

MASSEY PRODUCTS IN GALOIS COHOMOLOGY AND PYTHAGOREAN FIELDS

CLAUDIO QUADRELLI

ABSTRACT. We prove that a strengthened version of Minač–Tân’s Massey Vanishing Conjecture holds true for fields with a finite number of square classes whose maximal pro-2 Galois group is of elementary type (as defined by I. Efrat). In particular, this proves Minač–Tân’s Massey Vanishing Conjecture for Pythagorean fields with a finite number of square classes and their finite extensions.

1. INTRODUCTION

One of the topics which gained great interest in Galois theory, in recent years, is the study of *Massey products* in Galois cohomology. Let G be a pro- p group — where p is a prime number —, and let \mathbb{F}_p denote the finite field with p elements considered as a trivial G -module. For $n \geq 2$, the n -fold *Massey product* with respect to \mathbb{F}_p is a multi-valued map from the first \mathbb{F}_p -cohomology group $H^1(G, \mathbb{F}_p)$ to the second \mathbb{F}_p -cohomology group $H^2(G, \mathbb{F}_p)$: namely, it associates a sequence of length n of elements $\alpha_1, \dots, \alpha_n$ (non-necessarily all distinct to each other) of $H^1(G, \mathbb{F}_p)$ to a (possibly empty) subset of $H^2(G, \mathbb{F}_p)$, denoted by $\langle \alpha_1, \dots, \alpha_n \rangle$.

Given a sequence $\alpha_1, \dots, \alpha_n$ of elements of $H^1(G, \mathbb{F}_p)$, the associated n -fold Massey product $\langle \alpha_1, \dots, \alpha_n \rangle$ is said to be *defined* if it is not the empty set, and moreover it is said to *vanish* if $0 \in \langle \alpha_1, \dots, \alpha_n \rangle$. A pro- p group is said to have the *n -Massey vanishing property* with respect to \mathbb{F}_p if, for any sequence $\alpha_1, \dots, \alpha_n$ of elements of $H^1(G, \mathbb{F}_p)$, the n -fold Massey product $\langle \alpha_1, \dots, \alpha_n \rangle$ vanishes whenever it is defined.

Given a field \mathbb{K} , let $G_{\mathbb{K}}(p)$ denote the *maximal pro- p Galois group* of \mathbb{K} — namely, $G_{\mathbb{K}}(p)$ is the maximal pro- p quotient of the absolute Galois group of \mathbb{K} . The recent hectic research on Massey products in Galois cohomology started with the paper [20], where M.J. Hopkins and K.G. Wickelgren proved that if \mathbb{K} is a global field of characteristic not 2, then its maximal pro-2 Galois group $G_{\mathbb{K}}(2)$ has the 3-Massey vanishing property, and asked whether this is true for any field of characteristic not 2.

Subsequently, J. Minač and N.D. Tân conjectured the following (cf. [35]).

Conjecture 1.1. *Let \mathbb{K} be a field containing a root of 1 of order p . Then the maximal pro- p Galois group $G_{\mathbb{K}}(p)$ of \mathbb{K} satisfies the n -Massey vanishing property for every $n > 2$.*

In the meanwhile, the following remarkable results have been obtained: E. Matzri proved that $G_{\mathbb{K}}(p)$ has the 3-Massey vanishing property if \mathbb{K} contains a root of 1 of order

Date: February 23, 2024.

2010 Mathematics Subject Classification. Primary 12G05; Secondary 20E18, 20J06, 12F10.

Key words and phrases. Galois cohomology, Massey products, Pythagorean fields, absolute Galois groups, elementary type conjecture.

p (see the preprint [28], see also the published works [11, 37]); J. Minač and N.D. Tân proved Conjecture 1.1 for local fields (see [39]); Y. Harpaz and O. Wittenberg proved Conjecture 1.1 for number fields (see [19]); A. Merkurjev and F. Scavia proved that the maximal pro-2 Galois group of every field satisfies the 4-Massey vanishing property (see [31]). Further interesting results on Massey products in Galois cohomology have been obtained by various authors (see, e.g., [16–18, 26, 29, 30, 51]). For an overview on Massey products in Galois cohomology, we direct the reader to [39].

In this work, we focus on a strong version of the Massey vanishing property, introduced by A. Pál and E. Szábo in [42]. If the n -fold Massey product $\langle \alpha_1, \dots, \alpha_n \rangle$, associated to a sequence $\alpha_1, \dots, \alpha_n$ of elements of the first \mathbb{F}_p -cohomology group of a pro- p group G , is defined, then necessarily one has

$$(1.1) \quad \alpha_1 \smile \alpha_2 = \dots = \alpha_{n-1} \smile \alpha_n = 0,$$

where \smile denotes the *cup-product* (see, e.g., [43, Rem. 2.2]). A pro- p group G is said to have the *strong n -Massey vanishing property* if every sequence $\alpha_1, \dots, \alpha_n$ of elements of $H^1(G, \mathbb{F}_p)$ satisfying (1.1) yields an n -fold Massey product $\langle \alpha_1, \dots, \alpha_n \rangle$ which vanishes.

It has been show by A. Pál and G. Quick that the maximal pro-2 Galois group of a field with virtual cohomological dimension at most 1 satisfies the strong n -Massey vanishing property with respect to \mathbb{F}_2 for every $n > 2$ (see [41]). Our main result is to show that the same holds for *Pythagorean fields*.

Theorem 1.2. *Let \mathbb{K} be a Pythagorean field with finitely many square classes, and let \mathbb{L}/\mathbb{K} be an extension of finite degree. Then the maximal pro-2 Galois group $G_{\mathbb{L}}(2)$ of \mathbb{L} satisfies the strong n -Massey vanishing property with respect to \mathbb{F}_2 for every $n > 2$.*

Recall that a field is said to be *Pythagorean* if any sum of two squares is a square. Equivalently, a field \mathbb{K} is Pythagorean if, and only if, its Witt ring $W(\mathbb{K})$ is torsion free as an additive abelian group. Pythagorean fields play an important role in the study of quadratic forms (see, e.g., [14, 21, 22]).

The proof of Theorem 1.2 relies on the description of the maximal pro-2 Galois group of a Pythagorean fields with finitely many square classes provided by J. Minač in [33]: namely, the maximal pro-2 Galois group of such a field may be constructed starting from cyclic groups of order 2 and iterating a finite number of times free pro-2 products and semidirect products with free abelian pro-2 groups with action given by inversion (see also [34, § 6.2]).

Such pro-2 groups constitute a subfamily of the family of pro-2 groups of *elementary type*. For an arbitrary prime p , the family of pro- p groups of elementary type (introduced by I. Efrat, see [7]) is the family of finitely generated pro- p groups which may be constructed starting from free pro- p groups and *Demushkin* pro- p groups (which include the cyclic group of order 2 if $p = 2$) and iterating free pro- p products and certain semidirect products with \mathbb{Z}_p (see Definition 3.4 below for the detailed definition). In fact, we prove the following more general result.

Theorem 1.3. *Let G be a pro-2 group of elementary type. Then every open subgroup H of G has the strong n -Massey vanishing property with respect to \mathbb{F}_2 for every $n > 2$.*

By the work of J. Minač on the maximal pro-2 Galois group of Pythagorean fields, Theorem 1.3 implies Theorem 1.2. The proof of Theorem 1.3 uses a result — whose original formulation, for discrete groups, is due to W. Dwyer, see [4] — which interprets the vanishing of Massey products in the \mathbb{F}_p -cohomology of a pro- p group G in terms of the existence of certain upper unitriangular representations of G .

Theorem 1.3 was proved by the author for every prime p in [43], but with restrictions for the case $p = 2$ — for example, excluding cyclic groups of order 2 among the “building bricks” of pro-2 groups of elementary type, and thus excluding maximal pro-2 groups of Pythagorean fields. Therefore, Theorem 1.3 — where such restrictions are dropped — is complementary to [43, Thm. 1.2].

In the '90s, I. Efrat formulated the *Elementary Type Conjecture* on maximal pro- p Galois groups, which predicts that if \mathbb{K} is a field containing a root of 1 of order p and $G_{\mathbb{K}}(p)$ is finitely generated, then $G_{\mathbb{K}}(p)$ is of elementary type, see [5]. This is known to be true, for example, if \mathbb{K} is an extension of relative transcendence degree 1 of a pseudo algebraically closed field (see [15, Ch. 11] and [8, § 5]); or if \mathbb{K} is an algebraic extension of a global field of characteristic not p (see [6]); see also Proposition 3.9 below. Hence, Theorem 1.3 implies the following.

Corollary 1.4. *Let \mathbb{K} be one of the following:*

- (a) *a local field, or an extension of transcendence degree 1 of a local field;*
- (b) *a pseudo algebraically closed (PAC) field, or an extension of relative transcendence degree 1 of a PAC field;*
- (c) *a 2-rigid field (for the definition of p -rigid fields see [50, p. 722]);*
- (d) *an algebraic extension of a global field of characteristic not p ;*
- (e) *a valued 2-Henselian field with residue field κ , and $G_{\kappa}(2)$ satisfies the strong n -Massey vanishing property for every $n > 2$.*

Suppose further that \mathbb{K} has a finite number of square classes. Then $G_{\mathbb{L}}(2)$ has the strong n -Massey vanishing property for every $n > 2$, for any finite extension \mathbb{L}/\mathbb{K} .

