building blocks from much smaller p-groups inductively. (See Theorem 3.1, due to B. Dwyer, and our use of it in Section 6.) Thus these two conjectures together provide us with valuable tools for telling us which Galois p-groups we should be able to construct automatically from smaller Galois groups, and how we can proceed to build entire maximal p-extensions of any field. Our paper contributes to the developments of new directions in studies of Galois p-extensions of fields. It complements methods in current research in abelian birational geometry ([BT1], [BT2] and [Pop]).

In retrospect we now understand the initial Artin–Schreier results from this new point of view, and we better appreciate A. Weil's intuition about the significance of these results for future developments in Galois theory (see Remark 4.8).

It seems that our use of triple Massey products for detecting higher commutators is the first time when the rather restrictive assumption that all cup products have to vanish was removed (see e.g. [Ef2, Gä, Mor, Vo1, Vo2]). In fact this suggests that there is a comprehensive extension of the theory described in [Vo2, Appendix] where the assumption on the relations of G contained in a large enough weight of the free group mapping on G can be considerably weakened if $G = G_F(p)$ for some prime p. (Here $G_F(p)$ is the maximal pro-p quotient of the absolute Galois group G_F.) Work on this theory is in progress (see [GMTT]).

In the following discussion, we refer to [DGMS] for definitions of formality of differential graded algebras and the motivation for studying formality, as well as connections with Massey products. (For the notion of differential graded algebras abbreviated as DGAs, see Section 2.) Let $\mathcal{C}^\bullet := \mathcal{C}^\bullet(\mathrm{Spec}\, F, \mathbb{Z}/2) = \mathcal{C}^\bullet(G_F, \mathbb{Z}/2)$ be the DGA of inhomogeneous continuous cochains of G_F with coefficients in $\mathbb{Z}/2$. In [HW], the following extremely interesting question was posed.

Question 1.7 ([HW, Question 1.3]). Is $\mathcal{C}^\bullet(\mathrm{Spec}\, F, \mathbb{Z}/2)$ formal?

It is known that if $\mathcal{C}^\bullet(\mathrm{Spec}\, F, \mathbb{Z}/2)$ is formal, then all higher Massey products vanish. Therefore the vanishing property of Massey products makes the question above a natural one.

The structure of our paper is as follows. In Sections 2 and 3, basic facts on Massey products are reviewed. Some examples on groups satisfying the vanishing Massey product property are discussed in Section 4. In Section 5 we provide the first proof of Theorem 1.2 using splitting varieties [HW]. In Section 6 we present the second proof of Theorem 1.2 using Galois theory and some results of [GLMS]. In Section 7 we apply our results to show some strong restrictions on the shape of relations of $G_F(2)$ for a field F. In the last section we point out certain notions related to our results and possibly interesting directions for further research.

2. Review of Massey products

In this section and the next one, we review some basic facts about Massey products; we use [Dwy], [Ef2], [HW] and [Wic1] as main sources. For other references on Massey products, see e.g. [Fe, Kra, May, Mor, Vo1].

Let A be a unital commutative ring. Recall that a *differential graded algebra* (DGA) over A is a graded A-algebra

$$\mathcal{C}^\bullet = \bigoplus_{k\geq 0} \mathcal{C}^k = \mathcal{C}^0 \oplus \mathcal{C}^1 \oplus \mathcal{C}^2 \oplus \cdots$$

with a product $\cup$ and a differential $\partial\colon \mathcal{C}^\bullet \to \mathcal{C}^{\bullet+1}$ such that

- ∂ is a derivation, i.e.,

$$\partial(a \cup b) = \partial a \cup b + (-1)^k a \cup \partial b \quad (a \in \mathcal{C}^k);$$

- $\partial^2 = 0$.

Then as usual the cohomology is $H^\bullet := \ker\partial/\operatorname{im}\partial$. We shall assume that $a_1,\ldots,a_n$ are elements in H^1.

Definition 2.1. A collection $M = (a_{ij})$, $1 \leq i < j \leq n+1$, $(i,j) \neq (1,n+1)$, of elements of $\mathcal{C}^1$ is called a *defining system* for the *n-fold Massey product* $\langle a_1,\ldots,a_n\rangle$ if the following conditions are fulfilled:

- $a_{i,i+1}$ represents a_i;
- $\partial a_{ij} = \sum_{l=i+1}^{j-1} a_{il} \cup a_{lj}$ for $i+1 < j$.

Then $\sum_{k=2}^{n} a_{1k} \cup a_{k,n+1}$ is a 2-cocycle. Its cohomology class in H^2 is called the *value* of the product relative to the defining system M, and is denoted by $\langle a_1,\ldots,a_n\rangle_M$.

The product $\langle a_1,\ldots,a_n\rangle$ itself is the subset of H^2 consisting of all elements which can be written in the form $\langle a_1,\ldots,a_n\rangle_M$ for some defining system M. The product $\langle a_1,\ldots,a_n\rangle$ is *uniquely defined* if it contains only one element.

When $n = 3$ we will speak about a *triple* Massey product.

For $n \geq 2$ we say that $\mathcal{C}^\bullet$ has the *vanishing n-fold Massey product property* if every defined Massey product $\langle a_1,\ldots,a_n\rangle$, where $a_1,\ldots,a_n \in \mathcal{C}^1$, necessarily contains 0.

Remark 2.2. Let $a_1,\ldots,a_n \in H^1$. Suppose that $M = (a_{ij})$, $1 \leq i < j \leq n+1$ and $(i,j) \neq (1,n+1)$, is a defining system for $\langle a_1,\ldots,a_n\rangle$. It is straightforward to see that

$$\langle a_1,\ldots,a_n\rangle_M + a_1 \cup H^1 + H^1 \cup a_n \subset \langle a_1,\ldots,a_n\rangle.$$

And if $n = 3$ then

$$\langle a_1,a_2,a_3\rangle_M + a_1 \cup H^1 + H^1 \cup a_3 = \langle a_1,a_2,a_3\rangle.$$

In particular, $\langle a_1,a_2,a_3\rangle$ is uniquely defined if and only if $a_1 \cup H^1 = H^1 \cup a_3 = 0$.

3. Massey products and unipotent representations

Let G be a profinite group and let A be a finite commutative ring considered as a trivial discrete G-module. The complex $\mathcal{C}^\bullet = (\mathcal{C}^\bullet(G, A), \partial)$ of inhomogeneous continuous cochains of G with coefficients in A is a DGA with the cup product [NSW, Ch. I, §2 and Proposition 1.4.1]. (Technically [NSW, Proposition 1.4.1] deals with homogeneous continuous cochains. However, it is straightforward to see, using this proposition and the relationship between homogeneous and inhomogeneous continuous cochains in [NSW, Ch. I, §2], that this proposition is also true for inhomogeneous continuous cochains.) We write $H^i(G, A)$ for the corresponding cohomology groups. As observed by Dwyer [Dwy] in the discrete context (see also [Ef2, §8] in the profinite case), defining systems for this DGA can be interpreted in terms of upper-triangular unipotent representations of G, as follows.

Let $n \geq 3$ be an integer. Let $\mathbb{U}_{n+1}(A)$ be the group of all upper-triangular unipotent $(n+1) \times (n+1)$-matrices with entries in A. Let $Z_{n+1}(A)$ be the subgroup of all such matrices with all off-diagonal entries being 0 except at position $(1, n+1)$. This group is the center of $\mathbb{U}_{n+1}(A)$. We may identify $\mathbb{U}_{n+1}(A)/Z_{n+1}(A)$ with the group $\bar{\mathbb{U}}_{n+1}(A)$ of all upper-triangular unipotent $(n+1) \times (n+1)$-matrices with entries over A with the $(1, n+1)$-entry omitted, i.e. replaced by a blank space.

For a representation $\rho\colon G \to \mathbb{U}_{n+1}(A)$ and $1 \leq i < j \leq n+1$ let $\rho_{ij}\colon G \to A$ be the composition of ρ with the projection from $\mathbb{U}_{n+1}(A)$ to its (i, j)-coordinate. We use similar notation for representations $\bar\rho\colon G \to \bar{\mathbb{U}}_{n+1}(A)$. Note that $\rho_{i,i+1}$ (resp., $\bar\rho_{i,i+1}$) is a group homomorphism.

Theorem 3.1 ([Dwy, Theorem 2.4]). *Let $\alpha_1, \dots, \alpha_n \in H^1(G, A)$. There is a one-one correspondence $M \leftrightarrow \bar\rho_M$ between defining systems M for $\langle \alpha_1, \dots, \alpha_n \rangle$ and group homomorphisms $\bar\rho_M\colon G \to \bar{\mathbb{U}}_{n+1}(A)$ with $(\bar\rho_M)_{i,i+1} = -\alpha_i$ for $1 \leq i \leq n$.*

Moreover $\langle \alpha_1, \dots, \alpha_n \rangle_M = 0$ in $H^2(G, A)$ if and only if the dotted arrow exists in the commutative diagram

$$\begin{tikzcd}
 & & & G \arrow[dl, dashed] \arrow[d, "\bar\rho_M"] & \\
0 \arrow[r] & A \arrow[r] & \mathbb{U}_{n+1}(A) \arrow[r] & \bar{\mathbb{U}}_{n+1}(A) \arrow[r] & 1
\end{tikzcd}$$

Explicitly, for a defining system $M = (a_{ij})$ for $\langle \alpha_1, \dots, \alpha_n \rangle$, $\bar\rho_M\colon G \to \bar{\mathbb{U}}_{n+1}(A)$ is given by letting $(\bar\rho_M)_{ij} = -a_{ij}$.

Remark 3.2. Let $G(p)$ be the maximal pro-p quotient of G. Then the natural map

$$\pi^*\colon H^1(G(p), \mathbb{F}_p) \to H^1(G, \mathbb{F}_p),$$

induced from the quotient map $\pi\colon G \to G(p)$, is an isomorphism. Let $\alpha_1, \dots, \alpha_n \in H^1(G(p), \mathbb{F}_p)$. Then the following are equivalent:

- $\langle \alpha_1, \dots, \alpha_n \rangle$ is defined and contains 0 in $H^2(G(p), \mathbb{F}_p)$.
- $\langle \pi^*(\alpha_1), \dots, \pi^*(\alpha_n) \rangle$ is defined and contains 0 in $H^2(G, \mathbb{F}_p)$.

This follows from Theorem 3.1 and from the fact that $\mathbb{U}_{n+1}(\mathbb{F}_p)$ and $\bar{\mathbb{U}}_{n+1}(\mathbb{F}_p)$ are (finite) p-groups.

Definition 3.3. Let the notation be as above. We say that G has the *vanishing n-fold Massey product property* (*with respect to* A) if the DGA $\mathcal{C}^\bullet(G, A)$ has the vanishing n-fold Massey product property.

