

ON THE MASSEY VANISHING CONJECTURE AND FORMAL HILBERT 90

ALEXANDER MERKURJEV AND FEDERICO SCAVIA

ABSTRACT. Let p be a prime number, let G be a profinite group, let $\theta: G \rightarrow \mathbb{Z}_p^\times$ be a continuous character, and for all $n \geq 1$ write $\mathbb{Z}/p^n\mathbb{Z}(1)$ for the twist of $\mathbb{Z}/p^n\mathbb{Z}$ by the G -action. Suppose that (G, θ) satisfies a formal version of Hilbert's Theorem 90: for all open subgroups $H \subset G$ and every $n \geq 1$, the map $H^1(H, \mathbb{Z}/p^n\mathbb{Z}(1)) \rightarrow H^1(H, \mathbb{Z}/p\mathbb{Z}(1))$ is surjective. We show that the Massey Vanishing Conjecture for triple Massey products and some degenerate fourfold Massey products holds for G . A key step in our proof is the construction of a Hilbert 90 module for (G, θ) : a discrete G -module M which plays the role of the Galois module F_{sep}^\times for the absolute Galois group of a field F of characteristic different from p .

1. INTRODUCTION

Let G be a profinite group and p be a prime number. The cohomology ring $H^*(G, \mathbb{Z}/p\mathbb{Z})$ carries a multiplication, called cup product, as well as higher-order operations, called Massey products. When $G = \Gamma_F$ is the absolute Galois group of a field F containing a primitive p -th root of unity, the Norm-Residue Isomorphism Theorem of Voevodsky and Rost [HW19] describes the cup product on $H^*(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$ by giving a presentation by generators and relations.

If $\chi_1, \dots, \chi_n \in H^1(G, \mathbb{Z}/p\mathbb{Z})$, the Massey product of χ_1, \dots, χ_n is a certain subset $\langle \chi_1, \dots, \chi_n \rangle \subset H^2(G, \mathbb{Z}/p\mathbb{Z})$; see Section 5 for the definition. We say that $\langle \chi_1, \dots, \chi_n \rangle$ is defined if it is not empty, and that it vanishes if it contains 0. Massey products are the object of the Massey Vanishing Conjecture, due to Mináč–Tân [MT17] and inspired by earlier work of Hopkins–Wickelgren [HW15].

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

Conjecture 1.1 is motivated by the Profinite Inverse Galois Problem, that is, the open problem of determining which profinite groups are absolute Galois groups of fields. Indeed, the Conjecture predicts a new restriction for a profinite group to be an absolute Galois group.

Conjecture 1.1 has attracted a lot of attention in recent years, and has been established in a number of cases. It is known when $n = 3$, by Hopkins–Wickelgren [HW15] when F is a number field and $p = 2$, and by work of Efrat–Matzri and Mináč–Tân [Mat18, EM17, MT16] in general. It is also known when $n = 4$ and $p = 2$: when F is a number field this is due to Guillot–Mináč–Topaz–Wittenberg [GMT18], and when F is arbitrary to [MS23]. When F is a number field, the

Date: August 2023.

2020 Mathematics Subject Classification. 12G05; 55S30, 20E18, 20J06.

conjecture has been proved for all $n \geq 3$ and all primes p by Harpaz–Wittenberg [HW23].

In this paper, we investigate the Massey Vanishing Conjecture for all profinite groups which satisfy a formal version of Hilbert’s Theorem 90. As we now explain, this class of profinite groups contains all absolute Galois groups but is substantially larger.

Let p be a prime number, and denote by \mathbb{Z}_p the topological ring of p -adic integers, with the p -adic topology. Let (G, θ) be a p -oriented profinite group, that is, a profinite group G equipped with a continuous group homomorphism $\theta: G \rightarrow \mathbb{Z}_p^\times$. For all $n \geq 1$, we write $\mathbb{Z}/p^n\mathbb{Z}(1)$ for the G -module with underlying abelian group $\mathbb{Z}/p^n\mathbb{Z}$ and where G acts by multiplication via θ . We say that (G, θ) satisfies formal Hilbert 90 if, for all $n \geq 1$ and all open subgroups $H \subset G$, the reduction map

$$H^1(H, \mathbb{Z}/p^n\mathbb{Z}(1)) \rightarrow H^1(H, \mathbb{Z}/p\mathbb{Z}(1))$$

is surjective. In the literature, the p -oriented profinite groups (G, θ) satisfying formal Hilbert 90 are sometimes called 1-cyclotomic; see e.g. [DCF22, Definition 4.1] or [BCQ23, Definition 2.9(ii)].