Analogously to Theorem 1.3, Corollary 1.4 has been proved by the author for every prime p , but with the further assumption that $\sqrt{-1} \in \mathbb{K}$ if $p = 2$ (see [43, Cor. 1.3]), which is dropped here. So, Corollary 1.4 is complementary to [43, Cor. 1.3].

Acknowledgments. The author wishes to thank I. Efrat, E. Matzri, J. Minač, F.W. Pasini, and N.D. Tân, for several inspiring discussions on Massey products in Galois cohomology and pro- p groups of elementary type, which occurred in the past years; and the anonymous referee for the helpful comments.

2. PRELIMINARIES

Given an arbitrary group Γ , and two elements $g, h \in \Gamma$, we use the following notation:

$${}^g h = ghg^{-1} \quad \text{and} \quad [g, h] = {}^g h \cdot h^{-1} = ghg^{-1}h^{-1}.$$

Henceforth, given a pro-2 group G subgroups will be implicitly assumed to be closed with respect to the pro-2 topology, and generators are to be intended in the topological sense.

2.1. \mathbb{F}_p -cohomology of pro- p groups. Given a pro- p group G , consider \mathbb{F}_p as a trivial G -module. Here we recall some basic facts on \mathbb{F}_p -cohomology of pro- p groups, which will be used throughout the paper. As references for \mathbb{F}_p -cohomology of pro- p groups, we direct the reader to [47, Ch. I, § 4] and to [40, Ch. I and Ch. III, § 3].

Henceforth, $H^s(G)$ will denote the s -th \mathbb{F}_p -cohomology group of G . For the first \mathbb{F}_p -cohomology group one has

$$(2.1) \quad H^1(G) = \text{Hom}(G, \mathbb{F}_p) = (G/G^p[G, G])^*,$$

where the middle term is the \mathbb{F}_p -vector space of the homomorphisms of pro- p groups $G \rightarrow \mathbb{F}_p$, while in the right-side term $G^p[G, G]$ denotes the Frattini subgroup of G , namely, the subgroup of G generated by $\{x^p[y, z] \mid x, y, z \in G\}$, and $_*$ denotes the \mathbb{F}_p -dual space (cf. [47, Ch. I, § 4.2]).

In particular, if G is finitely generated, and $\mathcal{X} = \{x_1, \dots, x_d\}$ is a minimal generating set of G , then

$$\mathcal{B} = \{ \chi_1, \dots, \chi_d \in H^1(G) \mid \chi_h(x_k) = \delta_{hk} \text{ for } h, k = 1, \dots, d \}$$

is a basis of $H^1(G)$, and it is said to be the basis dual to \mathcal{X} .

The cup-product is a bilinear map

$$H^s(G) \times H^t(G) \xrightarrow{\smile} H^{s+t}(G), \quad s, t \geq 0,$$

and it is skew-symmetric, i.e., $\beta \smile \alpha = (-1)^{st} \alpha \smile \beta$ for all $\alpha \in H^s(G)$ and $\beta \in H^t(G)$ (cf. [40, Prop. 1.4.4]). Thus, in case $p = 2$ the cup-product is symmetric, and for $\alpha \in H^1(G, \mathbb{F}_2)$ we write $\alpha^2 = \alpha \smile \alpha$. One has the following (cf. [12, Lemma 2.4]).

Lemma 2.1. *Let G be a pro-2 group. Given $\alpha \in H^1(G)$, one has $\alpha^2 = 0$ if, and only if, there exists a homomorphism of pro-2 groups $\tilde{\alpha}: G \rightarrow \mathbb{Z}/4$ such that the diagram*

$$\begin{array}{ccc} & G & \\ \tilde{\alpha} \swarrow & & \downarrow \alpha \\ \mathbb{Z}/4 & \xrightarrow{\pi} & \mathbb{F}_2 \end{array}$$

commutes (here $\pi: \mathbb{Z}/4 \rightarrow \mathbb{F}_2$ denotes the canonical projection).

Remark 2.2. Let \mathbb{K} be a field containing a root of 1 of order p , and let \mathbb{K}^\times denote its multiplicative group. By Kummer theory, one has an isomorphism of \mathbb{F}_p -vector spaces

$$\mathbb{K}^\times / (\mathbb{K}^\times)^p \simeq H^1(G_{\mathbb{K}}(p))$$

(cf., e.g., [47, Ch. I, § 1.2, Rem. 2]). In particular, if $p = 2$ then $G_{\mathbb{K}}(2)$ is finitely generated if, and only if, \mathbb{K} has a finite number of square classes.

Now assume that G has a minimal presentation

$$(2.2) \quad G = \langle x_1, \dots, x_d \mid r_1 = \dots = r_m = 1 \rangle$$

(for the definition of a presentation, and of a minimal presentation, of a pro- p group see, e.g., [3, § 4.6 and p. 311]). Then the number of defining relations m is equal to the dimension of $H^2(G)$ (cf. [47, Ch. I, § 4.3]).

Moreover, for $p = 2$ one has the following result (which is a special case of [40, Prop. 3.9.13]), which connects the behavior of the cup-product and the shape of the defining relations.

Proposition 2.3. *Let G be a pro-2 group with minimal presentation (2.2), yielding the dual basis $\{\chi_1, \dots, \chi_d\}$ of $H^1(G)$, and suppose that for each defining relation r_l , $l = 1, \dots, m$, one has*

$$r_l \equiv \prod_{1 \leq h < h'} [x_h, x_{h'}]^{a(l)_{h,h'}} \cdot \prod_{1 \leq k \leq d} x_k^{2b(l)_k} \pmod{G^4[G^2, G^2]},$$

for some $a(l)_{h,h'}, b(l)_k \in \mathbb{F}_2$ — here $G^4[G^2, G^2]$ denotes the subgroup generated by $\{x^4[y, z] \mid x \in G, y, z \in G^2\}$. Then for each $l = 1, \dots, m$ there is a linear form $\text{tr}_l: H^2(G, \mathbb{F}_2) \rightarrow \mathbb{F}_2$ such that

$$\text{tr}_l(\chi_h \smile \chi_{h'}) = \begin{cases} a(l)_{h,h'} & \text{if } h < h' \\ b(l)_h & \text{if } h = h', \end{cases}$$

for all $1 \leq h \leq h' \leq d$.

2.2. Massey products and upper unitriangular matrices. For a survey on Massey products in Galois cohomology we direct the reader to [48], [39], or [43]. Throughout the paper, we will need only the “translation” of Massey products in terms of unipotent representations, recalled here below.

For $n \geq 2$ let

$$\mathbb{U}_{n+1} = \left\{ \left(\begin{array}{cccc} 1 & a_{1,2} & \cdots & a_{1,n+1} \\ & 1 & a_{2,3} & \cdots \\ & & \ddots & \ddots \\ & & & 1 & a_{n,n+1} \\ & & & & 1 \end{array} \right) \mid a_{i,j} \in \mathbb{F}_p \right\} \subseteq \text{GL}_{n+1}(\mathbb{F}_p)$$

be the group of unipotent upper-triangular $(n+1) \times (n+1)$ -matrices over \mathbb{F}_p . Let I_{n+1} denote the $(n+1) \times (n+1)$ identity matrix, and for $1 \leq i < j \leq n+1$, let E_{ij} denote the $(n+1) \times (n+1)$ -matrix with 1 at the entry (i, j) , and 0 elsewhere.

Now let G be a pro- p group. For a homomorphism of pro- p groups $\rho: G \rightarrow \mathbb{U}_{n+1}$, and for $1 \leq i \leq n$, let $\rho_{i,i+1}$ denote the projection of ρ on the $(i, i+1)$ -entry. Observe that $\rho_{i,i+1}: G \rightarrow \mathbb{F}_p$ is a homomorphism of pro- p groups, and thus we may consider $\rho_{i,i+1}$ as an element of $H^1(G, \mathbb{F}_p)$. One has the following “pro- p translation” of Dwyer’s result on Massey products (cf., e.g., [9, § 8]).

Proposition 2.4. *Let G be a pro- p group and let $\alpha_1, \dots, \alpha_n$ be a sequence of elements of $H^1(G, \mathbb{F}_p)$, with $n \geq 2$. The n -fold Massey product $\langle \alpha_1, \dots, \alpha_n \rangle$ vanishes if, and only if, there exists a continuous homomorphism $\rho: G \rightarrow \mathbb{U}_{n+1}$ such that $\rho_{i,i+1} = \alpha_i$ for every $i = 1, \dots, n$.*

Employing Proposition 2.4, and the universal properties of free pro- p groups and free pro- p products of pro- p groups respectively, it is fairly easy to prove the following (cf., e.g., [39, Ex. 4.1] and [1, Th. 5.1]; for the definition of free pro- p product of pro- p groups see, e.g., [45, § 9.1]).

Proposition 2.5. (i) *A free pro- p group has the strong n -Massey vanishing property for every $n > 2$.*

(ii) *Let G_1, G_2 be two pro- p groups with the the strong n -Massey vanishing property for every $n > 2$. Then also the free pro- p product $G_1 * G_2$ has the strong n -Massey vanishing property for every $n > 2$.*

Remark 2.6. If a field \mathbb{K} has characteristic equal to 2, then the maximal pro-2 Galois group $G_{\mathbb{K}}(2)$ is a free pro-2 group (cf., e.g., [40, Thm. 6.1.4]), and thus it has the strong n -Massey vanishing property for every $n > 2$ by Proposition 2.5. So, henceforth we may always tacitly assume that every field we deal with has characteristic not 2.