Corollary 3.4. *Let $n \geq 3$ be an integer. The following conditions are equivalent:*

(i) *G has the vanishing n-fold Massey product property with respect to A.*
(ii) *For every representation $\bar{\rho}\colon G \to \bar{\mathbb{U}}_{n+1}(A)$, there is a representation $\rho\colon G \to \mathbb{U}_{n+1}(A)$ such that $\rho_{i,i+1} = \bar{\rho}_{i,i+1}$ for $i = 1, \dots, n$.*

Corollary 3.5. *Let $n \geq 3$ be an integer. Let $G(p)$ be the maximal pro-p quotient of G and assume that $A = \mathbb{F}_p$. Then the following conditions are equivalent:*

(i) *G has the vanishing n-fold Massey product property with respect to $\mathbb{F}_p$.*
(ii) *$G(p)$ has the vanishing n-fold Massey product property with respect to $\mathbb{F}_p$.*

Proposition 3.6 ([Dwy, p. 182, Remark], see also [Ef2, Proposition 8.3]). *Let $\bar{\rho}_M\colon G \to \bar{\mathbb{U}}_{n+1}(A)$ correspond to a defining system $M = (c_{ij})$ for $\langle \alpha_1, \dots, \alpha_n \rangle$ as in Theorem 3.1. Then the central extension associated with $\langle \alpha_1, \dots, \alpha_n \rangle_M$ is the pullback*

$$0 \to A \to \mathbb{U}_{n+1}(A) \times_{\bar{\mathbb{U}}_{n+1}(A)} G \to G \to 1$$

via $\bar{\rho}_M\colon G \to \bar{\mathbb{U}}_{n+1}(A)$ of the extension

$$0 \to A \to \mathbb{U}_{n+1}(A) \to \bar{\mathbb{U}}_{n+1}(A) \to 1.$$

Now assume that $G = S/R$ is the quotient of some profinite group S by some normal subgroup R. Then we have the transgression map [NSW, Chapter I, Proposition 1.6.6]

$$\mathrm{trg}\colon H^1(R, A)^G \to H^2(G, A).$$

Let $\bar{\rho}\colon G \to \bar{\mathbb{U}}_{n+1}(A)$ be a representation of G and let $\langle -\bar{\rho}_{12}, \dots, -\bar{\rho}_{n,n+1} \rangle_{\bar{\rho}}$ be the n-fold Massey product value relative to the defining system corresponding to $\bar{\rho}$. Suppose that $\rho\colon S \to \mathbb{U}_{n+1}(A)$ is a *lift* of $\bar{\rho}$, i.e., ρ is a homomorphism such that the diagram

$$\begin{tikzcd}
S \arrow[r] \arrow[d, "\rho"] & G \arrow[r] \arrow[d, "\bar{\rho}"] & 1 \\
\mathbb{U}_{n+1}(A) \arrow[r] & \bar{\mathbb{U}}_{n+1}(A) \arrow[r] & 1
\end{tikzcd}$$

commutes. We can define (see [Sh, p. 8]) $\Lambda(\rho) \in H^1(R, A)^G$ by

$$\Lambda(\rho)(\tau) = -\rho_{1,n+1}(\tau)$$

for $\tau \in R$. Then by the same argument as in [Sh, Lemma 2.3] and by Proposition 3.6, we obtain the following result. We include a proof for the convenience of the reader.

Lemma 3.7. *We have* $\mathrm{trg}(\Lambda(\rho)) = \langle -\bar{\rho}_{12}, \dots, -\bar{\rho}_{n,n+1}\rangle_{\bar{\rho}}$.

Proof. We consider the diagram

$$\begin{tikzcd}
1 \arrow[r] & R \arrow[r] \arrow[d, "-\Lambda(\rho)"] & S \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, equal] & 1 \\
0 \arrow[r] & A \arrow[r] \arrow[d, equal] & \mathcal{E} \arrow[r] \arrow[d, dashed] & G \arrow[r] \arrow[d, equal] & 1 \\
0 \arrow[r] & A \arrow[r] \arrow[d, equal] & \mathbb{U}_{n+1}(A) \times_{\bar{\mathbb{U}}_{n+1}(A)} G \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, "\bar{\rho}"'] & 1 \\
0 \arrow[r] & A \arrow[r] & \mathbb{U}_{n+1}(A) \arrow[r] & \bar{\mathbb{U}}_{n+1}(A) \arrow[r] & 1
\end{tikzcd}$$

and we read the diagram from top to bottom. Here the second exact sequence is the pushout of the first exact sequence via $\Lambda(\rho)\colon R \to A$. Then its equivalence class as an element in $H^2(G, A)$ is $\mathrm{trg}(\Lambda(\rho))$.

On the other hand, by Proposition 3.6 the equivalence class of the third central extension in $H^2(G, A)$ is $\langle -\bar{\rho}_{12}, \dots, -\bar{\rho}_{n,n+1}\rangle_{\bar{\rho}}$. In order to prove the lemma, we only need to prove that there exists a dashed arrow $\mathcal{E} \dashrightarrow \mathbb{U}_{n+1}(A) \times_{\bar{\mathbb{U}}_{n+1}(A)} G$ making the above diagram commute. But this follows from the universal properties of the pullback $\mathbb{U}_{n+1}(A) \times_{\bar{\mathbb{U}}_{n+1}(A)} G$ and the pushout $\mathcal{E}$. □

Now let $A = \mathbb{F}_p$, with p a prime number. As shown for example in [Ef2, Gä, Mor, Vo1], Massey products in $\mathcal{C}^\bullet(G, \mathbb{F}_p)$ are also intimately related to the *p-Zassenhaus filtration* $G_{(n)}$, $n = 1, 2, \dots,$ of G. Recall that this filtration is defined inductively by

$$G_{(1)} = G, \quad G_{(n)} = G^p_{(\lceil n/p \rceil)} \prod_{i+j=n} [G_{(i)}, G_{(j)}],$$

where $\lceil n/p \rceil$ is the least integer which is greater than or equal to n/p.

Lemma 3.8. *Let G be a profinite group.*

1. *Every (continuous) homomorphism $\rho\colon G \to \mathbb{U}_{n+1}(\mathbb{F}_p)$ is trivial on $G_{(n+1)}$.*
2. *Every (continuous) homomorphism $\rho\colon G \to \bar{\mathbb{U}}_{n+1}(\mathbb{F}_p)$ is trivial on $G_{(n+1)}$.*

Proof. These follow from the fact that $\mathbb{U}_{n+1}(\mathbb{F}_p)_{(n+1)} = 1$. □

Lemma 3.9. *The profinite group G has the vanishing n-fold Massey product property with respect to $\mathbb{F}_p$ if and only if $G/G_{(n+1)}$ has this property.*

Proof. This follows from Corollary 3.4 and Lemma 3.8. □

Proposition 3.10. *Let N, N' be closed normal subgroups of a free pro-p-group S such that $NS_{(n+1)} = N'S_{(n+1)}$. Then $G = S/N$ has the vanishing n-fold Massey product property with respect to $\mathbb{F}_p$ if and only if $G' = S/N'$ has this property.*

Proof. Because surjective homomorphisms take nth p-Zassenhaus filtrations onto nth p-Zassenhaus filtrations, using our assumption we have

$$G/G_{(n+1)} \cong S/NS_{(n+1)} = S/N'S_{(n+1)} \cong G'/G'_{(n+1)}.$$

Therefore our result follows from Lemma 3.9. □

4. First examples

Example 4.1. If G is a free pro-p-group, then it has the n-fold Massey product vanishing property for every $n \geq 2$ because $H^2(G, \mathbb{F}_p) = 0$. Alternatively, this follows from the universal property of G and condition (ii) of Corollary 3.4.

Recall that a profinite group G is *projective* (in the category of profinite groups) if for any finite groups A and B, and for any surjective morphisms $\rho\colon G \to A$ and $\alpha\colon B \to A$, there exists a homomorphism $\gamma : G \to B$ such that $\rho = \gamma \circ \alpha$ (see [FJ, p. 207]).

Example 4.2. Let G be a projective group. Then it has the n-fold Massey product vanishing property for every $n \geq 3$ and for every p. This follows directly from the definition of projective groups and condition (ii) of Corollary 3.4.

A pro-p-group G is said to be a *Demushkin group* if

- $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) < \infty$,
- $\dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p) = 1$,
- the cup product $H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ is a non-degenerate bilinear form.

Theorem 4.3. *Let $n \geq 3$ be an integer and p a prime number. Then every pro-p Demushkin group has the vanishing n-fold Massey product property with respect to $\mathbb{F}_p$.*

The following proof is adapted from that of [HW, Lemma 3.5].

Proof. Let G be a pro-p Demushkin group. Let $\chi_1, \dots, \chi_n \in H^1(G, \mathbb{F}_p)$. Assume that $\langle \chi_1, \dots, \chi_n \rangle$ is defined. If $\chi_1 = 0$ then by [Fe, Lemma 6.2.4], which is valid in the profinite case as well, $\langle \chi_1, \dots, \chi_n \rangle$ contains 0. So we may assume that $\chi_1 \neq 0$. In this case, to show that $\langle \chi_1, \dots, \chi_n \rangle$ contains 0, we only need to show that

$$\chi_1 \cup (-)\colon H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$$

is surjective, by Remark 2.2. From the definition of Demushkin groups, one has

$$H^2(G, \mathbb{F}_p) \simeq \mathbb{F}_p.$$

So it is enough to show that the map $\chi_1 \cup (-)$ is non-zero. But this follows from the non-degeneracy of the cup product $H^1(G, \mathbb{F}_p) \times H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$. □

Remark 4.4. If F is a finite field extension of $\mathbb{Q}_p$ containing a primitive pth root of unity, then $G_F(p)$ is a pro-p Demushkin group. In [Sha], Shafarevich showed that if F is as above, but contains no primitive pth root of unity, then $G_F(p)$ is a free pro-p-group.

Demushkin groups along with free pro-p-groups, abelian torsion free pro-p-groups, and cyclic groups of order 2 play a dominant role in the current investigation of finitely generated subgroups of maximal pro-p quotients $G_F(p)$ of absolute Galois groups. The elementary conjecture predicts that the groups above are all "building blocks" for $G_F(p)$ (see [Ef1, Mar, LLMS, JW]).

Proposition 4.5. *Let G_1, G_2 be two pro-p-groups. Then the free pro-p-product $G_1 * G_2$ has the vanishing n-fold Massey product property with respect to $\mathbb{F}_p$ if and only if both G_1 and G_2 have this property.*

Proof. Assume that G_1, G_2 have the vanishing n-fold Massey product property. Let $\bar\rho\colon G_1 * G_2 \to \bar{\mathbb{U}}_{n+1}(\mathbb{F}_p)$ be any homomorphism. By Corollary 3.4, we need to find a homomorphism $\rho\colon G_1 * G_2 \to \mathbb{U}_{n+1}(\mathbb{F}_p)$ such that $\rho_{j,j+1} = \bar\rho_{j,j+1}$, $j = 1, \dots, n$.

For each $i = 1, 2$ let $\kappa_i\colon G_i \to G_1 * G_2$ be the natural monomorphism, and set $\bar\rho_i = \bar\rho\circ\kappa_i$. Since G_i has the vanishing n-fold Massey product property, there is a representation $\rho_i\colon G_i \to \mathbb{U}_{n+1}(\mathbb{F}_p)$ such that $(\rho_i)_{j,j+1} = (\bar\rho_i)_{j,j+1}$ for $j = 1, \dots, n$. The universal property of free products yields a unique homomorphism $\rho\colon G_1 * G_2 \to \mathbb{U}_{n+1}(\mathbb{F}_p)$ such that $\rho\circ\kappa_i = \rho_i$, $i = 1, 2$. For $i = 1, 2$ and $j = 1, \dots, n$ we have

$$\rho_{j,j+1}\circ\kappa_i = (\rho\circ\kappa_i)_{j,j+1} = (\rho_i)_{j,j+1} = (\bar\rho_i)_{j,j+1} = (\bar\rho\circ\kappa_i)_{j,j+1} = \bar\rho_{j,j+1}\circ\kappa_i,$$

so $\rho_{j,j+1} = \bar\rho_{j,j+1}$, as desired.

Conversely, assume that $G_1 * G_2$ has the vanishing n-fold Massey product property. Let $\bar\rho_1\colon G_1 \to \bar{\mathbb{U}}_{n+1}(\mathbb{F}_p)$ be any representation of G_1. Let $\bar\rho_2\colon G_2 \to \bar{\mathbb{U}}_{n+1}(\mathbb{F}_p)$ be the trivial homomorphism. Then by the universal property of free products, there exists a homomorphism $\bar\rho\colon G_1 * G_2 \to \bar{\mathbb{U}}_{n+1}(\mathbb{F}_p)$ such that $\bar\rho_1 = \bar\rho\circ\kappa_1$. Since $G_1 * G_2$ has the vanishing n-fold Massey product property, there exists a homomorphism $\rho\colon G_1 * G_2 \to \mathbb{U}_{n+1}(\mathbb{F}_p)$ such that $\rho_{i,i+1} = \bar\rho_{i,i+1}$ for $i = 1, \dots, n$. Let $\rho_1\colon G_1 \to \mathbb{U}_{n+1}(\mathbb{F}_p)$ be the composite $\rho\circ\kappa_1$. Then for $i = 1, \dots, n$, we have

$$(\rho_1)_{i,i+1} = (\rho\circ\kappa_1)_{i,i+1} = \rho_{i,i+1}\circ\kappa_1 = \bar\rho_{i,i+1}\circ\kappa_1 = (\bar\rho\circ\kappa_1)_{i,i+1} = (\bar\rho_1)_{i,i+1}.$$

Hence by Corollary 3.4, G_1 has the vanishing n-fold Massey product property.