It is a consequence of Hilbert’s Theorem 90 that for every field F of characteristic different from p , letting Γ_F be the absolute Galois group of F and $\theta_F: \Gamma_F \rightarrow \mathbb{Z}_p^\times$ be the canonical p -orientation (the cyclotomic character), the pair (Γ_F, θ_F) is a p -oriented profinite group which satisfies formal Hilbert 90; see Example 2.2. Other profinite groups admitting a p -orientation satisfying formal Hilbert 90 are: étale fundamental groups of semilocal $\mathbb{Z}[1/p]$ -schemes, affine \mathbb{F}_p -schemes, and smooth curves over algebraically closed fields; see [DCF22, Propositions 4.9, 4.10, 4.11].

Question 1.2. *Let p be a prime number, let $n \geq 3$ be an integer, and let G be a profinite group. Suppose that there exists a p -orientation θ of G such that (G, θ) satisfies formal Hilbert 90. Is it true that, for all $\chi_1, \dots, \chi_n \in H^1(G, \mathbb{Z}/p\mathbb{Z})$, if the Massey product $\langle \chi_1, \dots, \chi_n \rangle \subset H^2(G, \mathbb{Z}/p\mathbb{Z})$ is defined, then it vanishes?*

We show that the answer to Question 1.2 is affirmative when $n = 3$.

Theorem 1.3. *Let p be a prime number, let (G, θ) be a p -oriented profinite group satisfying formal Hilbert 90 and let $\chi_1, \chi_2, \chi_3 \in H^1(G, \mathbb{Z}/p\mathbb{Z})$. The following are equivalent:*

- (1) $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = 0$ in $H^2(G, \mathbb{Z}/p\mathbb{Z})$;
- (2) the mod p Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ is defined;
- (3) the mod p Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ vanishes.

Theorem 1.3 confirms a conjecture of Quadrelli [Qua21, Conjecture 1.5]; see Remark 6.2.

We also show that the answer to Question 1.2 is affirmative for certain degenerate mod 2 fourfold Massey products of the form $\langle \chi_1, \chi_2, \chi_3, \chi_1 \rangle$. The importance of these Massey products stems from the fact that they need not be defined even when $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = \chi_3 \cup \chi_1 = 0$ in $H^2(G, \mathbb{Z}/2\mathbb{Z})$; see [GMT18, Example A.15] and [MS22, Theorem 1.4].

Theorem 1.4. *Let (G, θ) be a 2-oriented profinite group satisfying formal Hilbert 90 and let $\chi_1, \chi_2, \chi_3 \in H^1(G, \mathbb{Z}/2\mathbb{Z})$. If the mod 2 Massey product $\langle \chi_1, \chi_2, \chi_3, \chi_1 \rangle$ is defined, then it vanishes.*

In the case of absolute Galois groups, this had been proved in [MS22, Theorem 1.3] by using quadratic forms theory (in particular, the theory of Albert forms associated to biquaternion algebras) and a number of facts on quaternion algebras split by a biquadratic extension (see [MS22, Appendix A]). Theorem 1.4 generalizes [MS22, Theorem 1.3] and shows that the latter can be proved using Hilbert's Theorem 90 only.

We proved Conjecture 1.1 for $n = 4$ and $p = 2$ in [MS23, Theorem 1.2]. The proof used tools from algebraic geometry which go beyond Hilbert 90. For this reason, we do not know whether the result can be generalized to 2-oriented profinite groups satisfying formal Hilbert 90.