Proposition 2.4 is also useful to show that, in order to check that a pro- p group satisfies the strong n -Massey vanishing property, it suffices to verify that every sequence of length at most n of *non-trivial* cohomology elements of degree 1 whose cup-products satisfy the triviality condition (1.1) yields a Massey product containing 0, as stated by the following (cf. [43, Prop. 2.8]).

Proposition 2.7. *Given $N > 2$, a pro- p group G satisfies the strong n -Massey vanishing property for every $3 \leq n \leq N$ if, and only if, for every $3 \leq n \leq N$, every sequence $\alpha_1, \dots, \alpha_n$ of non-trivial elements of $H^1(G)$ satisfying the triviality condition (1.1) yields an n -fold Massey product containing 0.*

Now fix $n \geq 2$. Here we will write \mathbb{U} instead of \mathbb{U}_{n+1} , and I instead of I_{n+1} . For every $k \geq 1$ let $\mathbb{U}_{(k)}$ denote the k -th term of the descending central series of \mathbb{U} : namely, $\mathbb{U}_{(k)}$ is the subgroup of \mathbb{U} whose elements have (i, j) -entries equal to 0 if $0 < j - i < k$. For example,

$$\mathbb{U}_{(1)} = \mathbb{U} \quad \text{and} \quad \mathbb{U}_{(n)} = \{ I + E_{1,n+1}a \mid a \in \mathbb{F}_p \},$$

while $\mathbb{U}_{(k)}$ is the trivial subgroup if $k > n$.

From [43, Prop. 2.10] one deduces the following.

Lemma 2.8. *Let $A = (a_{i,j}) \in \mathbb{U}$ a matrix such that $a_{1,2} = a_{2,3} = \dots = a_{n,n+1} = 1$. For every $\mu \in \mathbb{Z}_2$ multiple of 4, there exists a matrix $C(\mu) \in \mathbb{U}_{(3)}$ such that*

$$(2.3) \quad [C(\mu), A] = A^\mu.$$

Proof. First, we observe that the order of A is a power of 2 with exponent at least 2, as \mathbb{U} is a finite 2-group, and $A^2 \neq I$ as $n \geq 3$.

Since the $(i, i+1)$ - and $(i, i+2)$ -entries of A^4 are 0, A^μ lies in the subgroup $\mathbb{U}_{(4)}$. Then by [43, Prop. 2.10] there exists a matrix $C(\mu) \in \mathbb{U}_{(4-1)}$ satisfying (2.3). \square

3. ORIENTED PRO- p GROUPS

3.1. Orientations of pro- p groups. Let

$$1 + p\mathbb{Z}_p = \{ 1 + p\lambda \mid \lambda \in \mathbb{Z}_p \}$$

be the multiplicative group of principal units of \mathbb{Z}_p . Recall that for $p = 2$ one has

$$1 + 2\mathbb{Z}_2 = \{\pm 1\} \times (1 + 4\mathbb{Z}_2) \simeq (\mathbb{Z}/2) \times \mathbb{Z}_2,$$

where the right-side isomorphism is an isomorphism of abelian pro-2 groups. A homomorphism of pro- p groups $\theta: G \rightarrow 1 + p\mathbb{Z}_p$ is called an *orientation*, and the pair (G, θ) is called an *oriented pro- p group* (cf. [44]).

The most important example of oriented pro- p groups comes from Galois theory.

Example 3.1. Let \mathbb{K} be a field containing a root of 1 of order p . If ζ is a root of 1 of order a power of p lying in the separable closure of \mathbb{K} , then ζ lies also in the maximal pro- p -extension of \mathbb{K} , whose Galois group is the maximal pro- p Galois group $G_{\mathbb{K}}(p)$. The pro- p group $G_{\mathbb{K}}(p)$ may be endowed with a natural orientation, the *p -cyclotomic character* $\theta_{\mathbb{K}}: G_{\mathbb{K}}(p) \rightarrow 1 + p\mathbb{Z}_p$, satisfying

$$g(\zeta) = \zeta^{\theta_{\mathbb{K}}(g)} \quad \forall g \in G_{\mathbb{K}}(p)$$

(cf. [13, § 4]). The image of $\theta_{\mathbb{K}}$ is $1 + p^f\mathbb{Z}_p$, where f is the maximal positive integer such that \mathbb{K} contains the roots of 1 of order p^f — if such a number does not exist, i.e., if \mathbb{K} contains all roots of 1 of p -power order, then $\text{Im}(\theta_{\mathbb{K}}) = \{1\}$, and one sets $f = \infty$. Observe that if $p = 2$ then $\text{Im}(\theta_{\mathbb{K}}) \subseteq 1 + 4\mathbb{Z}_2$ if $\sqrt{-1} \in \mathbb{K}$; on the other hand $\text{Im}(\theta_{\mathbb{K}}) = \{\pm 1\}$ if $\sqrt{-1} \notin \mathbb{K}$ and $\mathbb{K}(\sqrt{-1})$ contains all roots of 1 of order a power of 2.

From now on, given an orientation $\theta: G \rightarrow 1 + p\mathbb{Z}_p$ of a pro- p group G , the notation $\text{Im}(\theta) = 1 + p^\infty\mathbb{Z}_p$ will mean that the image of θ is trivial.

In the family of oriented pro- p groups one has the following two constructions (cf. [7, § 3]).

- (a) Let (G_0, θ) be an oriented pro-2 group, and let Z be a free abelian pro-2 group. The *semidirect product* $(Z \rtimes_{\theta} G_0, \tilde{\theta})$ is the oriented pro- p group where $Z \rtimes_{\theta} G_0$ is the semidirect product of pro- p groups with action $gzg^{-1} = z^{\theta(g)}$ for every $g \in G_0$ and $z \in Z$, and where

$$\tilde{\theta}: Z \rtimes_{\theta} G_0 \longrightarrow 1 + p\mathbb{Z}_p$$

is the orientation induced by θ , i.e., $\tilde{\theta} = \theta \circ \pi$, where $\pi: Z \rtimes_{\theta} G_0 \rightarrow G_0$ is the canonical projection.

- (b) Let $(G_1, \theta_1), (G_2, \theta_2)$ be two oriented pro- p groups. The *free product* $(G_1 * G_2, \theta)$ is the oriented pro- p group, while

$$\theta: G_1 * G_2 \longrightarrow 1 + p\mathbb{Z}_p$$

is the orientation induced by the orientations θ_1, θ_2 via the universal property of the free pro- p product.

3.2. Demushkin pro-2 groups and orientations. Another important source of oriented pro- p groups are Demushkin pro- p groups. A Demushkin group G is a pro- p group whose \mathbb{F}_p -cohomology algebra satisfies the following three conditions:

- (i) the dimension of $H^1(G)$ is finite, i.e., G is finitely generated;
- (ii) the dimension of $H^2(G)$ is one, i.e., G has one defining relation;
- (iii) the cup-product induces a non-degenerate pairing

$$H^1(G) \times H^1(G) \xrightarrow{\smile} H^2(G)$$

(cf., e.g., [40, Def. 3.9.9]). Demushkin groups have been studied and classified by S.P. Demuškin, J-P. Serre and J.P. Labute (cf. [2, 24, 46]). In particular, Serre proved that every Demushkin group may be endowed with a canonical orientation $\theta_G: G \rightarrow 1 + p\mathbb{Z}_p$.

By condition (ii) above, a Demushkin pro- p group G has a single defining relation, namely,

$$(3.1) \quad G = \langle x_1, \dots, x_d \mid r = 1 \rangle, \quad d = \dim(\mathrm{H}^1(G)),$$

yielding the dual bases $\{\chi_1, \dots, \chi_d\}$ of $\mathrm{H}^1(G)$.

Henceforth we focus on Demushkin pro-2 groups. Altogether, one has four cases, depending on whether d is even or odd, and on the shape of the defining relation r (cf. [24]).

3.2.1. *First case:* $\mathrm{Im}(\theta) \subseteq 1 + 4\mathbb{Z}_2$. The number d is even and the defining relation is

$$r = [x_1, x_2]x_2^{-2^f} [x_3, x_4] \cdots [x_{d-1}, x_d],$$

for some $f \in \{2, 3, 4, \dots, \infty\}$. The canonical orientation $\theta_G: G \rightarrow 1 + 2\mathbb{Z}_2$ is defined by

$$\theta_G(x_1) = 1 + 2^f \quad \text{and} \quad \theta_G(x_h) = 1 \text{ for } h = 2, \dots, d;$$

thus $\mathrm{Im}(\theta_G) = 1 + 2^f\mathbb{Z}_2$. This is the only case with $\mathrm{Im}(\theta_G) \subseteq 1 + 4\mathbb{Z}_2$, and the only case of Demushkin pro-2 groups taken into consideration in [43].

Moreover, $\mathrm{H}^2(G)$ is generated by χ_1^2 , and one has the relations

$$\chi_1^2 = \chi_2 \smile \chi_3 = \dots = \chi_{d-1} \smile \chi_d$$

and $\chi_h \smile \chi_{h'} = 0$ for any other pair (h, h') , with $h \leq h'$, different to $(1, 2)$, $(3, 4)$, \dots , $(d-1, d)$.