Similarly, G_2 has the vanishing n-fold Massey product property. □

Let $p > 2$ be an odd prime and G a pro-p-group. Let $\chi \in H^1(G, \mathbb{F}_p)$. In [Kra, Section 3], Kraines defined a restricted n-fold Massey product $\langle\chi\rangle^n$. If a restricted n-fold Massey product $\langle\chi\rangle^n$ is defined then so is the n-fold Massey product $\langle\chi, \dots, \chi\rangle$, and the latter contains the former. Kraines showed that $\langle\chi\rangle^n = 0$ for $n = 2, \dots, p-1$ and $\langle\chi\rangle^p$ is defined [Kra, Theorem 15]. In fact $\langle\chi\rangle^p = -\beta(\chi)$, where $\beta\colon H^1(G, \mathbb{F}_p) \to H^2(G, \mathbb{F}_p)$ is the Bockstein homomorphism, i.e., the connecting homomorphism induced by the exact sequence

$$0 \to \mathbb{Z}/p \to \mathbb{Z}/p^2 \to \mathbb{Z}/p \to 0.$$

Using Kraines' results mentioned above, we obtain the following result.

Proposition 4.6. *Let n be an integer with $2 < n \leq p$. Let F be any field containing a primitive pth root of unity if* $\mathrm{char}(F) \neq p$. *Let G be the absolute Galois group G_F of F or its maximal pro-p quotient $G_F(p)$. Then for any $\chi \in H^1(G, \mathbb{F}_p)$, the n-fold Massey product $\langle \chi, \dots, \chi \rangle$ is defined and contains* 0.

Proof. It is enough to consider the case $G = G_F(p)$ by Remark 3.2. Also if $\mathrm{char}\, F = p$ then since $G_F(p)$ is a free pro-p-group, we have$\langle \chi, \dots, \chi \rangle = 0$. So we may assume that $\mathrm{char}\, F \neq p$; let us fix a primitive pth root of unity ξ. Then $\chi = \chi_a$ for some $a \in F^*$, where $\chi_a \in H^1(G_F, \mathbb{F}_p) = H^1(G_F(p), \mathbb{F}_p)$ is the character associated to a via the Kummer map $F^* \to H^1(G_F, \mathbb{F}_p) = H^1(G_F(p), \mathbb{F}_p)$.

If $n < p$ then by [Kra, Theorem 15], $\langle \chi_a, \dots, \chi_a \rangle$ contains $0 = \langle \chi_a \rangle^n$.

Now we consider the case $n = p$. Then $\langle \chi_a \rangle^p = -\beta(\chi_a)$. By [EM1, proof of Proposition 3.2], $\beta(\chi_a) = \chi_a \cup \chi_\xi$ ($\xi \in F^*$ is a fixed primitive pth root of unity). Hence by Remark 2.2, one has

$$0 = \langle \chi_a \rangle^p + \chi_a \cup \chi_\xi \in \langle \chi_a, \dots, \chi_a \rangle,$$

as claimed. □

Example 4.7. Let p be an odd prime number and $G = \mathbb{Z}/p\mathbb{Z}$. Let $\chi \in H^1(G, \mathbb{F}_p)$ be the identity map. Then the p-fold Massey product $\langle \chi, \dots, \chi \rangle$ is defined but does not contain 0. Indeed, suppose it does; then there exists a representation $\rho\colon G \to \mathbb{U}_{p+1}(\mathbb{F}_p)$ such that $\rho_{i,i+1} = \chi$ for $i = 1, \dots, p$. Let $B := \rho(\bar{1}) \in \mathbb{U}_{p+1}(\mathbb{F}_p)$. Then all entries of B at positions $(i, i+1)$, $i = 1, \dots, p$, are 1. Hence $B^p \neq 1$, contradicting the fact that B is the image of an element of order p.

Remark 4.8. Proposition 4.6 and Example 4.7 immediately provide an explanation to a part of the well-known Artin–Schreier theorem [AS1, AS2] (respectively, Becker's theorem [Be]) which says that the absolute Galois group G_F (respectively, its maximal pro-p quotient $G_F(p)$) of any field F cannot have an element of odd prime order. (Note also that if $G_F \simeq \mathbb{Z}/p\mathbb{Z}$ then F contains a primitive pth root of unity.)

In [MTE], using Galois automatic realization of given groups, we shall prove a more general result than Proposition 4.6 in which the condition $n \leq p$ can be omitted, provided that if $p = 2$ then -1 is a square in F. One can then use this generalized result to show the full Artin–Schreier theorem (respectively, Becker's theorem) (see [MTE]).

5. Splitting variety and the vanishing property

Let F be a field of characteristic $\neq 2$. Let $G = G_F(2)$ be the maximal pro-2 Galois group of F. Let $a, b, c \in F^*$ and $\chi_a, \chi_b, \chi_c \in H^1(G, \mathbb{F}_2)$ be the characters corresponding to a, b, c via the Kummer map $F^* \to H^1(G, \mathbb{F}_2)$. Let $X_{a,b,c}$ be the variety in $\mathbb{G}_{\mathrm{m}} \times \mathbb{A}^4$ defined by the equation

$$bX^2 = (Y_1^2 - aY_2^2 + cY_3^2 - acY_4^2)^2 - 4c(Y_1Y_3 - aY_2Y_4)^2.$$

First proof of Theorem 1.2. If a (or b, or c) is in $(F^*)^2$ then the corresponding character χ_a (or χ_b, or χ_c) is the trivial character, and hence the Massey product $\langle \chi_a, \chi_b, \chi_c\rangle$ contains 0 by [Fe, Lemma 6.2.4]. So we may assume that a, b and c are not in $(F^*)^2$. The following well-known fact will be used frequently: $\chi_a \cup \chi_b = 0$ if and only if b is in $N_{F(\sqrt{a})/F}(F(\sqrt{a})^*)$ (see e.g. [HW, Introduction, p. 4], [Se2, Chapter XIV, Propositions 4–5], or [Sri, Lemma 8.4]). There are two cases to consider.

Case 1: a/c is in $(F^*)^2$. Then $\chi_a = \chi_c$ and hence $\langle \chi_a, \chi_b, \chi_c\rangle = \langle \chi_a, \chi_b, \chi_a\rangle$ and we can assume $a = c$. Since $\langle \chi_a, \chi_b, \chi_a\rangle$ is defined, $\chi_a \cup \chi_b = 0$. Hence $b \in N_{F(\sqrt{a})/F}(F(\sqrt{a})^*)$ and there exist $\alpha_1, \alpha_2 \in F$ such that

$$b = N_{F(\sqrt{a})/F}(\alpha_1 + \alpha_2\sqrt{a}) = \alpha_1^2 - a\alpha_2^2.$$

If $\alpha_1 \neq 0$ then let $x = 4\alpha_1 \neq 0$, $y_1 = 2\alpha_1$, $y_2 = y_3 = \alpha_2$, $y_4 = 0$. One has

$$\begin{aligned}(y_1^2 - ay_2^2 + ay_3^2 - a^2y_4^2)^2 - 4a(y_1y_3 - ay_2y_4)^2 &= (4\alpha_1^2)^2 - 4a(2\alpha_1\alpha_2)^2\\ &= 16\alpha_1^2(\alpha_1^2 - a\alpha_2^2) = bx^2.\end{aligned}$$

If $\alpha_1 = 0$ then $b = -a\alpha_2^2$. Let $x = 4a \neq 0$, $y_1 = a$, $y_2 = y_3 = \alpha_2$, $y_4 = -1$. Then

$$(y_1^2 - ay_2^2 + ay_3^2 - a^2y_4^2)^2 - 4a(y_1y_3 - ay_2y_4)^2 = 0 - 4a(2a\alpha_2)^2 = bx^2.$$

Case 2: a/c is not in $(F^*)^2$. Since $\langle \chi_a, \chi_b, \chi_c\rangle$ is defined, $\chi_a \cup \chi_b = 0 = \chi_b \cup \chi_c$. Hence $b \in N_{F(\sqrt{a})/F}(F(\sqrt{a})^*)$ and $b \in N_{F(\sqrt{c})/F}(F(\sqrt{c})^*)$. Thus, there exist $\alpha_1, \alpha_2, \gamma_1, \gamma_2 \in F$ such that

$$\begin{aligned}b &= N_{F(\sqrt{a})/F}(\alpha_1 + \alpha_2\sqrt{a}) = \alpha_1^2 - a\alpha_2^2\\ &= N_{F(\sqrt{c})/F}(\gamma_1 + \gamma_2\sqrt{c}) = \gamma_1^2 - c\gamma_2^2.\end{aligned}$$

Hence $c\gamma_2^2 - a\alpha_2^2 = \gamma_1^2 - \alpha_1^2 \neq 0$ because a/c and b are not in $(F^*)^2$. Therefore $\alpha_1 + \gamma_1 \neq 0$.

Let

$$x = 2(\alpha_1 + \gamma_1), \quad y_1 = \alpha_1 + \gamma_1, \quad y_2 = \alpha_2, \quad y_3 = \gamma_2, \quad y_4 = 0.$$

Then

$$\begin{aligned}(y_1^2 - ay_2^2 + cy_3^2 - acy_4^2)^2 - 4c(y_1y_3 - ay_2y_4)^2 &\\ &= [(\alpha_1 + \gamma_1)^2 - a\alpha_2^2 + c\gamma_2^2]^2 - 4c[(\alpha_1 + \gamma_1)\gamma_2]^2\\ &= [(\alpha_1 + \gamma_1)^2 + \gamma_1^2 - \alpha_1^2]^2 - 4c(\alpha_1 + \gamma_1)^2\gamma_2^2\\ &= 4(\alpha_1 + \gamma_1)^2\gamma_1^2 - 4c(\alpha_1 + \gamma_1)^2\gamma_2^2\\ &= 4(\alpha_1 + \gamma_1)^2(\gamma_1^2 - c\gamma_2^2) = 4(\alpha_1 + \gamma_1)^2 b = bx^2.\end{aligned}$$

Therefore the variety $X_{a,b,c}$ contains an F-rational point, namely (x, y_1, y_2, y_3, y_4). Hence $\langle \chi_a, \chi_b, \chi_c\rangle$ contains 0 by [HW, Corollary 2.7]. □

6. Field theory and the vanishing property

In this section we present another proof of Theorem 1.2 using Galois theory and [GLMS].

Notation: For a, b in a field F of characteristic $\neq 2$, $(a, b)_F$ is the quaternion algebra generated by i and j such that $i^2 = a$, $j^2 = b$ and $ij = -ji$. For x, y in a group, $[x, y] = x^{-1}y^{-1}xy$.

Second proof of Theorem 1.2. As in the first proof, we may assume that a, b and c are not in $(F^*)^2$.

Assume that $\langle \chi_b, \chi_a, \chi_c\rangle$ is defined; we will show that it contains 0. (Note that the order in the triple Massey product here is different from the one in the first proof, because we want to be consistent with the notation of [GLMS].)

Case 1: $a \equiv b \equiv c \bmod (F^*)^2$. Then $\langle \chi_b, \chi_a, \chi_c\rangle = \langle \chi_b, \chi_b, \chi_b\rangle$. Since $(b, b)_F = 0$, b is a norm of $F(\sqrt{b})/F$, i.e., $b = N_{F(\sqrt{b})/F}(\beta)$ for some $\beta \in F(\sqrt{b})$. Let $L = F(\sqrt{\beta})$. Then L/F is a Galois extension which is cyclic of order 4. Its Galois group is generated by $\sigma_b \in \mathrm{Gal}(L/F)$, where $\sigma_b(\sqrt{\beta}) = \sqrt{b}/\sqrt{\beta}$.

One can define a homomorphism $\varphi\colon \mathrm{Gal}(L/F) \to \mathbb{U}_4(\mathbb{F}_2)$ by letting

$$\sigma_b \mapsto B := \begin{bmatrix} 1 & 1 & 0 & 0\\ 0 & 1 & 1 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Let ρ be the composite homomorphism $\mathrm{Gal}_F \to \mathrm{Gal}(L/F) \overset{\varphi}{\to} \mathbb{U}_4(\mathbb{F}_2)$. Then one can check that

$$\rho_{i,i+1} = \chi_b \quad \forall i = 1, 2, 3.$$

(Note that $\sigma_b|_{F(\sqrt{b})/F}$ maps $\sqrt{b}$ to $-\sqrt{b}$ and here we are identifying $\mathbb{F}_2 = \{-1, 1\} = \{0, 1\}$.) Hence by Theorem 3.1, $\langle \chi_b, \chi_b, \chi_b\rangle$ contains 0.