Our proofs of Theorems 1.3 and 1.4 are based on the notion of Hilbert 90 module. This is a p -divisible G -module M whose p -primary torsion subgroup is isomorphic to the colimit of the $\mathbb{Z}/p^n\mathbb{Z}(1)$, where $n \geq 1$, and such that $H^1(H, M) = 0$ for every open subgroup H of G . If F is a field of characteristic not p , the Γ_F -module F_{sep}^\times is a Hilbert 90 module for (Γ_F, θ_F) . The definition of Hilbert 90 module is quite natural but, to our knowledge, had not yet appeared in the literature.

If (G, θ) admits a Hilbert 90 module, then it is not difficult to show that it satisfies formal Hilbert 90. It turns out that the converse is also true.

Theorem 1.5. *Let (G, θ) be a p -oriented profinite group. Then (G, θ) satisfies formal Hilbert 90 if and only if it admits a Hilbert 90 module.*

By working with a Hilbert 90 module, we are able to generalize many familiar properties of the Galois cohomology of fields to the cohomology of p -oriented profinite groups satisfying formal Hilbert 90.

We conclude the Introduction with a summary of the content of each section. In Section 2, we introduce p -oriented profinite groups, the formal Hilbert 90 property and Hilbert 90 modules, and we prove some basic properties. In Section 3, we prove that a standard Galois cohomology sequence extends to the context of p -oriented profinite groups admitting a Hilbert 90 module; see Proposition 3.2. Section 4 is devoted to the proof of Theorem 1.5. The definition and basic properties of Massey products are recalled in Section 5. We prove Theorem 1.3 in Section 6 and Theorem 1.4 in Section 7. In the final Section 8, we illustrate Theorem 1.3 by a simple example; see Proposition 8.1.

Notation. Let G be a profinite group. A topological G -module is an abelian Hausdorff topological group on which G acts continuously on the left. A discrete G -module is a topological G -module which carries the discrete topology. In this article, the term G -module will always refer to a discrete G -module.

If A is a G -module, we write A^G for the subgroup of G -invariant elements of A . For all $i \geq 0$ we write $C^i(G, A)$, (resp. $Z^i(G, A)$) for the group of mod p non-homogeneous degree- i continuous cochains (resp. cocycles) of G , and we write $H^i(G, A)$ for the i -th cohomology group of A . If $H \subset G$ is an open subgroup, we write $\text{Res}_H^G: H^i(G, A) \rightarrow H^i(H, A)$ for the restriction maps, $\text{Cor}_H^G: H^i(H, A) \rightarrow H^i(G, A)$ for the corestriction maps (for $i = 0$, this is the norm map $N_{G/H}: A^H \rightarrow A^G$), and, when H is also normal, $\text{Inf}_{G/H}^G: H^i(G/H, A^H) \rightarrow H^i(G, A)$ for the inflation maps.

If H is a closed subgroup of G and B is an H -module, we write $\text{Ind}_H^G(B)$ for the G -module induced by B : it consists of all continuous maps $x: G \rightarrow B$ such that $x(hg) = hx(g)$ for all $g \in G$ and $h \in H$, and $g \in G$ acts on it by the formula

$(g \cdot x)(g') := x(g'g)$ for all $g' \in G$. If A is a G -module, we have an injective homomorphism of G -modules

$$(1.1) \quad i: A \rightarrow \text{Ind}_H^G(A), \quad (ia)(g) = ga \text{ for all } g \in G$$

and, if H is an open subgroup G , a homomorphism of G -modules

$$(1.2) \quad \nu: \text{Ind}_H^G(A) \rightarrow A, \quad \nu(x) = \sum_{gH \in G/H} gx(g^{-1}).$$

For any closed subgroup H of G , the G -modules $\text{Ind}_H^G(A)$ and $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/H], A)$ are canonically isomorphic.

If A is an abelian group, $n \geq 1$ is an integer, and p is a prime number, we denote by $A[n]$ the n -torsion subgroup of A and by $A\{p\}$ be p -primary torsion subgroup of A . If p is a prime number, we write \mathbb{Z}_p for the ring of p -adic integers, and $\mathbb{Z}_{(p)}$ for the localization of \mathbb{Z} at p .

2. THE FORMAL HILBERT 90 PROPERTY AND HILBERT 90 MODULES

2.1. Oriented profinite groups. Let p be a prime number, let G be a profinite group, and let $\theta: G \rightarrow \mathbb{Z}_p^\times$ be a continuous group homomorphism. We call θ a p -orientation of G and the pair (G, θ) a p -oriented profinite group.