Remark 3.2. Usually the defining relations of a Demushkin pro- p group are described adopting the convention $[x, y] = x^{-1}y^{-1}xy$ (this is the case, for example, of [24] and [40, Ch. III, § 9]). According to the aforementioned convention, the defining relation of this case reads

$$r = x_2^{2^f} [x_2, x_1][x_4, x_3] \cdots [x_d, x_{d-1}],$$

and analogously for the next cases.

3.2.2. *Second case:* $-1 \in \mathrm{Im}(\theta)$, d even. The number d is even and the defining relation is

$$r = [x_1, x_2]x_2^2 [x_3, x_4]x_4^{-2^f} [x_5, x_6] \cdots [x_{d-1}, x_d],$$

for some $f \in \{2, 3, 4, \dots, \infty\}$. The canonical orientation $\theta_G: G \rightarrow 1 + 2\mathbb{Z}_2$ is defined by

$$\theta_G(x_1) = -1, \quad \theta_G(x_3) = 1 + 2^f, \quad \text{and} \quad \theta_G(x_h) = 1 \text{ for } h = 2, 4, \dots, d;$$

thus $\mathrm{Im}(\theta_G) = \{\pm 1\} \times (1 + 2^f\mathbb{Z}_2)$.

Moreover, $\mathrm{H}^2(G)$ is generated by $\chi_1 \smile \chi_2$, and one has the relations

$$\chi_1 \smile \chi_2 = \chi_2^2 = \chi_3 \smile \chi_4 = \chi_5 \smile \chi_6 = \dots = \chi_{d-1} \smile \chi_d$$

and $\chi_h \smile \chi_{h'} = 0$ for any other pair (h, h') , with $h \leq h'$, different to $(1, 2)$, $(2, 2)$, $(3, 4)$, \dots , $(d-1, d)$.

3.2.3. *Third case:* $\text{Im}(\theta) = \langle -1 + 2^f \rangle$. The number d is even and the defining relation is

$$r = [x_1, x_2]x_2^{2-2^f}[x_3, x_4] \cdots [x_{d-1}, x_d],$$

for some $f \in \{2, 3, 4, \dots, \infty\}$. The canonical orientation $\theta_G: G \rightarrow 1 + 2\mathbb{Z}_2$ is defined by

$$\theta_G(x_1) = -1 + 2^f \quad \text{and} \quad \theta_G(x_h) = 1 \text{ for } h = 2, \dots, d;$$

thus $\text{Im}(\theta_G) = \langle -1 + 2^f \rangle \simeq \mathbb{Z}_2$.

Moreover, $H^2(G)$ is generated by $\chi_1 \smile \chi_2$, and one has the relations

$$\chi_1 \smile \chi_2 = \chi_2^2 = \chi_3 \smile \chi_4 = \dots = \chi_{d-1} \smile \chi_d$$

and $\chi_h \smile \chi_{h'} = 0$ for any other pair (h, h') , with $h \leq h'$, different to $(1, 2)$, $(2, 2)$, $(3, 4)$, \dots , $(d-1, d)$.

3.2.4. *Fourth case: d odd.* The number d is odd and the defining relation is

$$r = x_1^2[x_2, x_3]x_3^{-2^f}[x_4, x_5] \cdots [x_{d-1}, x_d],$$

for some $f \in \{2, 3, 4, \dots, \infty\}$. Observe that if $d = 1$ then G is a cyclic group of order 2 (in this case we set implicitly $f = \infty$). The canonical orientation $\theta_G: G \rightarrow 1 + 2\mathbb{Z}_2$ is defined by

$$\theta_G(x_1) = -1, \quad \theta_G(x_2) = 1 + 2^f, \quad \text{and} \quad \theta_G(x_h) = 1 \text{ for } h = 3, \dots, d;$$

thus $\text{Im}(\theta_G) = \{\pm 1\} \times (1 + 2^f\mathbb{Z}_2)$.

Moreover, $H^2(G)$ is generated by $\chi_1 \smile \chi_2$, and one has the relations

$$\chi_1^2 = \chi_2 \smile \chi_3 = \chi_4 \smile \chi_5 = \dots = \chi_{d-1} \smile \chi_d$$

and $\chi_h \smile \chi_{h'} = 0$ for any other pair (h, h') , with $h \leq h'$, different to $(1, 1)$, $(2, 3)$, $(4, 5)$, \dots , $(d-1, d)$.

Remark 3.3. If \mathbb{K} is an ℓ -adic local field, with ℓ an odd prime, then its maximal pro-2 Galois group $G_{\mathbb{K}}(2)$ is a 2-generated Demushkin pro-2 group (cf. [40, Prop. 7.5.9]). On the other hand, if \mathbb{K} is a 2-adic local field, then its maximal pro-2 Galois group $G_{\mathbb{K}}(2)$ is a Demushkin pro-2 group with $d = [\mathbb{K} : \mathbb{Q}_p] + 2$ generators (cf. [40, Thm. 7.5.11]). Finally, $\mathbb{Z}/2$ (which is the Demushkin pro-2 group with defining relation (d) and $d = 1$) is the maximal pro-2 Galois group of $\mathbb{K} = \mathbb{R}$. It is not known whether every Demushkin pro-2 group occurs as the maximal pro-2 Galois group of a field — for example, this is not known for

$$G = \langle x_1, x_2, x_3 \mid x_1^2[x_2, x_3] = 1 \rangle,$$

(cf. [23, Rem. 5.5], see also [43, Rem 3.3]). Yet, if a Demushkin pro-2 group does, then necessarily the canonical orientation coincides with the 2-cyclotomic character (cf. [24, Thm. 4]).

3.3. Oriented pro- p groups of elementary type. The following definition is due to I. Efrat.

Definition 3.4. The family \mathcal{E}_p of *oriented pro- p groups of elementary type* is the smallest family of oriented pro- p groups containing

- (a) every oriented pro- p group (G, θ) , where G is a finitely generated free pro- p group, and $\theta: F \rightarrow 1 + p\mathbb{Z}_p$ is arbitrary (including $G = \{1\}$),
- (b) every Demushkin pro- p group together with its canonical orientation (G, θ_G) ;

and such that

- (c) if (G_0, θ) is an oriented pro- p group of elementary type, then also the semidirect product $(\mathbb{Z}_p \rtimes_{\theta} G_0, \tilde{\theta})$, as defined in § 3.1, is in \mathcal{E}_p ,
- (d) if $(G_1, \theta_1), (G_2, \theta_2)$ are two oriented pro- p groups of elementary type, then also the free product $(G_1 * G_2, \theta)$, as defined in § 3.1, is in \mathcal{E}_p .

Remark 3.5. If (G, θ) is an oriented pro-2 group of elementary type, and H is a finitely generated subgroup of G , then also the oriented pro-2 group $(H, \theta|_H)$ is of elementary type (cf., e.g., [44, Rem. 5.10–(b)]).

Example 3.6. The oriented pro-2 group

$$(G, \theta) = \mathbb{Z}_2 \rtimes_{\theta_2} ((\mathbb{Z}_1 \rtimes_{\theta_1} ((G_1, \theta_1) * (G_2, \theta_2))) * (G_3, \theta_3))$$

— where G_1 and G_3 are Demushkin pro-2 groups,

$$G_1 = \langle x_1, x_2, x_3 \mid x_1^2[x_2, x_3] = 1 \rangle, \quad G_3 = \langle x_5, x_6 \mid [x_5, x_6]x_6^{-2} = 1 \rangle,$$

$G_2 = \langle x_4 \rangle \simeq \mathbb{Z}_2$ is free on one generator with $\theta_2(x_4) = 1 + 4$, and $Z_i = \langle z_i \rangle \simeq \mathbb{Z}_2$ — is an oriented pro-2 group of elementary type.

The Elementary Type Conjecture asks whether $(G_{\mathbb{K}}(p), \theta_{\mathbb{K}}) \in \mathcal{E}_p$ for every field \mathbb{K} containing a root of 1 of order p such that $[\mathbb{K}^{\times} : (\mathbb{K}^{\times})^p] < \infty$ (cf. [5], see also [6, Question 4.8], [27, § 10], [44, § 7.5] and [34, Conj. 4.8]).

Now let \mathcal{EE}_2 be the smallest subfamily of \mathcal{E}_2 containing the trivial group $\{1\}$ with the trivial orientation, the oriented pro-2 group (G, θ_G) with G the cyclic group of order 2 and $\theta_G: G \rightarrow \{\pm 1\}$ — namely, G is the Demushkin pro-2 group with $d = 1$ —; and closed with respect to semidirect products with \mathbb{Z}_2 , and free pro-2 groups. In other words, \mathcal{EE}_2 consists of those oriented pro-2 groups of elementary type obtained using only cyclic groups of order 2 as “building bricks”.

By the work of J. Minač [33], one has the following (see also [34, § 6.2]).

Proposition 3.7. *Let \mathbb{K} be a field with a finite number of square classes. Then \mathbb{K} is Pythagorean if, and only if, $(G_{\mathbb{K}}(2), \theta_{\mathbb{K}}) \in \mathcal{EE}_2$.*

Remark 3.8. A Pythagorean field \mathbb{K} such that $\sqrt{-1} \notin \mathbb{K}$ (and thus such that $\text{Im}(\theta_{\mathbb{K}}) \not\subseteq 1 + 4\mathbb{Z}_2$, cf. Ex. 3.1) is *formally real*. On the other hand, if $\sqrt{-1} \in \mathbb{K}$, then $(\mathbb{K}^{\times})^2 = \mathbb{K}^{\times}$ (cf. [25, p. 255]), and thus $G_{\mathbb{K}}(2)$ is trivial.