Case 2: $a \equiv b \bmod (F^*)^2$ and $a \not\equiv c \bmod (F^*)^2$. This case can be treated in a similar way to Case 3 below.

Case 3: $a \not\equiv b \bmod (F^*)^2$ and $c \equiv a \bmod (F^*)^2$. Then $\langle \chi_b, \chi_a, \chi_c\rangle = \langle \chi_b, \chi_a, \chi_a\rangle$. Since $(a, a)_F = (a, b)_F = 0$ in the Brauer group $\mathrm{Br}(F)$, by construction in [GLMS, Section 3] we have a Galois extension L/F which contains $F(\sqrt{a}, \sqrt{b})$ with Galois group G_1 described below. Also there exist $\sigma_a, \sigma_b \in \mathrm{Gal}(L/F)$ such that

$$\sigma_a(\sqrt{a}) = -\sqrt{a}, \quad \sigma_a(\sqrt{b}) = \sqrt{b}, \quad \sigma_b(\sqrt{a}) = \sqrt{a}, \quad \sigma_a(\sqrt{b}) = -\sqrt{b}.$$

Let G_1 be the group generated by two symbols x, y subject to the relations: $x^4 = y^2 = 1 = (x, y)^2 = (x, y, x)^2$ and (x, y, x) commutes with x and y. Then it is shown in [GLMS] that σ_a, σ_b generate $\mathrm{Gal}(L/F)$, and $\mathrm{Gal}(L/F)$ is isomorphic to G_1 by letting $\sigma_a \mapsto x$ and $\sigma_b \mapsto y$.

Let

$$u := \begin{bmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 1 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad v := \begin{bmatrix} 1 & 1 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then $u^4 = v^2 = [u, v]^2 = 1$ and $[[u, v], u]$ is central and of order 2 in $\mathbb{U}_4(\mathbb{F}_2)$. Hence one can define a homomorphism $\varphi\colon \mathrm{Gal}(L/F) \to \mathbb{U}_4(\mathbb{F}_2)$ by letting $\sigma_a \mapsto u$, $\sigma_b \mapsto v$. (The homomorphism φ is in fact injective so it induces an isomorphism between $\mathrm{Gal}(L/F)$ and the subgroup generated by u, v. This follows from $Z(G_1) = \mathbb{Z}/2\mathbb{Z}$, which is the smallest non-trivial normal subgroup of G_1 and $[[u, v], u] \neq 1$.)

Let ρ be the composite $\mathrm{Gal}_F \to \mathrm{Gal}(L/F) \xrightarrow{\varphi} \mathbb{U}_4(\mathbb{F}_2)$. Then one can check that

$$\rho_{12} = \chi_b \quad \text{and} \quad \rho_{23} = \rho_{34} = \chi_a.$$

Hence by Theorem 3.1, $\langle \chi_b, \chi_a, \chi_a \rangle$ contains 0.

Case 4: $a \not\equiv b \bmod (F^*)^2$ and $c \equiv b \bmod (F^*)^2$. Then $\chi_b = \chi_c$ and hence $\langle \chi_b, \chi_a, \chi_c \rangle = \langle \chi_b, \chi_a, \chi_b \rangle$. By assumption, we have $(a, b)_F = 0$. Hence $b = N_{F(\sqrt{a})/F}(\beta)$ for some $\beta \in F(\sqrt{a})$. Let $L = F(\sqrt{a}, \sqrt{b}, \sqrt{\beta})$. We define $\sigma_a, \sigma_b \in \mathrm{Gal}(L/F)$ as follows:

$$\sigma_a\colon \sqrt{a} \mapsto -\sqrt{a};\ \sqrt{b} \mapsto \sqrt{b};\ \sqrt{\beta} \mapsto -\sqrt{b}/\sqrt{\beta};$$
$$\sigma_b\colon \sqrt{a} \mapsto \sqrt{a};\ \sqrt{b} \mapsto -\sqrt{b};\ \sqrt{\beta} \mapsto \sqrt{\beta}.$$

Then the subgroup of $\mathrm{Gal}(L/F)$ generated by σ_a, σ_b is isomorphic to the dihedral group D_4 of order $8 = [L : F]$. Hence $\mathrm{Gal}(L/F)$ is isomorphic to D_4 and generated by σ_a, σ_b. One can define a homomorphism $\varphi\colon \mathrm{Gal}(L/F) \to \mathbb{U}_4(\mathbb{F}_2)$ by letting

$$\sigma_a \mapsto u := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \sigma_b \mapsto v := \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Let ρ be the composite $\mathrm{Gal}_F \to \mathrm{Gal}(L/F) \xrightarrow{\varphi} \mathbb{U}_4(\mathbb{F}_2)$. Then one can check that

$$\rho_{23} = \chi_a \quad \text{and} \quad \rho_{12} = \rho_{34} = \chi_b.$$

Hence by Theorem 3.1, $\langle \chi_b, \chi_a, \chi_b \rangle$ contains 0.

Case 5: $a \not\equiv b \bmod (F^*)^2$ and $c \equiv ab \bmod (F^*)^2$. Then $\langle \chi_b, \chi_a, \chi_c \rangle = \langle \chi_b, \chi_a, \chi_{ab} \rangle$. By assumption, we have $(a, b)_F = (a, ab)_F = 0$. Hence $(a, b)_F = (a, a)_F = 0$. As in Case 3, we can construct a Galois extension L/F with Galois group isomorphic to G_1. Let

$$A := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad B := \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then $A^4 = B^2 = [A, B]^2$ and $[[A, B], A]$ is central and of order 2 in $\mathbb{U}_4(\mathbb{F}_2)$. Hence one can define a homomorphism $\varphi\colon \mathrm{Gal}(L/F) \to \mathbb{U}_4(\mathbb{F}_2)$ by letting $\sigma_a \mapsto A$, $\sigma_b \mapsto B$. Here σ_a, σ_b are as in Case 3. (The homomorphism φ is in fact injective so that it induces an isomorphism between $\mathrm{Gal}(L/F)$ and the subgroup generated by A, B. This follows from $Z(G_1) = \mathbb{Z}/2\mathbb{Z}$ and $[[A, B], A] \neq 1$.)

Let $\rho\colon \mathrm{Gal}_F \to \mathrm{Gal}(L/F) \xrightarrow{\varphi} \mathbb{U}_4(\mathbb{F}_2)$. Then one can check that

$$\rho_{12} = \chi_b, \qquad \rho_{23} = \chi_a, \qquad \rho_{34} = \chi_{ab}.$$

Hence by Theorem 3.1, $\langle \chi_b, \chi_a, \chi_{ab}\rangle$ contains 0.

Case 6: a, b, c are $\mathbb{F}_2$-independent in F^*/F^{*2}. Because $\langle \chi_b, \chi_a, \chi_c\rangle$ is defined, $(b, a)_F = (a, c)_F = 0$. As in [GLMS], we have the following construction. There exist $\beta \in F(\sqrt{b})$ and $\gamma \in F(\sqrt{c})$ such that $N_{F(\sqrt{b})/F}(\beta) = N_{F(\sqrt{c})/F}(\gamma) = a$. Let $E = F(\sqrt{b}, \sqrt{c})$. Then [Wad, Lemma 2.14] implies that there exist $\delta \in E$ and $d \in F$ such that $N_{E/F(\sqrt{b})}(\delta) = \beta d$ and $N_{E/F(\sqrt{c})}(\delta) = \gamma d$. Let $E' = E(\sqrt{a})$, $K = E'(\sqrt{\beta d}, \sqrt{\gamma d})$ and $L = K(\sqrt{\delta})$. It is shown in [GLMS, proof of Proposition 4.6] that there exist $\sigma_a, \sigma_b, \sigma_c \in \mathrm{Gal}(L/F)$ such that σ_a fixes $\sqrt{b}, \sqrt{c}$ and $\sigma_a(\sqrt{a}) = -\sqrt{a}$, and similarly for σ_b, σ_c. Furthermore, $\sigma_a, \sigma_b, \sigma_c$ generate $\mathrm{Gal}(L/F)$.

Let

$$X := \begin{bmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 1 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad Y := \begin{bmatrix} 1 & 1 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad Z := \begin{bmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

By direct computation one has

(1) $X^2 = Y^2 = Z^2 = 1$, $[X, Y]^2 = [X, Z]^2 = [Y, Z] = 1$,

(2) $[Y, [X, Z]] = [Z, [X, Y]]$ is in the center and of order dividing 2.

Hence there is a natural homomorphism φ from $\mathrm{Gal}(L/F) \simeq G_2$ to $\mathbb{U}_4(\mathbb{F}_2)$ (G_2 is defined in [GLMS, Definition 4.4] as the group generated by x, y, z satisfying (1)–(2) above). As X, Y, Z generates $\mathbb{U}_4(\mathbb{F}_2)$, φ is surjective and hence an isomorphism because $|\mathrm{Gal}(L/F)| = |\mathbb{U}_4(\mathbb{F}_2)| = 64$. Also from [GLMS, proof of Proposition 4.7] one deduces that φ maps σ_a to X, σ_b to Y, and σ_c to Z.

Let $\rho\colon \mathrm{Gal}_F \to \mathrm{Gal}(L/F) \overset{\varphi}{\simeq} \mathbb{U}_4(\mathbb{F}_2)$. Then one can check that

$$\rho_{12} = \chi_b, \qquad \rho_{23} = \chi_a, \qquad \rho_{34} = \chi_c.$$

(Note that χ_a is the composite $\mathrm{Gal}_F \to \mathrm{Gal}(L/F) \to \mathrm{Gal}(F(\sqrt{a})/F) \simeq \mathbb{F}_2$, where the last map sends $\sigma_a|_{F(\sqrt{a}/F)}$ to 1, and similarly for χ_b, χ_c. Since all the maps $\rho, \chi_a, \chi_b, \chi_c$ factor through $\mathrm{Gal}(L/F)$, it is enough to check on $\sigma_a, \sigma_b, \sigma_c$.)

Hence by Theorem 3.1, $\langle \chi_b, \chi_a, \chi_c\rangle$ contains 0. □

Remark 6.1. Because the Galois extensions L/F with Galois group isomorphic to $\mathbb{U}_4(\mathbb{F}_2)$ play a fundamental role in the theory of triple Massey products, and for their use in Galois theory, we shall describe the structure of these extensions. For further related results see [GLMS] where $\mathbb{U}_4(\mathbb{F}_2)$ is denoted G_2. Let X, Y, Z be matrices defined as in Case 6 of the previous proof. Then observe that

$$\begin{aligned}\mathbb{U}_4(\mathbb{F}_2) &= \{X^\alpha Y^\beta Z^\gamma [X, Y]^\lambda [X, Z]^\mu [[X, Y], Z]^\nu \mid \alpha, \beta, \gamma, \lambda, \mu, \nu = 0 \text{ or } 1\}\\ &= W \rtimes V,\end{aligned}$$

where V is isomorphic to the Klein 4-group $V_4 \simeq V = \langle Y, Z\rangle$ and $W \simeq \mathbb{F}_2[V]$.

Now let L/F be a $\mathbb{U}_4(\mathbb{F}_2)$-Galois extension. Let E be the fixed field of L under W. Then E/F is a V_4-extension, so $E = F(\sqrt{b}, \sqrt{c})$ for some $b, c \in F^*$ where b, c are linearly independent mod $(F^*)^2$.

Since W is a 2-elementary group, we have $\mathrm{Gal}(L/E) = W$, and by Kummer theory one has $L = E(\sqrt{M})$, where $M \subset E^*/(E^*)^2$ is dual to W. Then M is isomorphic to $\mathbb{F}_2[V]$.