We write $\mathbb{Z}_p(1)$ for the topological G -module with underlying topological group \mathbb{Z}_p and where G acts via θ , that is, $g \cdot v := \theta(g)v$ for every $g \in G$ and every $v \in \mathbb{Z}_p$. For all $n \geq 0$, we set $\mathbb{Z}/p^n\mathbb{Z}(1) := \mathbb{Z}_p(1)/p^n\mathbb{Z}_p(1)$.

We say that (G, θ) is *cyclotomic* if the image of θ is contained in $1 + p\mathbb{Z}_p$. The pair (G, θ) is cyclotomic if and only if the G -action on $\mathbb{Z}/p\mathbb{Z}(1)$ is trivial. Every 2-oriented profinite group is cyclotomic.

Example 2.1. Let F be a field and write Γ_F for the absolute Galois group of F . We define the *canonical p -orientation* θ_F on Γ_F as follows. If $\text{char}(F) \neq p$, we define θ_F as the continuous homomorphism $\theta_F: \Gamma_F \rightarrow \mathbb{Z}_p^\times$ given by $g(\zeta) = \zeta^{\theta_F(g)}$ for every root of unity ζ of p -power order. If $\text{char}(F) = p$, we let θ_F be the trivial homomorphism. The pair (Γ_F, θ_F) is a p -oriented profinite group.

2.2. The formal Hilbert 90 property. Let (G, θ) be a p -oriented profinite group. We say that (G, θ) *satisfies formal Hilbert 90* if for every open subgroup $H \subset G$ and all $n \geq 1$ the reduction map $H^1(H, \mathbb{Z}/p^n\mathbb{Z}(1)) \rightarrow H^1(H, \mathbb{Z}/p\mathbb{Z}(1))$ is surjective.

Example 2.2. Let F be a field, let Γ_F be the absolute Galois group of F , and let θ_F be the canonical orientation on Γ_F defined in Example 2.1. We now show that (Γ_F, θ_F) satisfies formal Hilbert 90. Let $H \subset \Gamma_F$ be an open subgroup, and set $L := (F_{\text{sep}})^H$.

(1) Suppose that $\text{char}(F) \neq p$. By Kummer Theory, for all $n \geq 1$ the reduction map $H^1(H, \mathbb{Z}/p^n\mathbb{Z}(1)) \rightarrow H^1(H, \mathbb{Z}/p\mathbb{Z}(1))$ is identified with the projection map $L^\times/L^{\times p^n} \rightarrow L^\times/L^{\times p}$, and in particular it is surjective.

(2) Suppose that $\text{char}(F) = p$. For all $n \geq 1$, we have $H^2(H, \mathbb{Z}/p^{n-1}\mathbb{Z}) = 0$ because L has cohomological p -dimension ≤ 1 ; see [Ser02, §2.2, Proposition 3]. The short exact sequence

$$0 \rightarrow \mathbb{Z}/p^{n-1}\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow 0$$

now implies the surjectivity of the reduction map $H^1(H, \mathbb{Z}/p^n\mathbb{Z}) \rightarrow H^1(H, \mathbb{Z}/p\mathbb{Z})$.

The group \mathbb{Z}_p^\times acts on the abelian group $\mathbb{Q}/\mathbb{Z}_{(p)}$ by multiplication. We let S be the G -module whose underlying abelian group is $\mathbb{Q}/\mathbb{Z}_{(p)}$ and on which G acts via θ . For all $n \geq 1$, we have an isomorphism of G -modules $\mathbb{Z}/p^n\mathbb{Z}(1) \rightarrow S[p^n]$ given by $a + p^n\mathbb{Z} \mapsto a/p^n + \mathbb{Z}_{(p)}$. Therefore, S is the colimit of the $\mathbb{Z}/p^n\mathbb{Z}(1)$ for $n \geq 1$.

For every $n \geq 1$, the map $S \rightarrow S$ given by multiplication by p^{n-1} restricts to a surjective G -module homomorphism $S[p^n] \rightarrow S[p]$. Then (G, θ) satisfies formal Hilbert 90 if and only if for every open subgroup $H \subset G$ and all $n \geq 1$ the induced map $H^1(H, S[p^n]) \rightarrow H^1(H, S[p])$ is surjective.