Altogether, for $p = 2$ one has the following (cf., e.g., [34, § 6]).

Proposition 3.9. *Let \mathbb{K} be a field with a finite number of square classes. Then $(G_{\mathbb{K}}(2), \theta_{\mathbb{K}}) \in \mathcal{E}_2$ in the following cases:*

- (i) \mathbb{K} is finite;
- (ii) \mathbb{K} is a PAC field, or an extension of relative transcendence degree 1 of a PAC field;
- (iii) \mathbb{K} is a local field, or an extension of transcendence degree 1 of a local field, with characteristic not p ;
- (iv) \mathbb{K} is 2-rigid (cf. [50, p. 722]);
- (v) \mathbb{K} is an algebraic extension of a global field of characteristic not 2;
- (vi) \mathbb{K} is a valued 2-Henselian field with residue field κ , and $(G_\kappa(p), \theta_\kappa) \in \mathcal{E}_2$;
- (vii) \mathbb{K} is a Pythagorean field.

4. MASSEY PRODUCTS AND PRO-2 GROUPS OF ELEMENTARY TYPE

4.1. Demushkin pro-2 groups and Massey products. A. Pál and E. Szabó proved that for every prime p , every Demushkin pro- p group satisfies the strong n -Massey vanishing property with respect to p for every $n > 2$. (cf. [42, Thm. 3.5]). Thus, for $p = 2$ one has the following.

Proposition 4.1. *Every Demushkin pro-2 group has the strong n -Massey vanishing property with respect to 2 for every $n > 2$.*

In particular, the cyclic group $G = \langle x \mid x^2 = 1 \rangle$ of order 2 — which is a Demushkin pro-2 group, cf. § 3.2.4 — has the strong n -Massey vanishing property with respect to 2 for every $n > 2$. Actually, this is easily shown using Proposition 2.4. Indeed, let $\chi: G \rightarrow \mathbb{F}_2$ the non-trivial homomorphism — i.e., $H^1(G) = \mathbb{F}_2 \cdot \chi$. Then χ^2 is not trivial by Lemma 2.1. Hence, a sequence $\alpha_1, \dots, \alpha_n$ of elements of $H^1(G)$ satisfies (1.1) if, and only if, given two consecutive terms α_i, α_{i+1} , they are not both equal to χ , namely, at least one of them is the 0-map. Hence, the matrix

$$A = I_{n+1} + \alpha_1(x)E_{1,2} + \alpha_2(x)E_{2,3} + \dots + \alpha_n(x)E_{n,n+1} \in \mathbb{U}_{n+1}$$

has order 2, and the assignment $x \mapsto A$ yields a homomorphism $\rho: G \rightarrow \mathbb{U}_{n+1}$ satisfying the properties prescribed in Proposition 2.4.

4.2. The infinite dihedral pro-2 group. Let

$$G_1 = \langle x_1 \mid x_1^2 = 1 \rangle \quad \text{and} \quad G_2 = \langle x_2 \mid x_2^2 = 1 \rangle$$

be two cyclic groups of order 2. Their free pro-2 product $G_1 * G_2$ is the *infinite dihedral pro-2 group* (i.e., the pro-2 completion of the abstract infinite dihedral group)

$$D_{2\infty} = \langle x_1, x_2 \mid x_1^2 = x_2^2 = 1 \rangle = \langle x, y \mid x^2 = [x, y]y^2 = 1 \rangle,$$

with $x = x_1$ and $y = x_1x_2$. In particular, if for $i = 1, 2$ we endow G_i with the non-trivial orientation $\theta_i: G_i \rightarrow \{\pm 1\}$, then

$$(D_{2\infty}, \theta_{D_{2\infty}}) := (G_1, \theta_1) * (G_2, \theta_2) \simeq Z \rtimes_{\theta_1} (G_1, \theta_1),$$

with $Z = \langle x_1x_2 \rangle \simeq \mathbb{Z}_2$. Thus, the oriented pro-2 group $(D_{2\infty}, \theta_{D_{2\infty}})$ is of elementary type.

Let $\{\chi_1, \chi_2\}$ and $\{\chi, \psi\}$ be the bases of $H^1(D_{2\infty})$ dual respectively to $\{x_1, x_2\}$ and to $\{x, y\}$. Then $\chi = \chi_1 + \chi_2$ and $\psi = \chi_2$. Moreover, by [40, Thm. 4.1.4] one has

$$H^2(D_{2\infty}) = H^2(G_1) \oplus H^2(G_2) = \mathbb{F}_2 \cdot \chi_1^2 \oplus \mathbb{F}_2 \cdot \chi_2^2,$$

and hence $\{\chi^2, \chi \smile \psi = \psi^2\}$ is another basis of $H^2(D_{2\infty})$.

Since both G_1, G_2 have the strong n -Massey vanishing property for every $n > 2$, by Proposition 2.5 also $D_{2\infty}$ has the strong n -Massey vanishing property for every $n > 2$. This implies the following.

Lemma 4.2. *For $n > 2$, there exist matrices $A_1, A_2, B_1, B_2 \in \mathbb{U}_{n+1}$ such that the $(i, i+1)$ -entries of both A_1 and A_2 are equal to 1, for all $i = 1, \dots, n$, and*

$$B_1 = \begin{pmatrix} 1 & 1 & & * \\ & 1 & 0 & \\ & & 1 & 1 \\ & & & 1 & 0 \\ & & & & \ddots & \ddots \\ & & & & & 1 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 1 & 0 & & * \\ & 1 & 1 & \\ & & 1 & 0 \\ & & & 1 & 1 \\ & & & & \ddots & \ddots \\ & & & & & 1 \end{pmatrix}$$

satisfying $[B_1, A_1] = A_1^{-2}$ and $[B_2, A_2] = A_2^{-2}$.

Proof. Consider the sequences $\alpha_1, \dots, \alpha_n$ and $\alpha'_1, \dots, \alpha'_n$ of elements of $H^1(D_{2\infty})$ of length n , with $\alpha_i = \alpha'_j = \chi + \psi$, for i odd and j even, and $\alpha_i = \alpha'_j = \psi$ for i even and j odd. Then both sequences satisfy (1.1), as

$$(\chi + \psi) \smile \psi = \chi \smile \psi + \psi^2 = 0.$$

Since $D_{2\infty}$ has the strong n -Massey vanishing property, by Proposition 2.4 there are two continuous homomorphisms $\rho, \rho' : D_{2\infty} \rightarrow \mathbb{U}_{n+1}$ satisfying $\rho_{i,i+1} = \alpha_i$ and $\rho'_{i,i+1} = \alpha'_i$ for all $i = 1, \dots, n$. Set $A_1 = \rho(y)$ and $A_2 = \rho'(y)$, and $B_1 = \rho(x)$ and $B_2 = \rho'(x)$. Then these matrices satisfy all the desired properties, as $[x, y] = y^{-2}$, and $\alpha_i(y) = \alpha'_i(y) = \psi(y) = 1$ for all i , while $\alpha_1(x) = \alpha'_2(x) = \chi(x) = 1$, and so on. \square

4.3. Semidirect products. The goal of this subsection is to show that if (G_0, θ_0) is an oriented pro-2 group of elementary type with $\text{Im}(\theta_0) \not\subseteq 1 + 4\mathbb{Z}_2$ such that G_0 has the strong n -Massey vanishing property for every $n > 2$, then the same holds for $Z \rtimes_{\theta_0} G_0$, with $Z \simeq \mathbb{Z}_2$.

Set $(G, \theta) = Z \rtimes_{\theta_0} (G_0, \theta_0)$, and let $z \in Z$ be a generator, and $\psi : Z \rightarrow \mathbb{F}_2$ the homomorphism dual to $\{z\}$ — namely, $\psi(z) = 1$, so that ψ generates $H^1(Z)$. Then it is well-known that

$$(4.1) \quad H^1(G) = H^1(G_0) \oplus H^1(Z),$$

while by the work of A. Wadsworth (cf. [49, Cor. 3.4 and Thm. 3.6]), one knows that

$$(4.2) \quad H^2(G) = H^2(G_0) \oplus (H^1(G_0) \smile \psi),$$

where the right-side summand denotes the subspace $\{\alpha \smile \psi \mid \alpha \in H^1(G_0)\}$, and one has $\alpha \smile \psi = 0$ if, and only if, $\alpha = 0$. In particular, if $\{\chi_1, \dots, \chi_d\}$ is a basis of $H^1(G_0)$, then $\{\chi_1 \smile \psi, \dots, \chi_d \smile \psi\}$ is a basis of $H^1(G_0) \smile \psi$.

Remark 4.3. By considering the elements of $H^1(G_0)$ and of $H^1(Z)$ as elements of $H^1(G)$ too, we commit a slight abuse of notation: actually, if $\alpha \in H^1(G_0)$, then we identify it with the element $\tilde{\alpha}$ of $H^1(G)$ such that $\tilde{\alpha}|_{G_0} = \alpha$, and $\tilde{\alpha}|_Z$ is the 0-map, and analogously if $\alpha \in H^1(Z)$.