Let $[\delta] \in E^*/(E^*)^2$ be a generator of M. We define $\sigma_b, \sigma_b \in \mathrm{Gal}(E/F)$ as follows: $\sigma_b(\sqrt{b}) = -\sqrt{b}$, $\sigma_b(\sqrt{c}) = \sqrt{c}$ and $\sigma_c(\sqrt{b}) = \sqrt{b}$, $\sigma_c(\sqrt{c}) = -\sqrt{c}$. Then

$$\sigma_b(\delta)\delta = N_{E/F(\sqrt{c})}(\delta), \quad \sigma_c(\delta)\delta = N_{E/F(\sqrt{b})}(\delta),$$

and we set

$$a := \sigma_b(\sigma_c(\delta))\sigma_c(\delta)\sigma_b(\delta)\delta = N_{E/F}(\delta).$$

Now since M is 4-dimensional, we have $a \notin (E^*)^2$. Thus we have shown that each $\mathbb{U}_4(\mathbb{F}_2)$-Galois extension L/F is a normal closure of $E(\sqrt{\delta})/F$ where

1. E/F is a V_4-extension;
2. $\delta \in E^*$ and $N_{E/F}(\delta) \notin (E^*)^2$.

One can see that the converse also holds: if L/F is a normal closure of $E(\sqrt{\delta})/F$ where E/F and δ satisfy conditions 1–2 above, then L/F is a $\mathbb{U}_4(\mathbb{F}_2)$-Galois extension.

Theorem 6.2. *Let G be the absolute Galois group G_F of a field F or its maximal 2-extension quotient $G_F(2)$. Then G has the vanishing triple Massey product property with respect to $\mathbb{F}_2$.*

Proof. It is enough to consider the case $G = G_F(2)$ by Corollary 3.5.

If F is of characteristic 2, then G is free and hence it has the vanishing triple Massey product property.

If F is of characteristic $\neq 2$, then G has the vanishing triple Massey product property by Theorem 1.2. □

Remark 6.3. After an ealier version of this paper was posted on arXiv:math, I. Efrat and E. Matzri [EMa] found yet another interesting approach which they used to find another proof of Theorem 1.2, and they also found another proof of the main theorem of [MT1].

7. Groups without the triple vanishing property

In this section, we construct pro-p-groups G which do not have the vanishing triple Massey product property. In particular, when $p = 2$, they are not realizable as $G_F(2)$ for any field F.

First we verify the following computational fact.

Lemma 7.1. *Let $a_i, b_i, c_i \in \mathbb{F}_p$, $i = 1, 2, 3$, and set*

$$A = \begin{bmatrix} 1 & 1 & a_1 & b_1 \\ 0 & 1 & 0 & c_1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & a_2 & b_2 \\ 0 & 1 & 1 & c_2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & a_3 & b_3 \\ 0 & 1 & 0 & c_3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then

$$[[B, C], A] = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Proof. A direct computation shows that A^{-1}, B^{-1}, C^{-1} are

$$\begin{bmatrix} 1 & -1 & -a_1 & c_1 - b_1 \\ 0 & 1 & 0 & -c_1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & -a_2 & -b_2 \\ 0 & 1 & -1 & -c_2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & -a_3 & a_3 - b_3 \\ 0 & 1 & 0 & -c_3 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

respectively. Therefore

$$[B, C] = \begin{bmatrix} 1 & 0 & 0 & a_2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad [B, C]^{-1} = \begin{bmatrix} 1 & 0 & 0 & -a_2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

and the assertion follows. □

Example 7.2. Let S be a free pro-p-group on generators $x_1, \dots, x_5$. Define $r = [x_4, x_5][[x_2, x_3], x_1]$, and let $\langle r \rangle$ be the closed normal subgroup of S generated by r. Note that it is contained in the Frattini subgroup $S_{(2)}$ of S. We show that $G = S/\langle r \rangle$ does not have the vanishing triple Massey product property. To this end let

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Let $\bar{A}, \bar{B}, \bar{C}$ be the images of A, B, C, respectively, in $\bar{\mathbb{U}}_4(\mathbb{F}_p)$. We define a representation $\bar{\rho}\colon S \to \bar{\mathbb{U}}_4(\mathbb{F}_p)$ by letting

$$\bar{\rho}(x_1) = \bar{A}, \quad \bar{\rho}(x_2) = \bar{B}, \quad \bar{\rho}(x_3) = \bar{C}, \quad \bar{\rho}(x_4) = 1, \quad \bar{\rho}(x_5) = 1.$$

By Lemma 7.1, $\bar{\rho}(r) = [[\bar{B}, \bar{C}], \bar{A}] = 1$, so $\bar{\rho}$ induces a representation $\bar{\rho}\colon G \to \bar{\mathbb{U}}_4(\mathbb{F}_p)$.

Now suppose that $\rho\colon S \to \mathbb{U}_4(\mathbb{F}_p)$ is a representation such that $\rho_{i,i+1} = \bar{\rho}_{i,i+1}$ for $i = 1, 2, 3$. By Corollary 3.4, we need to show that $\rho(r) \neq 1$. We may write

$$\rho(x_1) = \begin{bmatrix} 1 & 1 & a_1 & b_1 \\ 0 & 1 & 0 & c_1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \rho(x_2) = \begin{bmatrix} 1 & 0 & a_2 & b_2 \\ 0 & 1 & 1 & c_2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \rho(x_3) = \begin{bmatrix} 1 & 0 & a_3 & b_3 \\ 0 & 1 & 0 & c_3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\rho(x_4) = \begin{bmatrix} 1 & 0 & a_4 & b_4 \\ 0 & 1 & 0 & c_4 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \rho(x_5) = \begin{bmatrix} 1 & 0 & a_5 & b_5 \\ 0 & 1 & 0 & c_5 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

for some $a_i, b_i, c_i \in \mathbb{F}_p$, $i = 1, 2, 3, 4, 5$. We note that $\rho(x_4)$ and $\rho(x_5)$ commute, so by Lemma 7.1, $\rho(r) = [[\rho(x_2), \rho(x_3)], \rho(x_1)] \neq 1$, as claimed. □

Example 7.3. Let G be as in the previous example with $p = 2$. Then by Theorem 1.2 (or more precisely, Theorem 6.2), G is not realizable as $G_F(2)$ for any field F. For this statement, using [GLMS] we will provide another proof, which avoids Theorem 1.2 and the Massey product formalism technique.

Assume that $G = G_F(2)$ for some field F. Note that G is not a free pro-2-group, so F is of characteristic different from 2. We denote by σ_i the image of x_i in G. Let $\chi_1, \ldots, \chi_5 \in H^1(S, \mathbb{F}_2) = H^1(G, \mathbb{F}_2)$ be the characters dual to $x_1, \ldots, x_5$. Let $[a_1], \ldots, [a_5] \in F^*/(F^*)^2$ be elements corresponding to $\chi_1, \ldots, \chi_5$ via Kummer theory. This means $\chi_1(\sqrt{a_i}) = \sqrt{a_i}$ for $i \neq 1$ and $\chi_1(\sqrt{a_1}) = -\sqrt{a_1}$, etc.

By [NSW, Propositions 3.9.12-3.9.13], we have

$$a_2 \cup a_3 = a_3 \cup a_1 = 0.$$

Consider a field L/F attached to the triple a_2, a_3, a_1 (see [GLMS, Proposition 4.6]). Let σ_{a_i} be constructed as in [GLMS, proof of Proposition 4.6] with a, b, c there replaced by a_3, a_1, a_2, respectively. Then $[[\sigma_{a_2}, \sigma_{a_3}], \sigma_{a_1}]$ is a non-trivial element in $Z(\mathrm{Gal}(L/F)) \simeq \mathbb{Z}/2$. For each i, σ_i and σ_{a_i} act in the same way on $K = F(\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_3})$. Therefore $\sigma_i|_{L/F} = \sigma_{a_i}\gamma_i$ for γ_i in $\Phi(\mathrm{Gal}(L/F))$, the Frattini subgroup of $\mathrm{Gal}(L/F)$.

In the proof of the claim below we use basic commutator identities together with basic identities valid in $\mathrm{Gal}(L/F)$.

Claim. $[[\sigma_2, \sigma_3], \sigma_1]|_{L/F} = [[\sigma_{a_2}, \sigma_{a_3}], \sigma_{a_1}]$.

In fact,

$$[\sigma_2|_{L/F}, \sigma_3|_{L/F}] = [\sigma_{a_2}\gamma_2, \sigma_{a_3}\gamma_3] = [\sigma_{a_2}, \sigma_{a_3}][\sigma_{a_2}, \gamma_3][\gamma_2, \sigma_{a_3}] = [\sigma_{a_2}, \sigma_{a_3}]c,$$

where $c := [\sigma_{a_2}, \gamma_3][\gamma_2, \sigma_{a_3}]$, which is in the center of $\mathrm{Gal}(L/F)$. Hence

$$\begin{aligned}[[\sigma_2, \sigma_3], \sigma_1]|_{L/F} &= [[\sigma_2|_{L/F}, \sigma_3|_{L/F}], \sigma_1|_{L/F}] = [[\sigma_{a_2}, \sigma_{a_3}]c, \sigma_{a_1}\gamma_1] \\ &= [[\sigma_{a_2}, \sigma_{a_3}], \sigma_{a_1}\gamma_1] = [[\sigma_{a_2}, \sigma_{a_3}], \sigma_{a_1}].\end{aligned}$$

Therefore, $[[\sigma_2, \sigma_3], \sigma_1]|_{L/F}$ is a non-trivial element in $Z(\mathrm{Gal}(L/F)) \simeq \mathbb{Z}/2$.

Also observe that $[\sigma_4, \sigma_5]|_{L/F}$ is trivial because σ_4 and σ_5 act trivially on $K = F(\sqrt{a}, \sqrt{b}, \sqrt{c})$ and $\mathrm{Gal}(L/K)$ is abelian. Hence our relation $[\sigma_4, \sigma_5][[\sigma_2, \sigma_3], \sigma_1] = 1$ restricts non-trivially on L/F. Thus we obtain a contradiction showing that $G \not\simeq G_F(2)$ for any field F. □

Remark 7.4. As noted in [CEM, EM2], one can use [CEM, Proposition 9.1] (or [EM2, Corollary 6.3]) to show that various pro-2-groups occur as $G_F(2)$ for no field F of characteristic $\neq 2$. For the convenience of the reader, we recall this result for pro-2-groups below.

Proposition 7.5 ([CEM, Proposition 9.1], [EM2, Corollary 6.3]). *Let G_1, G_2 be pro-2-groups such that $G_1/(G_1)_{(3)} \simeq G_2/(G_2)_{(3)}$ and $H^*(G_1, \mathbb{F}_2) \not\simeq H^*(G_2, \mathbb{F}_2)$. Then at most one of G_1, G_2 can be isomorphic to the maximal pro-2 Galois group $G_F(2)$ of a field F of characteristic $\neq 2$.*

To show that a pro-2-group G_1 cannot be isomorphic to $G_F(2)$ for a field F of characteristic $\neq 2$, we choose a group G_2 such that the two conditions in the above corollary are satisfied and G_2 does occur as $G_L(2)$ for some field L of characteristic $\neq 2$, and we are done.

Now we consider the pro-2-group $G =: G_1$ defined as in the previous example, i.e., G is the quotient of the free pro-2-group S on generators $x_1, \dots, x_5$ by the relation $r = [x_4, x_5][[x_2, x_3], x_1]$. Then one might wonder whether we can use Proposition 7.5 to show that $G = G_1$ is not realizable as $G_F(2)$ for some field F of characteristic $\neq 2$. One very natural candidate for G_2 is the quotient of the free pro-2-group S by the relation $r_2 = [x_4, x_5]$. Then $G_1/(G_1)_{(3)} \simeq G_2/(G_2)_{(3)}$ and G_2 is the free product of the free pro-2-group on three generators x_1, x_2, x_3 with the group $\mathbb{Z}_2 \times \mathbb{Z}_2$. And it is known (see [JW, Theorem 3.6]) that G_2 is isomorphic to $G_F(2)$ for some field F of characteristic $\neq 2$. However, $H^*(G_1, \mathbb{F}_2) \simeq H^*(G_2, \mathbb{F}_2)$. In fact, let

$$H^1(G_1, \mathbb{F}_2) = U_1 \oplus V_1, \qquad H^1(G_2, \mathbb{F}_2) = U_2 \oplus V_2,$$

where for each $i = 1, 2$, U_i is spanned by the images of $\chi_1, \chi_2, \chi_3, \chi_4$ in $H^1(G_i, \mathbb{F}_2)$, and V_i is spanned by the image of χ_5 in $H^1(G_i, \mathbb{F}_2)$. Then using the usual transgression-relation pairing we see that:

- The cup product $U_i \otimes U_i \to H^2(G_i, \mathbb{F}_2)$ is trivial.
- The cup product $U_i \otimes V_i \to H^2(G_i, \mathbb{F}_2)$ is surjective, because $\chi_4 \cup \chi_5 \neq 0$ and $\dim H^2(G_i, \mathbb{F}_2) = 1$.