Lemma 2.3. *Let (G, θ) be a p -oriented profinite group which satisfies formal Hilbert 90. Then for every open subgroup $H \subset G$ and every $n \geq 1$ the maps*

$$Z^1(H, S[p^n]) \rightarrow Z^1(H, S[p^{n-1}]), \quad H^1(H, S[p^n]) \rightarrow H^1(H, S[p^{n-1}]).$$

are surjective.

Proof. We first prove the surjectivity of $H^1(H, S[p^n]) \rightarrow H^1(H, S[p^{n-1}])$ by induction on $n \geq 1$. The case $n = 1$ is trivial. Now let $n \geq 2$, and suppose that the statement is true for $n - 1$. We have a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & S[p^{n-1}] & \longrightarrow & S[p^n] & \xrightarrow{p^{n-1}} & S[p] \longrightarrow 0 \\ & & \downarrow p & & \downarrow p & & \parallel \\ 0 & \longrightarrow & S[p^{n-2}] & \longrightarrow & S[p^{n-1}] & \xrightarrow{p^{n-2}} & S[p] \longrightarrow 0. \end{array}$$

Passing to cohomology, we obtain the diagram

$$\begin{array}{ccccc} H^1(H, S[p^{n-1}]) & \longrightarrow & H^1(H, S[p^n]) & \longrightarrow & H^1(H, S[p]) \\ \downarrow \cong & & \downarrow & & \parallel \\ H^1(H, S[p^{n-2}]) & \longrightarrow & H^1(H, S[p^{n-1}]) & \longrightarrow & H^1(H, S[p]), \end{array}$$

where the rows are exact, the top-right horizontal map is surjective because (G, θ) satisfies formal Hilbert 90, and the left vertical map is surjective by inductive assumption. A diagram chase now shows that the middle vertical map is surjective. The conclusion follows by induction on n .

We now prove the surjectivity of the map $Z^1(H, S[p^n]) \rightarrow Z^1(H, S[p^{n-1}])$ for all $n \geq 1$. Let $\sigma \in Z^1(H, S[p^{n-1}])$. Since the map $H^1(H, S[p^n]) \rightarrow H^1(H, S[p^{n-1}])$ is surjective, there exist $\tau \in Z^1(H, S[p^n])$ and $a \in S[p^{n-1}]$ such that for all $h \in H$ we have $p\tau(h) - \sigma(h) = (h-1)a$ in $S[p^{n-1}]$. Let $b \in S[p^n]$ be such that $a = pb$, and define $\tilde{\sigma} \in Z^1(H, S[p^n])$ by $\tilde{\sigma}(h) = \tau(h) - (h-1)b$ for all $h \in H$. Then $p\tilde{\sigma} = \sigma$, as desired. \square

2.3. Hilbert 90 modules. Let (G, θ) be a p -oriented profinite group. A *Hilbert 90 module* for (G, θ) is a discrete G -module M such that

- (i) $pM = M$,
- (ii) $M\{p\} \simeq S$ as G -modules, and
- (iii) $H^1(H, M) = 0$ for any open subgroup $H \subset G$.

The definition of Hilbert 90 module is modeled on the following example.

Example 2.4. Let p be a prime number, let F be a field of characteristic different from p , let Γ_F be the absolute Galois group of F , and let θ be the canonical

orientation on Γ_F ; see Example 2.1. It follows from Hilbert's Theorem 90 that F_{sep}^\times is a Hilbert 90 module for (Γ_F, θ_F) .

Lemma 2.5. *Let (G, θ) be a p -oriented profinite group, and let M be a Hilbert 90 module for (G, θ) . Then M is also a Hilbert 90 module for $(H, \theta|_H)$ for every closed subgroup H of G .*

Proof. Since properties (i) and (ii) of the definition of Hilbert 90 module are clearly preserved by passing to subgroups, we need only check (iii). Let H' be an open subgroup of H . Then H' is equal to the intersection of all the subgroups $H'N$, where N ranges over all open normal subgroups of G . By [Koc02, Theorem 3.16], we have

$$H^1(H', M) = \operatorname{colim}_N H^1(H'N, M) = 0,$$

where we have used the fact that if N is open in G , then so is $H'N$. \square

We conclude this section by generalizing two basic properties of Galois cohomology to profinite groups admitting a Hilbert 90 module.