Since (G_0, θ_0) is a pro-2 group of elementary type, we take a minimal generating set \mathcal{X} of G_0 consisting of the union of the minimal generating sets of the building bricks — free pro-2 groups and Demushkin pro-2 groups — of G_0 , together with generators of the pro-2-cyclic factors of the occurring semidirect products. We write \mathcal{X} as follows:

$$\mathcal{X} = \{ u_1, \dots, u_s, v_1, \dots, v_t \},$$

where

- (a) $\theta_0(u_h) \equiv -1 \pmod{4}$ for all $h = 1, \dots, s$,
- (b) $\theta_0(v_l) \equiv 1 \pmod{4}$ for all $l = 1, \dots, t$.

In particular, every generator u_h is the first generator — called x_1 in § 3.2 — of a “Demushkin brick” of G_0 with defining relation different to case (a), or a generator of a “free brick” (whose image via the orientation of the brick is equivalent to $-1 \pmod{4}$).

The minimal generating set \mathcal{X} yields the dual basis $\mathcal{B} = \{\omega_1, \dots, \omega_s, \varphi_1, \dots, \varphi_t\}$ of $H^1(G_0)$.

As a set of defining relations of G_0 we take the union of the defining relations of the “Demushkin bricks”, together with the relations defining the action in the occurring semidirect products.

Altogether, a generator u_h may show up in a defining relation of the following types:

$$(4.3) \quad \begin{aligned} u_h^2 [v_{l_1}, v_{l_2}] v_{l_2}^{-2^f} [v_{l_3}, v_{l_4}] \cdots &= 1, \\ [u_h, v_{l_1}] v_{l_1}^2 [v_{l_2}, v_{l_3}] v_{l_3}^{-2^f} \cdots &= 1, \\ [u_h, v_{l_1}] v_{l_1}^{2-2^f} [v_{l_2}, v_{l_3}] \cdots &= 1; \end{aligned}$$

(where the first relation might be just $u_h^2 = 1$) and in at most one of the above not involving precisely two generators. Analogously, a generator v_l with $\theta_0(v_l) = 1 + 2^f$, $2 \leq f < \infty$, may show up in a defining relation of the type

$$(4.4) \quad [v_l, v_{l_1}] v_{l_1}^{-2^f} [v_{l_2}, v_{l_3}] \cdots = 1,$$

and in at most one of this involving more than two generators. On the other hand, the defining relations involving the generators v_l 's with $\theta_0(v_l) = 1$ are just products of elementary commutators involving these generators, namely

$$(4.5) \quad [v_{l_1}, v_{l_2}] \cdots [v_{l_{m-1}}, v_{l_m}] = 1.$$

Remark 4.4. Every defining relation of G_0 is the product of factors

$$(4.6) \quad [y, v_l] v_l^{1-\theta_0(y)} \quad \text{with } y \in \mathcal{X}, v_l \in \text{Ker}(\theta_0),$$

and, possibly, u_h^2 with $\theta_0(u_h) = -1$.

Example 4.5. Let (G_0, θ_0) be the oriented pro-2 group of elementary type constructed in Example 3.6. We may pick the following minimal generating set of G_0 :

$$\mathcal{X} = \{ u_1 = x_1, u_2 = x_5, v_1 = x_2, v_2 = x_3, v_3 = x_4, v_4 = x_6, v_5 = z_1, v_6 = z_2 \}.$$

The generator u_1 is involved in the defining relations

$$u_1^2 [v_1, v_2] = [u_1, v_5] v_5^2 = [u_1, v_6] v_6^2 = 1,$$

the generator u_2 is involved in the defining relations

$$[u_2, v_4] v_4^2 = [u_2, v_6] v_6^2 = 1,$$

while the generator v_3 is involved in the defining relations

$$[v_3, v_5]v_5^{-4} = [v_3, v_6]v_6^{-4} = 1.$$

Now consider $G = Z \rtimes_{\theta_0} G_0$. Proposition 2.3 implies that

$$\psi^2 = (\omega_1 + \dots + \omega_s) \smile \psi \neq 0,$$

as $[u_1, z]z^2 = \dots = [u_s, z]z^2 = 1$. In order to proceed toward our result, we change the minimal generating set of G_0 . Put $w_1 = u_1$, and $w_h = u_1 u_h$ for all $h = 2, \dots, s$. Then

$$\mathcal{X}' = \{w_1, \dots, w_s, v_1, \dots, v_t\}$$

is again a minimal generating set of G_0 . Moreover, put $\chi_0 = \omega_1 + \dots + \omega_s$. Then $\chi_0(w_1) = 1$ and

$$\chi_0(w_h) = \omega_1(w_h) + \omega_h(w_h) = \omega_1(u_1) + \omega_h(u_h) = 1 + 1 = 0$$

for all $h = 2, \dots, s$, while for $h = 2, \dots, s$ one has $\omega_h(w_1) = \omega_h(u_1) = 0$, and

$$\omega_h(w_{h'}) = \begin{cases} \omega_h(u_1) + \omega_h(u_h) = 0 + 1 = 1 & \text{if } h' = h, \\ \omega_h(u_1) + \omega_h(u_{h'}) = 0 + 0 = 0 & \text{if } h' \neq h. \end{cases}$$

Therefore, $\{\chi_0, \omega_2, \dots, \omega_s, \varphi_1, \dots, \varphi_t\}$ is the basis of $H^1(G_0)$ dual to \mathcal{X}' .

Lemma 4.6. *Let α, α' be elements of $H^1(G)$, $\alpha, \alpha' \neq 0$ (and possibly $\alpha = \alpha'$), such that $\alpha \smile \alpha' = 0$. Then either $\alpha, \alpha' \in H^1(G_0)$, or $\alpha' = \alpha + \chi_0$ and $\alpha(z) = \alpha'(z) = 1$.*

Proof. We keep the same notation as above. We may write

$$\alpha = a\chi_0 + \beta + b\psi \quad \text{and} \quad \alpha' = a'\chi_0 + \beta' + b'\psi,$$

with $a, b, a', b' \in \mathbb{F}_2$ and $\beta, \beta' \in \text{Span}(\omega_2, \dots, \omega_s, \varphi_1, \dots, \varphi_t)$, in a unique way. Then we compute

$$\begin{aligned} 0 &= \alpha \smile \alpha' \\ &= (aa'\chi_0^2 + (a\beta' + a'\beta) \smile \chi_0 + \beta \smile \beta') + \\ &\quad ((b\beta' + b'\beta) \smile \psi + (ab' + a'b)\chi_0 \smile \psi + bb'\psi^2) \\ &= \underbrace{((aa'\chi_0 + a\beta' + a'\beta) \smile \chi_0 + \beta \smile \beta')}_{\in H^2(G_0)} + \underbrace{((b\beta' + b'\beta) + (ab' + a'b + bb'))\chi_0 \smile \psi}_{\in H^1(G_0) \smile \psi}, \end{aligned}$$

as $\psi^2 = \chi_0 \smile \psi$. Therefore both summands are 0. In particular, the right-side summand is 0 if, and only if,

$$(4.7) \quad \begin{cases} b\beta' + b'\beta = 0 \\ ab' + a'b + bb' = 0, \end{cases}$$

as $\beta, \beta' \in \text{Span}(\omega_2, \dots, \varphi_t)$. If $b, b' = 0$ then $\alpha, \alpha' \in H^1(G_0)$, and the system (4.7) is satisfied. So assume that not both b, b' are 0.

Suppose first that $b = 1$ and $b' = 0$. Then the first equation of (4.7) implies $\beta' = 0$, and the second equation implies $a' = 0$, namely, $\alpha' = 0$, a contradiction. Analogously, the case $b = 0$ and $b' = 1$ leads to $\alpha = 0$, a contradiction. Therefore, $b, b' = 1$, and the first equation of (4.7) implies $\beta = \beta'$, while the second equation implies $a' = a + 1$. Hence

$$\alpha' = (a + 1)\chi_0 + \beta + \psi = \alpha + \chi_0,$$

and $\alpha(z) = \alpha'(z) = \psi(z) = 1$. \square

We are ready to prove the following.

Proposition 4.7. *Let (G_0, θ_0) be an oriented pro-2 group of elementary type, with $\text{Im}(\theta_0) \not\subseteq 1 + 4\mathbb{Z}_2$. If G_0 has the strong n -Massey vanishing property for every $n > 2$, then also the semidirect product $Z \rtimes_{\theta_0} G_0$, with $Z = \langle z \rangle \simeq \mathbb{Z}_2$, has the strong n -Massey vanishing property for every $n > 2$.*

Proof. We keep the same notation as above. Let $\alpha_1, \dots, \alpha_n$ a sequence of elements of $H^1(G)$ — by Proposition 2.7 we may assume that they are all different to 0 — satisfying (1.1). By Lemma 4.6, one has two cases: either $\alpha_1, \dots, \alpha_n \in H^1(G_0)$; or $\alpha_i \notin H^1(G_0)$ for some i , and hence $\alpha_i = \alpha_1$ if i is odd, and $\alpha_i = \alpha_1 + \chi_0$ if i is even, and moreover $\alpha_i(z) = 1$ for all $i = 1, \dots, n$.