Hence G_i are mild groups (see for example [Fo, Gä, LM]). In particular, $\mathrm{cd}\, G_1 = \mathrm{cd}\, G_2 = 2$ and $H^*(G_1, \mathbb{F}_2) = H^*(G_2, \mathbb{F}_2)$. Therefore we cannot easily apply Proposition 7.5 to this example.

Our discussion above shows that our techniques provide genuinely new cases of pro-2-groups which cannot occur as $G_F(2)$ over some field F. Theorems 7.8 and 7.12 below exhibit large families of pro-2-groups which are not of the form $G_F(2)$.

It is easy to provide examples as above with more relations. For example let $G = S/R$, where S is a free pro-2-group on generators $x_1, \dots, x_7$ and R is its normal subgroup generated by $r_1 = [x_4, x_5][[x_2, x_3], x_1]$ and $r_2 = [x_6, x_7]$. Then the proof above showing that $G \not\simeq G_F(2)$ for any field F is valid word-for-word with the very exception that we choose in our possible example of F an $\mathbb{F}_2$-basis $[a_1], \dots, [a_7]$ orthogonal to $\chi_1, \dots, \chi_7$ instead of the original basis $[a_1], \dots, [a_5]$. □

Let G be a pro-p-group. Let

$$1 \to R \to S \to G \to 1$$

be a minimal presentation of G, i.e., S a free pro-p-group and $R \subset S_{(2)}$. Then the inflation map

$$\mathrm{inf}\colon H^1(G, \mathbb{F}_p) \to H^1(S, \mathbb{F}_p)$$

is an isomorphism by which we identify the two groups. Since S is free, we have $H^2(S, \mathbb{F}_p) = 0$ and from the 5-term exact sequence we obtain the transgression map

$$\mathrm{trg}\colon H^1(R, \mathbb{F}_p)^G \to H^2(G, \mathbb{F}_p),$$

which is an isomorphism. Therefore any element $r \in R$ gives rise to a map

$$\mathrm{tr}_r\colon H^2(G, \mathbb{F}_p) \to \mathbb{F}_p,$$

which is defined by $\alpha \mapsto \mathrm{trg}^{-1}(\alpha)(r)$ and is called the *trace map* with respect to r.

Let $(x_i)_{i\in I}$ be a basis of S, where I is a well-ordered set. Let χ_i, $i \in I$, be the dual basis to x_i, $i \in I$, of $H^1(S, \mathbb{F}_p) = H^1(G, \mathbb{F}_p)$, i.e., $\chi_i(x_j) = \delta_{ij}$.

Let r be any element in $S_{(2)}$. Then r may be uniquely written as

$$r = \begin{cases} \prod_{i\in I} x_i^{2a_i} \prod_{i<j} [x_i, x_j]^{b_{ij}} \prod_{i<j,\, k\le j} [[x_i, x_j], x_k]^{c_{ijk}} \cdot r' & \text{if } p = 2, \\ \prod_{i<j} [x_i, x_j]^{b_{ij}} \prod_{i\in I} x_i^{3a_i} \prod_{i<j,\, k\le j} [[x_i, x_j], x_k]^{c_{ijk}} \cdot r' & \text{if } p = 3, \\ \prod_{i<j} [x_i, x_j]^{b_{ij}} \prod_{i<j,\, k\le j} [[x_i, x_j], x_k]^{c_{ijk}} \cdot r' & \text{if } p \neq 2, 3, \end{cases} \qquad (*)$$

where $a_i, b_{ij}, c_{ijk} \in \{0, 1, \dots, p-1\}$ and $r' \in S_{(4)}$ [Vo1, Propositions 1.3.2 and 1.3.3]. For convenience we call ($*$) the canonical decomposition of r modulo $S_{(4)}$ (with respect to the basis (x_i)) and we also set $u_{ij} = b_{ij}$ if $i < j$, and $u_{ij} = b_{ji}$ if $j < i$.

Lemma 7.6. *Let the notation be as above. Assume that $R = \langle r\rangle$ and that the triple Massey product $\langle -\chi_k, -\chi_i, -\chi_j\rangle$ is defined for some distinct i, j, k with $i < j$ and $k < j$. Then there exists $\alpha \in \langle -\chi_k, -\chi_i, -\chi_j\rangle$, which can be given explicitly, such that*

$$\mathrm{tr}_r(\alpha) = c_{ijk}.$$

Proof. Since $\langle -\chi_k, -\chi_i, -\chi_j\rangle$ is defined, $\chi_k \cup \chi_i = \chi_i \cup \chi_j = 0$. Hence by [Vo1, Proposition 1.3.2] (see also [NSW, Proposition 3.9.13]), we have $u_{ki} = u_{ij} = 0$.

Let

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Then $A^p = B^p = C^p = [A, C] = 1$.

We define a representation $\rho\colon S \to \mathbb{U}_4(\mathbb{F}_p)$ by letting

$$x_k \mapsto A, \quad x_i \mapsto B, \quad x_j \mapsto C, \quad x_l \mapsto 1, \ \forall l \neq i, j, k.$$

Then

$$\rho(r) = [A, C]^{u_{kj}}[[B, C], A]^{c_{ijk}} \cdot [[A, C], B]^{c_{kji}} = [[B, C], A]^{c_{ijk}}.$$

Hence $\rho(r) = 1$ in $\bar{\mathbb{U}}_4(\mathbb{F}_p)$. Thus ρ induces a group homomorphism $\bar{\rho}\colon G \to \bar{\mathbb{U}}_4(\mathbb{F}_p)$. Then ρ is a lift of $\bar{\rho}$ in the sense discussed before Lemma 3.7. By checking on the generators we see that

$$\bar{\rho}_{12} = \chi_k, \quad \bar{\rho}_{23} = \chi_i, \quad \bar{\rho}_{34} = \chi_j.$$

Let $\alpha \in \langle -\chi_k, -\chi_i, -\chi_j\rangle$ be the Massey product value relative to the defining system corresponding to $\bar{\rho}$ and let $f \in H^1(R, \mathbb{F}_p)^G$ be defined by

$$f(\tau) = -\rho_{14}(\tau) \quad \text{for } \tau \in R.$$

By Lemma 3.7, we have $\operatorname{trg}(f) = \alpha$. Hence

$$\operatorname{tr}_r(\alpha) = f(r) = -\rho_{14}(r) = c_{ijk},$$

as desired. □

Proposition 7.7. *Suppose that in* ($*$) *there exist distinct i, j, k such that $i, k < j$ and $u_{ij} = u_{kj} = u_{ki} = u_{kl} = u_{jl} = 0$ for all $l \neq i, j, k$. If $p = 2$ assume further that $a_k = a_j = 0$. Let $G = S/\langle r\rangle$ and $\chi_1, \dots, \chi_n$ be the $\mathbb{F}_p$-basis of $H^1(S, \mathbb{F}_p) = H^1(G, \mathbb{F}_p)$ dual to $x_1, \dots, x_n$. Then $\langle -\chi_k, -\chi_i, -\chi_j\rangle$ is uniquely defined and*

$$\operatorname{tr}_r(\langle -\chi_k, -\chi_i, -\chi_j\rangle) = c_{ijk}.$$

In particular, if further $c_{ijk} \neq 0$ then $\langle -\chi_k, -\chi_i, -\chi_j\rangle$ does not vanish.

Proof. By [Vo1, Proposition 1.3.2] (see also [NSW, Proposition 3.9.13]) and by assumption, we have

$$\operatorname{tr}_r(\chi_k \cup \chi_l) = \begin{cases} \pm u_{kl} = 0 & \text{if } l \neq k, \\ 0 & \text{if } l = k,\ p \neq 2, \\ a_k = 0 & \text{if } l = k,\ p = 2. \end{cases}$$

Hence $\chi_k \cup \chi_l = 0$ for all $l = 1, \dots, n$. Thus $\chi_k \cup H^1(G, \mathbb{F}_p) = 0$. Similarly $H^1(G, \mathbb{F}_p) \cup \chi_j = 0$. Therefore $\langle -\chi_k, -\chi_i, -\chi_j \rangle$ is uniquely defined. By Lemma 7.6,

$$\mathrm{tr}_r(\langle -\chi_k, -\chi_i, -\chi_j \rangle) = c_{ijk},$$

as desired. □

The following theorem generalizes Example 7.2.

Theorem 7.8. *Let $\mathcal{R}$ be a set of elements in $S_{(2)}$. Assume that there exists an element r in $\mathcal{R}$ and distinct indices i, j, k with $i, k < j$ such that:*

1. *in the canonical decomposition (∗) of r modulo $S_{(4)}$, $u_{ij} = u_{kj} = u_{ki} = u_{kl} = u_{jl} = 0$ for all $l \neq i, j, k$, and $c_{ijk} \neq 0$, and if $p = 2$ assume further that $a_k = a_j = 0$; and*
2. *for every $s \in \mathcal{R}$ different from r, the factors $[x_k, x_i]$, $[x_i, x_k]$ and $[x_i, x_j]$ do not occur in the canonical decomposition of s modulo $S_{(4)}$.*

Then $G = S/\langle \mathcal{R} \rangle$ does not have the vanishing triple Massey product property.

Proof. Let $G' = G/\langle r \rangle$ and let f be the canonical map $G' = S/\langle r \rangle \to G = S/\langle \mathcal{R} \rangle$. We shall identify the three groups $H^1(S, \mathbb{F}_p)$, $H^1(G, \mathbb{F}_p)$ and $H^1(G', \mathbb{F}_p)$ via inflation maps. We also use $\langle \cdot, \cdot, \cdot \rangle_G$ (respectively, $\langle \cdot, \cdot, \cdot \rangle_{G'}$) to denote Massey products in the cohomology groups of G (respectively, G').

By [Vo1, Proposition 1.3.2] (see also [NSW, Proposition 3.9.13]) and by assumption,

$$\mathrm{tr}_s(\chi_k \cup \chi_i) = \mathrm{tr}_s(\chi_i \cup \chi_j) = 0 \quad \text{for all } s \in \mathcal{R}.$$

Hence $\chi_k \cup \chi_i = \chi_i \cup \chi_j = 0$ and $\langle -\chi_k, -\chi_i, -\chi_j \rangle_G$ is defined.

By the naturality property of Massey products (see e.g. [Kra, p. 433], [Mor, Property 2.1.2]), one has

$$f^*(\langle -\chi_k, -\chi_i, -\chi_j \rangle_G) \subseteq \langle -\chi_k, -\chi_i, -\chi_j \rangle_{G'}.$$

By Proposition 7.7 applied to G', we see that $\langle -\chi_k, -\chi_i, -\chi_j \rangle_{G'}$ does not vanish. Therefore $\langle -\chi_k, -\chi_i, -\chi_j \rangle_G$ does not vanish either, and we are done. □

Lemma 7.9. *Let*

$$u := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad v := \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

be matrices in $\mathbb{U}_4(\mathbb{F}_p)$. Then

$$[[u, v], u] = \begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad [[u, v], v] = 1, \quad v^p = 1.$$

Furthermore, if $p \geq 3$ then $u^p = 1$.

Lemma 7.10. *Let the notation be as in Lemma 7.6. Assume that $R = \langle r\rangle$.*

1. *Assume that $\langle -\chi_j, -\chi_i, -\chi_i\rangle$ is defined for some $i < j$. Then there exists an $\alpha \in \langle -\chi_j, -\chi_i, -\chi_i\rangle$ such that $\mathrm{tr}_r(\alpha) = c_{iji}$.*
2. *Assume that $\langle -\chi_i, -\chi_j, -\chi_j\rangle$ is defined for some $i < j$. Then there exists an $\alpha \in \langle -\chi_i, -\chi_j, -\chi_j\rangle$ such that $\mathrm{tr}_r(\alpha) = c_{ijj}$.*

Proof. We only prove item 1 since item 2 can be proved similarly. Since $\langle -\chi_j, -\chi_i, -\chi_i\rangle$ is defined, $\chi_i \cup \chi_j = 0 = \chi_i \cup \chi_j$. Hence by [Vo1, Proposition 1.3.2] (see also [NSW, Proposition 3.9.13]), $u_{ij} = 0$ and if $p = 2$ then $a_i = 0$.