Lemma 2.6. *Let (G, θ) be a p -oriented profinite group, let M a Hilbert 90 module for (G, θ) , and let $a \in M^G$. For all $g \in G - G_a$, we have an exact sequence*

$$M^{G_a} \xrightarrow{g-1} M^{G_a} \xrightarrow{N_{G/G_a}} M^G.$$

This is a generalization of Hilbert's Theorem 90 for degree- p cyclic extensions.

Proof. We may assume that $G_a \neq G$. Let $C := G/G_a$, let $g \in G - G_a$, and let $\sigma := gG_a \in C$. Thus C is a cyclic group of order p , generated by σ , and M^{G_a} is naturally a C -module. By [NSW08, Proposition (1.2.6) and end of p. 23], the homology of the complex in the statement is isomorphic to the Tate cohomology group $\hat{H}^{-1}(C, M^{G_a})$. It thus suffices to show that $\hat{H}^{-1}(C, M^{G_a})$ is trivial.

By [NSW08, Proposition (1.6.7)], the inflation map $H^1(C, M^{G_a}) \rightarrow H^1(G, M)$ is injective. Since M is a Hilbert 90 module for (G, θ) , the group $H^1(G, M)$ is trivial, and hence $H^1(C, M^{G_a})$ is also trivial. Since C is a finite cyclic group, by [NSW08, Proposition (1.7.1)] the group $\hat{H}^{-1}(C, M^{G_a})$ is isomorphic to $H^1(C, M^{G_a})$, and hence it is also trivial, as desired. \square

Let (G, θ) be a cyclotomic p -oriented profinite group, and let M be a Hilbert 90 module for (G, θ) . We fix an injective homomorphism $\iota: \mathbb{Z}/p\mathbb{Z} \hookrightarrow M$. The short exact sequence

$$(2.1) \quad 0 \rightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{\iota} M \xrightarrow{p} M \rightarrow 0$$

induces an exact sequence

$$(2.2) \quad M^G \xrightarrow{p} M^G \xrightarrow{\partial} H^1(G, \mathbb{Z}/p\mathbb{Z}) \rightarrow 0.$$

For all $a \in M^G$, we set $\chi_a := \partial(a)$ and $G_a := \operatorname{Ker}(\chi_a)$. The exactness of (2.2) amounts to the following statement: Every $\chi \in H^1(G, \mathbb{Z}/p\mathbb{Z})$ is of the form χ_a for some $a \in M^G$, uniquely determined up to an element of $p(M^G)$.

Example 2.7. We maintain the notation of Example 2.4. The pair (Γ_F, θ_F) is cyclotomic if and only if F contains a primitive p -th root of unity. A choice of a primitive p -th root of unity $\zeta \in F$ determines an injection $\iota: \mathbb{Z}/p\mathbb{Z} \rightarrow F_{\text{sep}}^\times$. The map $\partial: F^\times \rightarrow H^1(\Gamma_F, \mathbb{Z}/p\mathbb{Z})$ of (2.2) sends $a \in F^\times$ to the character $\chi_a: \Gamma_F \rightarrow \mathbb{Z}/p\mathbb{Z}$ determined by $g(a) = \zeta^{\chi_a(g)} a$ for all $a \in F_{\text{sep}}^\times$.

Lemma 2.8. *Let (G, θ) be a cyclotomic p -oriented profinite group, let M be a Hilbert 90 module for (G, θ) , and let $a, b \in M^G$. Let $\omega_a \in H^2(G, \mathbb{Z})$ be the Bockstein of $\chi_a \in H^1(G, \mathbb{Z}/p\mathbb{Z})$, that is, the image of χ_a under the connecting homomorphism $H^1(G, \mathbb{Z}/p\mathbb{Z}) \rightarrow H^2(G, \mathbb{Z})$ associated to the short exact sequence of trivial G -modules*

$$0 \rightarrow \mathbb{Z} \xrightarrow{\times p} \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow 0.$$

Then the map $H^2(G, \mathbb{Z}/p\mathbb{Z}) \rightarrow H^2(G, M)$ sends $\chi_a \cup \chi_b$ to $b \cup \omega_a$.