Suppose we are in the first case — namely, $\alpha_i \in H^1(G_0)$ for all i 's. Since G_0 has the strong n -Massey vanishing property by hypothesis, the n -fold Massey product $\langle \alpha_1, \dots, \alpha_n \rangle$ vanishes (in the \mathbb{F}_2 -cohomology of G_0). Hence, by Proposition 2.4 there exists a homomorphism

$$\bar{\rho}: G_0 \longrightarrow \mathbb{U}_{n+1}$$

such that $\bar{\rho}_{i,i+1} = \alpha_i$ for every $i = 1, \dots, n$. We construct a homomorphism $\rho: G \rightarrow \mathbb{U}_{n+1}$ such that $\rho|_{G_0} = \bar{\rho}$, and $Z \subseteq \text{Ker}(\rho)$. Then ρ satisfies all the conditions prescribed by Proposition 2.4, so that the n -fold Massey product $\langle \alpha_1, \dots, \alpha_n \rangle$ vanishes also in the \mathbb{F}_2 -cohomology of G .

Suppose now that we are in the second case — namely, $\alpha_i \notin H^1(G_0)$ for some i , so that $\alpha_2 = \alpha_1 + \chi_0$, $\alpha_3 = \alpha_1$, and so on. Since $\text{Im}(\theta_0) \not\subseteq 1 + 4\mathbb{Z}_2$, G_0 has at least a generator $u_h \in \mathcal{X}$ — and thus a generator u_1 — as above. If $\alpha_1(u_1) = 1$, we put $A = A_1$ and $B = B_1$, while if $\alpha_1(u_1) = 0$, we put $A = A_2$ and $B = B_2$, where A_i, B_i are as in Lemma 4.2. Recall that ${}^B A = A^{-1}$. Then

$$[AB, A] = {}^A [B, A] \cdot [A, A] = {}^A (A^{-2}) \cdot I_{n+1} = A^{-2}.$$

Our goal is to construct a homomorphism $\rho: G \rightarrow \mathbb{U}_{n+1}$ satisfying all the properties prescribed in Proposition 2.4, by assigning a suitable matrix to every generator of G lying in $\mathcal{X} \cup \{z\}$.

We start with z and we set $\rho(z) = A$. Then we proceed with the generators u_1, \dots, u_s . So, pick u_h with $1 \leq h \leq s$, and suppose first that $\theta_0(u_h) = -1$:

- (a) if $\alpha_1(u_h) = \alpha_1(u_1)$, set $\rho(u_h) = B$;
- (b) if $\alpha_1(u_h) \neq \alpha_1(u_1)$, set $\rho(u_h) = AB$ — we underline that for every $i = 1, \dots, n$, if the $(i, i+1)$ -entry of B is 1, then the $(i, i+1)$ -entry of AB is 0, and vice versa.

In both cases one has

$$[\rho(u_h), \rho(z)] = [B, A] = A^{-2} = \rho(z)^{\theta_0(u_h)-1},$$

and

$$\rho(u_h)^2 = \begin{cases} B^2 = I_{n+1} & \text{in case (a),} \\ ABAB = A \cdot A^{-1} = I_{n+1} & \text{in case (b);} \end{cases}$$

moreover $\rho(u_h)_{i,i+1} = \alpha_i(u_h)$ for all i 's.

Suppose now that $\theta_0(u_h) = -1 + 2^f$ with $2 \leq f < \infty$:

- (a) if $\alpha_1(u_h) = \alpha_1(u_1)$, set $\rho(u_h) = BC(-2^f)$;
- (b) if $\alpha_1(u_h) \neq \alpha_1(u_1)$, set $\rho(u_h) = ABC(-2^f)$.

Since $C(-2^f) \in (\mathbb{U}_{n+1})_{(3)}$, the $(i, i+1)$ -entry of $BC(-2^f)$, respectively of $ABC(-2^f)$, is the same as in B , respectively in AB , namely, $\alpha_i(u_h)$. In both cases one has

$$[\rho(u_h), \rho(z)] = [BC(-2^f), A] = {}^B(A^{-2^f}) \cdot A^{-2} = A^{2^f-2} = \rho(z)^{\theta_0(u_h)-1},$$

and moreover $\rho(u_h)_{i,i+1} = \alpha_i(u_h)$ for all i 's.

We are done with the generators u_1, \dots, u_s , so we proceed with the generators v_1, \dots, v_t . Recall that the value of $\alpha_i(v_l)$ is the same for all i 's. Pick v_l , and suppose that $\theta_0(v_l) = 1 + 2^f$ with $2 \leq f < \infty$:

- (a) if $\alpha_1(v_l) = 0$, set $\rho(v_l) = C(2^f)$, whose $(i, i+1)$ -entry is 0 for all i 's;
- (b) if $\alpha_1(v_l) = 1$, set $\rho(v_l) = AC(2^f)$, whose $(i, i+1)$ -entry is 1 for all i 's.

In both cases one has

$$[\rho(v_l), \rho(z)] = [C(2^f), A] = A^{2^f} = \rho(z)^{\theta_0(v_l)-1},$$

and moreover $\rho(v_l)_{i,i+1} = \alpha_i(v_l)$ for all i 's.

Suppose now that $\theta_0(v_l) = 1$:

- (a) if $\alpha_1(v_l) = 0$, set $\rho(v_l) = I_{n+1}$;
- (b) if $\alpha_1(v_l) = 1$, set $\rho(v_l) = A$.

In both cases one has $[\rho(v_l), \rho(z)] = I_{n+1} = \rho(z)^{\theta_0(v_l)-1}$, and

$$[\rho(y), \rho(v_l)] = \begin{cases} [\rho(y), I_{n+1}] = I_{n+1} = \rho(v_l)^{\theta_0(y)-1} & \text{in case (a),} \\ [\rho(y), \rho(z)] = \rho(z)^{\theta_0(y)-1} = \rho(v_l)^{\theta_0(y)-1} & \text{in case (b),} \end{cases}$$

for any $y \in \mathcal{X}$, and moreover $\rho(v_l)_{i,i+1} = \alpha_i(v_l)$ for all i 's.

Altogether, the matrices $\rho(y)$, with $y \in \mathcal{X}$, and $\rho(z)$, satisfy the defining relations (4.3)–(4.5) of G_0 (see also Remark 4.4), and the relations $[y, z]z^{1-\theta_0(y)} = 1$. Therefore, the assignment

$$z \mapsto \rho(z), \quad y \mapsto \rho(y), \quad \text{with } y \in \mathcal{X}$$

induces a homomorphism $\rho: G \rightarrow \mathbb{U}_{n+1}$, satisfying $\rho_{i,i+1} = \alpha_i$ for all $i = 1, \dots, n$. Hence, the n -fold Massey product $\langle \alpha_1, \dots, \alpha_n \rangle$ vanishes by Proposition 2.4. \square

4.4. Proofs of Theorems 1.2–1.3.

Proof of Theorem 1.3. We follow the recursive construction of an oriented pro-2 group of elementary type.

If (G, θ) is an oriented pro-2 group with G a finitely generated free pro-2 group, then G has the strong n -Massey vanishing property for all $n > 2$ by Proposition 2.5. If (G, θ) is an oriented pro-2 group with G a Demushkin pro-2 group, then G has the strong n -Massey vanishing property for all $n > 2$ by Proposition 4.1. So, all building bricks of an oriented pro-2 group of elementary type have the strong n -Massey vanishing property for all $n > 2$.

If $(G_1, \theta_1), (G_2, \theta_2)$ are oriented pro-2 groups with G_1, G_2 both satisfying the strong n -Massey vanishing property for all $n > 2$, then also the free pro-2 product $G_1 * G_2$ has the strong n -Massey vanishing property for all $n > 2$ by Proposition 2.5.

If (G_0, θ_0) is an oriented pro-2 groups with G_0 satisfying the strong n -Massey vanishing property for all $n > 2$, then also the semidirect product $Z \rtimes_{\theta_0} G_0$, with $Z \simeq \mathbb{Z}_2$, has the strong n -Massey vanishing property for all $n > 2$ by Proposition 4.7.

Finally, if H is an open subgroup of G then it is finitely generated (cf., e.g., [3, Prop. 1.7]), and thus also the oriented pro-2 group $(H, \theta|_H)$ is of elementary type, and it has the strong n -Massey vanishing property for all $n > 2$ by the argument above. \square

Proof of Theorem 1.2. By [33], if \mathbb{K} is a Pythagorean field with a finite number of square classes, then $(G_{\mathbb{K}}(2), \theta_{\mathbb{K}})$ is an oriented pro-2 group of elementary type, and thus the maximal pro-2 Galois group $G_{\mathbb{K}}(2)$ has the strong n -Massey vanishing property for all $n > 2$ by Theorem 1.3.

If \mathbb{L}/\mathbb{K} is a finite extension, then the maximal pro-2 Galois group $G_{\mathbb{L}}(2)$ is an open subgroup of $G_{\mathbb{K}}(2)$, of index the maximal 2-power dividing $[\mathbb{L} : \mathbb{K}]$. Therefore, $G_{\mathbb{L}}(2)$ has the strong n -Massey vanishing property for all $n > 2$ by Theorem 1.3. \square

Corollary 1.4 follows from Theorem 1.3 and Proposition 3.9, with the same argument for the finite extensions as in the proof of Theorem 1.2.