Let u, v be the matrices of Lemma 7.9. We define a representation $\bar\rho\colon S \to \bar{\mathbb{U}}_4(\mathbb{F}_p)$ by letting

$$x_i \mapsto u, \qquad x_j \mapsto \bar v, \qquad x_l \mapsto 1,\ \forall l \neq i, j.$$

Then

$$\rho(r) = [[u,v],u]^{c_{iji}}[[u,v],v]^{c_{ijj}} = [[u,v],u]^{c_{iji}}.$$

Hence $\rho(r) = 1$ in $\bar{\mathbb{U}}_4(\mathbb{F}_p)$. Thus ρ induces a group homomorphism $\bar\rho\colon G \to \bar{\mathbb{U}}_4(\mathbb{F}_p)$. Then ρ is a lift of $\bar\rho$ in the sense discussed before Lemma 3.7. By checking on the generators we see that

$$\bar\rho_{12} = \chi_j, \qquad \bar\rho_{23} = \chi_i, \qquad \bar\rho_{34} = \chi_i.$$

Let $\alpha \in \langle -\chi_j, -\chi_i, -\chi_i\rangle$ be the Massey product value relative to the defining system corresponding to $\bar\rho$ and let $f \in H^1(R,\mathbb{F}_p)^G$ be defined by

$$f(\tau) = -\rho_{14}(\tau) \quad \text{for } \tau \in R.$$

By Lemma 3.7, we have $\mathrm{trg}(f) = \alpha$. Hence

$$\mathrm{tr}_r(\alpha) = f(r) = -\rho_{14}(r) = c_{iji},$$

as desired. □

Proposition 7.11. *Suppose that in (∗) there exist $i < j$ such that $u_{ij} = 0 = u_{il} = u_{jl}$ for all $l \neq i, j$. If $p = 2$ assume further that $a_i = a_j = 0$. Let $G = S/\langle r\rangle$ and $\chi_1, \dots, \chi_n$ be the $\mathbb{F}_p$-basis of $H^1(S,\mathbb{F}_p) = H^1(G,\mathbb{F}_p)$ dual to $x_1, \dots, x_n$. Then $\langle -\chi_j, -\chi_i, -\chi_i\rangle$ and $\langle -\chi_i, -\chi_j, -\chi_j\rangle$ are uniquely defined and*

$$\mathrm{tr}_r(\langle -\chi_j, -\chi_i, -\chi_i\rangle) = c_{iji}, \qquad \mathrm{tr}_r(\langle -\chi_i, -\chi_j, -\chi_j\rangle) = c_{ijj}.$$

In particular, if further $c_{iji} \neq 0$ (respectively, $c_{ijj} \neq 0$) then $\langle -\chi_j, -\chi_i, -\chi_i\rangle$ (respectively, $\langle -\chi_i, -\chi_j, -\chi_j\rangle$) does not vanish.

Proof. Under our assumption the triple Massey products $\langle -\chi_j, -\chi_i, -\chi_i\rangle$ and $\langle -\chi_i, -\chi_j, -\chi_j\rangle$ are uniquely defined. Then by Lemma 7.10,

$$\mathrm{tr}_r(\langle -\chi_j, -\chi_i, -\chi_i\rangle) = c_{iji}, \qquad \mathrm{tr}_r(\langle -\chi_i, -\chi_j, -\chi_j\rangle) = c_{ijj},$$

as desired. □

Theorem 7.12. *Let $\mathcal{R}$ be a set of elements in $S_{(2)}$. Assume that there exists an element r in $\mathcal{R}$ and indices i, j with $i < j$ such that:*

1. *in (∗), $u_{ij} = u_{il} = u_{jl} = 0$ for all $l \neq i, j$ and $c_{iji} \neq 0$ (respectively, $c_{ijj} \neq 0$) and if $p = 2$ assume further that $a_i = a_j = 0$; and*
2. *for every $s \in \mathcal{R}$ different from r, the factor $[x_i, x_j]$ does not occur in the canonical decomposition of s modulo $S_{(4)}$, and if $p = 2$ further x_i^2 (respectively, x_j^2) does not occur in the canonical decomposition of s modulo $S_{(4)}$.*

Then $G = S/\langle\mathcal{R}\rangle$ does not have the vanishing triple Massey product property.

Proof. Let $G' = G/\langle r\rangle$ and let f be the canonical map $G' = S/\langle r\rangle \to G = S/\langle\mathcal{R}\rangle$. We shall identify the three groups $H^1(S, \mathbb{F}_p)$, $H^1(G, \mathbb{F}_p)$ and $H^1(G', \mathbb{F}_p)$ via inflation maps. We also use $\langle\cdot,\cdot,\cdot\rangle_G$ (respectively, $\langle\cdot,\cdot,\cdot\rangle_{G'}$) to denote Massey products in the cohomology groups of G (respectively, G').

We only treat the case $c_{iji} \neq 0$. The other case is treated similarly.

By [Vo1, Proposition 1.3.2] (see also [NSW, Proposition 3.9.13]) and by assumption,

$$\mathrm{tr}_s(\chi_j \cup \chi_i) = \mathrm{tr}_s(\chi_i \cup \chi_i) = 0 \qquad \text{for all } s \in \mathcal{R}.$$

Hence $\chi_j \cup \chi_i = \chi_i \cup \chi_i = 0$ and $\langle -\chi_j, -\chi_i, -\chi_i\rangle_G$ is defined.

By the naturality property of Massey products (see e.g. [Kra, p. 433], [Mor, Property 2.1.2]), one has

$$f^*(\langle -\chi_j, -\chi_i, -\chi_i\rangle_G) \subseteq \langle -\chi_j, -\chi_i, -\chi_i\rangle_{G'}.$$

By Proposition 7.11 applied G', we see that $\langle -\chi_j, -\chi_i, -\chi_i\rangle_{G'}$ does not vanish. Therefore $\langle -\chi_j, -\chi_i, -\chi_i\rangle_G$ does not vanish either, and we are done. □

8. Further directions

Let p be a prime number. Let F be a field of characteristic $\neq p$ which contains a primitive pth root of unity. Let $G = G_F(p)$ be the maximal pro-p quotient of the absolute Galois group G_F of F. Denote by $G_{(i)}, i = 1, 2, \ldots,$ the p-Zassenhaus filtration of G. Let $F_{(i)}$ be the fixed field $F(p)^{G_{(i)}}$ of the group $G_{(i)}$, where $F(p)$ is the maximal p-extension of F.

When $p = 2$, $F_{(3)}$ is the compositum of all C_2, C_4, D_4-extensions K/F inside $F(2)$. This fact was proved by Villegas [Vi] and [MS2, Corollary 2.18] (see also [EM1, Corollary 11.3] for a more general result). Inspired by this beautiful fact, and the second proof of Theorem 1.2, we would like to propose the following conjecture.

Let C_n be the cyclic group of order n, D_4 the dihedral group of order 8, and let G_1 and G_2 be groups defined as in [GLMS] (see Cases 3 and 5 of the second proof of Theorem 1.2 for the definition). Explicitly, $G_2 \simeq \mathbb{U}_4(\mathbb{F}_2)$ and $G_1 \simeq$ the subgroup of $\mathbb{U}_4(\mathbb{F}_2)$ consisting of the upper-triangular unipotent 4×4-matrices (a_{ij}) with $a_{23} = a_{34}$.

Conjecture 8.1. *Let the notation be as above with $p = 2$. Then $F_{(4)}$ is the compositum of C_2, C_4, D_4, G_1, G_2-extensions K/F inside $F(2)$.*

We define the field F_ω as the compositum of C_2, C_4, D_4, G_1, G_2-extensions K/F inside $F(2)$. Then $F_\omega \subset F_{(4)}$ and the conjecture says that in fact $F_\omega = F_{(4)}$.

Definition 8.2. Let G be a pro-p-group and let $n \geq 1$ be an integer. We say that G has the *kernel n-unipotent property* if

$$G_{(n)} = \bigcap \ker(\rho\colon G \to \mathbb{U}_n(\mathbb{F}_p)),$$

where ρ runs over the set of all representations (continuous homomorphisms) $G \to \mathbb{U}_n(\mathbb{F}_p)$.

It is easy to see that for $n = 1, 2$, every pro-p-group G has the kernel n-unipotent property. It was shown that for $G = G_F(p)$, where F is a field containing a primitive pth root of unity, G has the kernel 3-unipotent property. (See [MS2, Vi, EM1] for the case $p = 2$ and [EM2, Example 9.5(1)] for the case $p > 2$.) For any fixed integer $n \geq 3$, in [MTE] we also give an example of a torsion free pro-p-group G such that G does not have the kernel n-unipotent property.

The following conjecture is a generalization of the above conjecture.

Conjecture 8.3 (Kernel n-Unipotent Conjecture). *Let F be a field containing a primitive pth root of unity and let $G = G_F(p)$. Let $n \geq 3$ be an integer. Then G has the kernel n-unipotent property.*

In a subsequent paper [MT2], we show that every pro-p Demushkin group has the kernel 4-unipotent property. In [MTE], we also show that pro-p Demushkin groups of rank 2 have the kernel n-unipotent property for all $n \geq 4$. It is shown in [Ef2, Theorem A] that every free pro-p-group has the kernel n-property for all $n \geq 3$. (In [MTE] we provide an alternative direct short proof.)

The results of this paper are also relevant in determining strong automatic realizations of canonical quotients of absolute Galois groups (see [MST]).

Finally, it is very interesting to extend the main theorems in this paper also to the case $p > 2$ (see [GMTT]).

Acknowledgments. We are grateful to Ido Efrat for his interest, encouragement, detailed notes, and suggesting various improvements which we have used. We thank Michael Hopkins and Kirsten Wickelgren for interesting discussions and correspondence, as well as their encouraging welcome of our results. We thank Murray Schacher and Suresh Venapally for their correspondence, and for information that they also obtained some of our results of Section 5. We also thank Julien Blondeau, Sunil Chebolu, Brian Conrad, Jochen Gärtner, Detlev Hoffmann, John Labute, Jeffrey Lagarias, Christian Maire, Claudio Quadrelli, Andrew Schultz, Romyar Sharifi, Nguyễn Quốc Thắng, Adam Topaz, Zack Wolske and Lei Zhang for their interest, encouragement and interesting discussions. We are also grateful to the referees for their comments and valuable suggestions which we used to improve our exposition. Last but not least, we would like to thank Leslie Hallock for her careful corrections of our use of the English language in this paper.

The first author is supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) grant R0370A01. The second author is supported in part by the National Foundation for Science and Technology Development (NAFOSTED) grant 101.04-2014.34.