When G is the absolute Galois group of a field of characteristic different from p , Lemma 2.8 reduces to a well-known property of the Brauer group of a field; see [Ser79, XIV.§2 Proposition 5], whose proof adapts to our more general situation without essential changes.

Proof. Let $\beta \in M$ be such that $p\beta = b$. By definition, $b \cup \omega_a$ is represented by the 2-cocycle $G \rightarrow M$ which sends a pair $(g, h) \in G \times G$ to

$$\beta \cup (\tilde{\chi}_a(g) + \tilde{\chi}_a(h) - \tilde{\chi}_a(gh)),$$

where $\tilde{\chi}_a: G \rightarrow \mathbb{Z}$ is a function lifting χ_a . The anticommutativity of the cup product gives $\chi_a \cup \chi_b = -\chi_b \cup \chi_a$. Using the formula for the cup product of two 1-cocycles of [CE56, p. 221], the image of $-\chi_b \cup \chi_a$ in $H^2(G, M)$ may be represented by the 2-cocycle which sends a pair $(g, h) \in G \times G$ to

$$-(g\beta - \beta)\tilde{\chi}_a(h).$$

The difference of these two cocycles sends a pair $(g, h) \in G \times G$ to

$$g\beta \cup \tilde{\chi}_a(h) - \beta \cup \tilde{\chi}_a(gh) + \beta \cup \tilde{\chi}_a(g).$$

This is the coboundary of the 1-cochain which sends $g \in G$ to $\beta \cup \tilde{\chi}_a(g)$. \square

3. THE STANDARD EXACT SEQUENCE

Lemma 3.1. *Let (G, θ) be a cyclotomic p -oriented profinite group, let M be a Hilbert 90 module for (G, θ) , and let H be an open subgroup of G . We have a commutative square*

$$\begin{array}{ccc} M^H & \xrightarrow{\partial} & H^1(H, \mathbb{Z}/p\mathbb{Z}) \\ \downarrow N_{G/H} & & \downarrow \text{Cor}_H^G \\ M^G & \xrightarrow{\partial} & H^1(G, \mathbb{Z}/p\mathbb{Z}), \end{array}$$

where the horizontal maps come from (2.2).

Proof. This follows from the fact that Cor_H^G commutes with connecting homomorphisms (see [NSW08, Proposition (1.5.2)]) and the fact that Cor_H^G coincides with $N_{G/H}$ in degree 0 (see [NSW08, §5, 4. p.47]). \square

Proposition 3.2. *Let (G, θ) be a p -oriented profinite group that admits a Hilbert 90 module. Let $\chi: G \rightarrow \mathbb{Z}/p\mathbb{Z}$ be a character and $H = \text{Ker}(\chi)$. Then the sequence*

$$H^1(H, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\text{Cor}} H^1(G, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\cup \chi} H^2(G, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\text{Res}} H^2(H, \mathbb{Z}/p\mathbb{Z})$$

is exact.

Proof. Let $G' := \theta^{-1}(1 + p\mathbb{Z}_p)$, let $\chi' := \chi|_{G'}$, and let $H' := \text{Ker}(\chi') = H \cap G'$. Note that G' is an open subgroup of G , the index $[G : G']$ divides $p - 1$ and $(G', \theta|_{G'})$ is cyclotomic. Since p does not divide $[G : G']$ and $[H : H']$, for all $i \geq 0$ the compositions

$$H^i(G, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\text{Res}} H^i(G', \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\text{Cor}} H^i(G, \mathbb{Z}/p\mathbb{Z})$$

and

$$H^i(H, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\text{Res}} H^i(H', \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\text{Cor}} H^i(H, \mathbb{Z}/p\mathbb{Z})$$

are isomorphisms. Therefore the sequence of Proposition 3.2 induced by χ is a direct summand of the sequence induced by χ' . In particular, if the latter is exact, so is the former. Replacing (G, θ) by $(G', \theta|_{G'})$, we may thus assume that (G, θ) is cyclotomic.