By [17, Example A.15], and by [31, Thm. 6.3], one knows that there are fields, with an infinite number of square classes, whose maximal pro-2 Galois group does not have the strong n -Massey vanishing property for $n = 4$ — for example, \mathbb{Q} is one of them. We ask whether, instead, a field with a finite number of square classes has maximal pro-2 Galois group with the strong n -Massey vanishing property for every $n > 2$ — as done in [43, Question 1.5] assuming further that the field contains $\sqrt{-1}$.

Question 4.8. *Let \mathbb{K} be a field with a finite number of square classes. Does the maximal pro-2 Galois group $G_{\mathbb{K}}(2)$ have the strong n -Massey vanishing property for every $n > 2$?*

REFERENCES

- [1] S. Blumer, A. Cassella, and C. Quadrelli, *Groups of p -absolute Galois type that are not absolute Galois groups*, J. Pure Appl. Algebra **227** (2023), no. 4, Paper No. 107262.
- [2] S.P. Demuškin, *The group of a maximal p -extension of a local field*, Izv. Akad. Nauk SSSR Ser. Mat. **25** (1961), 329–346 (Russian).
- [3] J.D. Dixon, M.P.F. du Sautoy, A. Mann, and D. Segal, *Analytic pro- p groups*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 61, Cambridge University Press, Cambridge, 1999.
- [4] W.G. Dwyer, *Homology, Massey products and maps between groups*, J. Pure Appl. Algebra **6** (1975), no. 2, 177–190.
- [5] I. Efrat, *Orderings, valuations, and free products of Galois groups*, Sem. Structure Algébriques Ordonnées, Univ. Paris VII (1995).
- [6] ———, *Pro- p Galois groups of algebraic extensions of \mathbf{Q}* , J. Number Theory **64** (1997), no. 1, 84–99.
- [7] ———, *Small maximal pro- p Galois groups*, Manuscripta Math. **95** (1998), no. 2, 237–249.
- [8] ———, *A Hasse principle for function fields over PAC fields*, Israel J. Math. **122** (2001), 43–60.
- [9] ———, *The Zassenhaus filtration, Massey products, and homomorphisms of profinite groups*, Adv. Math. **263** (2014), 389–411.
- [10] ———, *The lower p -central series of a free profinite group and the shuffle algebra*, J. Pure Appl. Algebra **224** (2020), no. 6, 106260, 13.
- [11] I. Efrat and E. Matzri, *Triple Massey products and absolute Galois groups*, J. Eur. Math. Soc. (JEMS) **19** (2017), no. 12, 3629–3640.
- [12] I. Efrat and J. Minač, *On the descending central sequence of absolute Galois groups*, Amer. J. Math. **133** (2011), no. 6, 1503–1532.

- [13] I. Efrat and C. Quadrelli, *The Kummerian property and maximal pro- p Galois groups*, J. Algebra **525** (2019), 284–310.
- [14] R. Elman and T.Y. Lam, *Quadratic forms over formally real fields and pythagorean fields*, Amer. J. Math. **94** (1972), 1155–1194.
- [15] M. D. Fried and M. Jarden, *Field arithmetic*, 4th ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, vol. 11, Springer, Cham, 2023. Revised by M. Jarden.
- [16] J. Gärtner, *Higher Massey products in the cohomology of mild pro- p -groups*, J. Algebra **422** (2015), 788–820.
- [17] P. Guillot, J. Minač, and A. Topaz, *Four-fold Massey products in Galois cohomology*, Compos. Math. **154** (2018), no. 9, 1921–1959. With an appendix by O. Wittenberg.
- [18] P. Guillot and J. Minač, *Extensions of unipotent groups, Massey products and Galois theory*, Adv. Math. **354** (2019), article no. 106748.
- [19] Y. Harpaz and O. Wittenberg, *The Massey vanishing conjecture for number fields*, Duke Math. J. **172** (2023), no. 1, 1–41.
- [20] M.J. Hopkins and K.G. Wickelgren, *Splitting varieties for triple Massey products*, J. Pure Appl. Algebra **219** (2015), no. 5, 1304–1319.
- [21] B. Jacob, *On the structure of Pythagorean fields*, J. Algebra **68** (1981), no. 2, 247–267.
- [22] ———, *The Galois cohomology of Pythagorean fields*, Invent. Math. **65** (1981/82), no. 1, 97–113.
- [23] B. Jacob and R. Ware, *A recursive description of the maximal pro-2 Galois group via Witt rings*, Math. Z. **200** (1989), no. 3, 379–396.
- [24] J.P. Labute, *Classification of Demushkin groups*, Canadian J. Math. **19** (1967), 106–132.
- [25] T.Y. Lam, *Introduction to quadratic forms over fields*, Grad. Stud. Math., vol. 67, American Mathematical Society, Providence, RI, 2005.
- [26] Y.H.J. Lam, Y. Liu, R.T. Sharifi, P. Wake, and J. Wang, *Generalized Bockstein maps and Massey products*, Forum Math. Sigma **11** (2023), Paper No. e5.
- [27] M. Marshall, *The elementary type conjecture in quadratic form theory*, Algebraic and arithmetic theory of quadratic forms, Contemp. Math., vol. 344, Amer. Math. Soc., Providence, RI, 2004, pp. 275–293.
- [28] E. Matzri, *Triple Massey products in Galois cohomology*, 2014. Preprint, available at [arXiv:1411.4146](https://arxiv.org/abs/1411.4146).
- [29] ———, *Triple Massey products of weight $(1, n, 1)$ in Galois cohomology*, J. Algebra **499** (2018), 272–280.
- [30] ———, *Higher triple Massey products and symbols*, J. Algebra **527** (2019), 136–146.
- [31] A. Merkurjev and F. Scavia, *Degenerate fourfold Massey products over arbitrary fields*, 2022. Preprint, available at [arXiv:2208.13011](https://arxiv.org/abs/2208.13011).
- [32] ———, *The Massey Vanishing Conjecture for fourfold Massey products modulo 2*, 2023. Preprint, available at [arXiv:2301.09290](https://arxiv.org/abs/2301.09290).
- [33] J. Minač, *Galois groups of some 2-extensions of ordered fields*, C. R. Math. Rep. Acad. Sci. Canada **8** (1986), no. 2, 103–108.
- [34] J. Minač, F.W. Pasini, C. Quadrelli, and N.D. Tân, *Koszul algebras and quadratic duals in Galois cohomology*, Adv. Math. **380** (2021), article no. 107569.
- [35] J. Minač and N.D. Tân, *The kernel unipotent conjecture and the vanishing of Massey products for odd rigid fields*, Adv. Math. **273** (2015), 242–270.
- [36] ———, *Triple Massey products over global fields*, Doc. Math. **20** (2015), 1467–1480.
- [37] ———, *Triple Massey products vanish over all fields*, J. London Math. Soc. **94** (2016), 909–932.
- [38] ———, *Counting Galois $\mathbb{U}_4(\mathbb{F}_p)$ -extensions using Massey products*, J. Number Theory **176** (2017), 76–112.
- [39] ———, *Triple Massey products and Galois theory*, J. Eur. Math. Soc. (JEMS) **19** (2017), no. 1, 255–284.
- [40] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer-Verlag, Berlin, 2008.
- [41] A. Pál and G. Quick, *Real projective groups are formal*, 2022. Preprint, available at [arXiv:2206.14645](https://arxiv.org/abs/2206.14645).

- [42] A. Pál and E. Szabó, *The strong Massey vanishing conjecture for fields with virtual cohomological dimension at most 1*, 2020. Preprint, available at [arXiv:1811.06192](https://arxiv.org/abs/1811.06192).
- [43] C. Quadrelli, *Massey products in Galois cohomology and the elementary type conjecture*, J. Number Theory **258** (2024), 40–65.
- [44] C. Quadrelli and Th.S. Weigel, *Profinite groups with a cyclotomic p -orientation*, Doc. Math. **25** (2020), 1881–1916.
- [45] L. Ribes and P.A. Zalesskii, *Profinite groups*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, vol. 40, Springer-Verlag, Berlin, 2010.
- [46] J-P. Serre, *Structure de certains pro- p -groupes (d'après Demuškin)*, Séminaire Bourbaki, Vol. 8, Soc. Math. France, Paris, 1995, pp. Exp. No. 252, 145–155 (French).
- [47] ———, *Galois cohomology*, Corrected reprint of the 1997 English edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. Translated from the French by Patrick Ion and revised by the author.
- [48] D. Vogel, *Massey products in the Galois cohomology of number fields*, 2004, <http://www.uni-heidelberg.de/archiv/4418>. PhD thesis, University of Heidelberg.
- [49] A. Wadsworth, *p -Henselian field: K -theory, Galois cohomology, and graded Witt rings*, Pacific J. Math. **105** (1983), no. 2, 473–496.
- [50] R. Ware, *Galois groups of maximal p -extensions*, Trans. Amer. Math. Soc. **333** (1992), no. 2, 721–728.
- [51] K. Wickelgren, *Massey products $\langle y, x, x, \dots, x, x, y \rangle$ in Galois cohomology via rational points*, J. Pure Appl. Algebra **221** (2017), no. 7, 1845–1866.

DEPARTMENT OF SCIENCE & HIGH-TECH, UNIVERSITY OF INSUBRIA, COMO, ITALY EU
Email address: claudio.quadrelli@uninsubria.it