References

[AS1] Artin, E., Schreier, O.: Algebraische Konstruktion reeller Körper. Abh. Math. Sem. Univ. Hamburg **5**, 85–99 (1927). Reprinted in: Artin's Collected Papers (eds. S. Lang and J. Tate), Springer, New York, 258–272 (1965) JFM 52.0120.05 MR 3069467

[AS2] Artin, E., Schreier, O.: Eine Kennzeichnung der reell abgeschlossenen Körper. Abh. Math. Sem. Univ. Hamburg **5**, 225–231 (1927). Reprinted in: Artin's Collected Papers (eds. S. Lang and J. Tate), Springer, New York, 289–295 (1965) JFM 53.0144.01 MR 3069477

[Ax] Ax, J.: The elementary theory of finite fields. Ann. of Math. **88**, 239–271 (1968) Zbl 0195.05701 MR 0229613

[Be] Becker, E.: Euklidische Körper und euklidische Hüllen von Körpern. J. Reine Angew. Math. **268/269**, 41–52 (1974) Zbl 0289.12103 MR 0354625

[BT1] Bogomolov, F., Tschinkel, Y.: Introduction to birational anabelian geometry. In: Current Developments in Algebraic Geometry, Math. Sci. Res. Inst. Publ. 59, Cambridge Univ. Press, Cambridge, 17–63 (2012) Zbl 1290.14017 MR 2931864

[BT2] Bogomolov, F., Tschinkel, Y.: Galois theory and projective geometry. Comm. Pure Appl. Math. **66**, 1335–1359 (2013) Zbl 1311.11105 MR 3078692

[CEM] Chebolu, S. K., Efrat, I., Mináč, J.: Quotients of absolute Galois groups which determine the entire Galois cohomology. Math. Ann. **352**, 205–221 (2012) Zbl 1272.12015 MR 2885583

[DGMS] Deligne, P., Griffiths, P., Morgan, J., Sullivan, D.: Real homotopy theory of Kähler manifolds. Invent. Math. **29**, 245–274 (1975) Zbl 0312.55011 MR 0382702

[De1] Demushkin, S. P.: The group of the maximum p-extension of a local field. Izv. Akad. Nauk. SSSR Ser. Mat. **25**, 329–346 (1961) (in Russian)

[De2] Demushkin, S. P.: On 2-extensions of a local field. Sibirsk. Mat. Zh. **4**, 951–955 (1963) (in Russian) Zbl 0199.09805 MR 0161854

[Dwy] Dwyer, W. G.: Homology, Massey products and maps between groups. J. Pure Appl. Algebra **6**, 177–190 (1975) Zbl 0338.20057 MR 0385851

[Ef1] Efrat, I.: Valuations, Orderings, and Milnor K-theory. Math. Surveys Monogr. 124, Amer. Math. Soc., Providence, RI (2006) Zbl 1103.12002 MR 2215492

[Ef2] Efrat, I.: The Zassenhaus filtration, Massey products, and representations of profinite groups. Adv. Math. **263**, 389–411 (2014) Zbl 1346.20027 MR 3239143

[EH] Efrat, I., Haran, D.: On Galois groups over Pythagorean and semi-real closed fields. Israel J. Math. **85**, 57–78 (1994) Zbl 0799.12002 MR 1264339

[EMa] Efrat, I., Matzri, E.: Vanishing of Massey products and Brauer groups. Canad. Math. Bull. **58**, 730–740 (2015) Zbl 06527783 MR 3415664

[EM1] Efrat, I., Mináč, J.: On the descending central sequence of absolute Galois groups. Amer. J. Math. **133**, 1503–1532 (2011) Zbl 1236.12003 MR 2863369

[EM2] Efrat, I., Mináč, J.: Galois groups and cohomological functors. Trans. Amer. Math. Soc., doi: 10.1090/tran/6724

[Er] Ershov, Y. L.: Free products of absolute Galois groups. Dokl. Math. **56**, 915–917 (1997) Zbl 0961.12002

[Fe] Fenn, R.: Techniques of Geometric Topology. London Math. Soc. Lecture Note Ser. 57, Cambridge Univ. Press (1983) Zbl 0517.57001 MR 0787801

[Fo] Forré, P.: Strongly free sequences and pro-p-groups of cohomological dimension 2. J. Reine Angew. Math. **658**, 173–192 (2011) Zbl 1292.12004 MR 2831517

[Frey] Frey, G.: Pseudo algebraically closed fields with nonarchimedian real valuations. J. Algebra **26**, 202–207 (1973) Zbl 0264.12105 MR 0325584

[FJ] Fried, R. D., Jarden, M.: Field Arithmetic. 3rd ed., Ergeb. Math. Grenzgeb. 11, Springer, Berlin (2008) Zbl 1145.12001 MR 2445111

[GLMS] Gao, W., Leep, D., Mináč, J., Smith, T. L.: Galois groups over nonrigid fields. In: Valuation Theory and its Applications, Vol. II (Saskatoon, SK, 1999), Fields Inst. Comm. 33, Amer. Math. Soc., Providence, RI, 61–77 (2003) Zbl 1049.12004 MR 2018550

[Gä] Gärtner, J.: Higher Massey products in the cohomology of mild pro-p-groups. J. Algebra **422**, 788–820 (2015) Zbl 1329.20066 MR 3272101

[GMTT] Gärtner, J., Mináč, J., Tân, N. D., Topaz, A.: Triple Massey products and Galois theory II. In preparation

[HJP] Haran, D., Jarden, M., Pop, F.: Projective group structures as absolute Galois structures with block approximation. Mem. Amer. Math. Soc. **189**, no. 884, 56 pp. (2007) Zbl 1129.12006 MR 2340100

[HW] Hopkins, M., Wickelgren, K.: Splitting varieties for triple Massey products. J. Pure Appl. Algebra **219**, 1304–1319 (2015) Zbl 1323.55014 MR 3299685

[I] Iwasawa, K.: On Galois groups of local fields. Trans. Amer. Math. Soc. **80**, 448–469 (1955) Zbl 0074.03101 MR 0075239

[JW] Jacob, B., Ware, R.: A recursive description of the maximal pro-2 Galois group via Witt rings. Math. Z. **200**, 379–396 (1989) Zbl 0663.12018 MR 0978598

[JaWi] Jannsen, U., Wingberg, K.: Die Struktur der absoluten Galoisgruppe $\mathfrak{p}$-adischer Zahlkörper. Invent. Math. **70**, 71–78 (1982) Zbl 0534.12010 MR 0679774

[Ko1] Koch, H.: Über Galoissche Gruppen von $\mathfrak{p}$-adischen Zahlkörpern. Math. Nachr. **29**, 77–111 (1965) Zbl 0128.26401 MR 0177982

[Ko2] Koch, H.: Galois Theory of p-extensions. Springer Monogr. Math., Springer (2001) Zbl 1023.11002 MR 1930372

[Koe1] Koenigsmann, J.: Solvable absolute Galois groups are metabelian. Invent. Math. **144**, 1–22 (2001) Zbl 1016.12005 MR 1821143

[Koe2] Koenigsmann, J.: Relatively projective groups as absolute Galois groups. Israel J. Math. **127**, 93–129 (2002) Zbl 1006.12003 MR 1900696

[Kra] Kraines, D.: Massey higher products. Trans. Amer. Math. Soc. **124**, 431–449 (1996) Zbl 0146.19201 MR 0202136

[La] Labute, J.: Classification of Demushkin groups. Canad. J. Math. **19**, 106–132 (1966) Zbl 0153.04202 MR 0210788

[LLMS] Labute, J., Lemire, N., Mináč, J., Swallow, J.: Demuškin groups, Galois modules, and the elementary type conjecture. J. Algebra **304**, 1130–1146 (2006) Zbl 1168.12003 MR 2265509

[LM] Labute, J., Mináč, J.: Mild pro-2-groups and 2-extensions of $\mathbb{Q}$ with restricted ramification. J. Algebra **332**, 136–158 (2011) Zbl 1266.11117 MR 2774682

[LvdD] Lubotzky, A., van den Dries, L.: Subgroups of free profinite groups and large subfields of $\tilde{\mathbb{Q}}$. Israel J. Math. **39**, 25–45 (1981) Zbl 0485.20021 MR 0617288

[Mar] Marshall, M.: The elementary type conjecture in quadratic form theory. In: Algebraic and Arithmetic Theory of Quadratic Forms, Contemp. Math. 344, Amer. Math. Soc., Providence, RI, 275–293 (2004) Zbl 1143.11315 MR 2060204

[May] May, J. P.: Matric Massey products. J. Algebra **12**, 533–568 (1969) Zbl 0192.34302 MR 0238929

[MeSu] Merkurjev, A. S., Suslin, A. A.: K-cohomology of Severi–Brauer varieties and the norm residue homomorphism. Math. USSR Izv. **21**, 307–340 (1983) Zbl 0525.18008 MR 0675529

[MS1] Mináč, J., Spira, M.: Formally real fields, Pythagorean fields, C-fields and W-groups. Math. Z. **205**, 519–530 (1990) Zbl 0692.12005 MR 1082872

[MS2] Mináč, J., Spira, M.: Witt rings and Galois groups. Ann. of Math. (2) **144**, 35–60 (1996) Zbl 0861.11030 MR 1405942

[MST] Mináč, J., Swallow, J., Topaz, A.: Galois module structure of (ℓ^n)th classes of fields. Bull. London Math. Soc. **46**, 143–154 (2014) Zbl 1301.12003 MR 3161770

[MTE] Mináč, J., Tân, N. D.: The Kernel Unipotent Conjecture and Massey products on an odd rigid field (with an appendix by I. Efrat. J. Mináč and N. D. Tân), Adv. Math. **273**, 242–270 (2015) Zbl 1334.12005 MR 3311763

[MT1] Mináč, J., Tân, N. D.: Triple Massey products over global fields. Doc. Math. **20**, 1467–1480 (2015) Zbl 06572186 MR 3452187

[MT2] Mináč, J., Tân, N. D.: The Kernel Unipotent Conjecture in Galois theory. In preparation

[Mor] Morishita, M.: Milnor invariants and Massey products for prime numbers. Compos. Math. **140**, 69–83 (2004) Zbl 1066.11048 MR 2004124

[NSW] Neukirch, J., Schmidt, A., Wingberg, K.: Cohomology of Number Fields. 2nd ed., Grundlehren Math. Wiss. 323, Springer, Berlin (2008) Zbl 0948.11001 MR 2392026

[Pop] Pop, F.: On the birational anabelian program initiated by Bogomolov I. Invent. Math. **187**, 511–533 (2012) Zbl 1239.14025 MR 2891876

[Se1] Serre, J.-P.: Structures de certains pro-p-groupes (d'après Demuškin). Sém. Bourbaki, exp. 252 (1962/63) MR 1611538

[Se2] Serre, J.-P.: Local Fields. Grad. Texts in Math. 67, Springer, New York (1979) Zbl 0423.12016 MR 0554237

[Sha] Shafarevich, I. R.: On p-extensions. Mat. Sbornik **20** (62), 351–363 (1947) (in Russian) Zbl 0041.17101 MR 0020546

[Sh] Sharifi, R.: Massey products and ideal class groups. J. Reine Angew. Math. **603**, 1–33 (2007) Zbl 1163.11077 MR 2312552

[Sri] Srinivas, V.: Algebraic K-theory. Reprint of the 1996 second edition, Modern Birkhäuser Classics, Birkhäuser Boston, Boston, MA (2008) Zbl 1125.19300 MR 2371852

[Vi] Villegas, F. R.: Relations between quadratic forms and certain Galois extensions. Ohio State Univ. (1988); http://www.math.utexas.edu/users/villegas/osu.pdf

[Voe] Voevodsky, V.: On motivic cohomology with $\mathbb{Z}/l$-coefficients. Ann. of Math. (2) **174**, 401–438 (2011) Zbl 1236.14026 MR 2811603

[Vo1] Vogel, D.: Massey products in Galois cohomology of number fields. Ph.D thesis, Univ. Heidelberg (2004) Zbl 1071.11068

[Vo2] Vogel, D.: On the Galois group of 2-extensions with restricted ramification. J. Reine Angew. Math. **581**, 117–150 (2005) Zbl 1143.11042 MR 2132673

[Wad] Wadsworth, A. R.: Merkurjev's elementary proof of Merkurjev's theorem. In: Applications of Algebraic K-theory to Algebraic Geometry and Number Theory, Parts I, II (Boulder, CO, 1983), Contemp. Math. 55, Amer. Math. Soc., Providence, RI, 741–776 (1986) Zbl 0604.16022 MR 0862663

[Wa] Ware, R.: When are Witt rings group rings? II. Pacific J. Math. **76**, 541–564 (1978) Zbl 0405.12019 MR 0568320

[Wei] Weil, A.: Review: "The Collected Papers of Emil Artin". Scripta Math. **28**, 237–238 (1967)

[Wic1] Wickelgren, K.: Lower central series obstructions to homotopy sections of curves over number fields. Ph.D. thesis, Stanford Univ. (2009) MR 2713908

[Wic2] Wickelgren, K.: n-nilpotent obstruction to π_1 sections of $\mathbb{P}^1_{\mathbb{Q}} - \{0, 1, \infty\}$ and Massey products. In: Galois Teichmüller Theory and Arithmetic Geometry (Kyoto, 2010), H. Nakamura et al. (eds.), Adv. Stud. Pure Math. 63, Math. Soc. Japan, 579–600 (2012) Zbl 1321.11116 MR 3051256

[Wi] Witt, E.: Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f. J. Reine Angew. Math. **174**, 237–245 (1936) Zbl 0013.19601