The conclusion is clear if $\chi = 0$, hence we may assume that $\chi \neq 0$. We first prove exactness at $H^2(G, \mathbb{Z}/p\mathbb{Z})$. Let $C := G/H$, so that C is a cyclic group of order p , and let $\bar{\chi} : C \rightarrow \mathbb{Z}/p\mathbb{Z}$ be the homomorphism induced by χ . Let M be a Hilbert 90 module for (G, θ) , fix an inclusion $\iota : \mathbb{Z}/p\mathbb{Z} \hookrightarrow M$, and write $\iota_* : H^2(G, \mathbb{Z}/p\mathbb{Z}) \rightarrow H^2(G, M)$ for the induced map.

Let $\alpha \in H^2(G, \mathbb{Z}/p\mathbb{Z})$ be such that $\text{Res}_H^G(\alpha) = 0$, and set $\alpha_1 := \iota_*(\alpha)$. Since $H^1(H, M) = 0$, by [NSW08, Proposition (1.6.7)] the sequence

$$0 \rightarrow H^2(C, M^H) \xrightarrow{\text{Inf}} H^2(G, M) \xrightarrow{\text{Res}} H^2(H, M)$$

is exact. As α restricts to zero on H , so does α_1 , and so there is $\alpha_2 \in H^2(C, M^H)$ such that $\alpha_1 = \text{Inf}_C^G(\alpha_2)$. Let

$$\beta : H^1(G, \mathbb{Z}/p\mathbb{Z}) \rightarrow H^2(G, \mathbb{Z}), \quad \bar{\beta} : H^1(C, \mathbb{Z}/p\mathbb{Z}) \rightarrow H^2(C, \mathbb{Z}),$$

be the connecting homomorphisms associated to the short exact sequence

$$0 \rightarrow \mathbb{Z} \xrightarrow{p} \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow 0,$$

viewed as a sequence of trivial G -modules and trivial C -modules, respectively. Since cup products commute with inflation maps (see [NSW08, Proposition (1.5.3)(ii)]), we have a commutative square

$$\begin{array}{ccc} H^0(C, M^H) & \xrightarrow{\cup \bar{\beta}(\bar{\chi})} & H^2(C, M^H) \\ \parallel \text{Inf} & & \downarrow \text{Inf} \\ H^0(G, M) & \xrightarrow{\cup \beta(\chi)} & H^2(G, M). \end{array}$$

Note that $H^0(C, M^H) = H^0(G, M) = M^G$. As the group C is cyclic, the top horizontal map is surjective; see [NSW08, Proposition (1.7.1)]. Thus, there exists $m \in M^G$ such that $m \cup \bar{\beta}(\bar{\chi}) = \alpha_2$ in $H^2(C, M^H)$, and hence $m \cup \beta(\chi) = \alpha_1$ in $H^2(G, M)$.

By [GS17, Proposition 3.4.9] applied to the pairing of G -modules $M \times \mathbb{Z} \rightarrow M$ given by $(v, n) \mapsto nv$, the diagram

$$\begin{array}{ccc} H^1(G, M[p]) \otimes H^1(G, \mathbb{Z}/p\mathbb{Z}) & \xrightarrow{\cup} & H^2(G, \mathbb{Z}/p\mathbb{Z}) \\ \partial \uparrow & & \downarrow \iota_* \\ H^0(G, M) \otimes H^2(G, \mathbb{Z}) & \xrightarrow{\cup} & H^2(G, M), \end{array}$$

is anti-commutative, that is, $\iota_*(\partial(v) \cup \psi) = -v \cup \beta(\psi)$ for all $v \in H^0(G, M) = M^G$ and $\psi \in H^1(G, \mathbb{Z}/p\mathbb{Z})$. Therefore

$$\iota_*(\alpha) = \alpha_1 = m \cup \beta(\chi) = -\iota_*(\partial(m) \cup \chi) = \iota_*(-\partial(m) \cup \chi).$$

Since $H^1(G, M) = 0$, the map ι_* is injective, and hence $\alpha = -\partial(m) \cup \chi$. This proves exactness at $H^2(G, \mathbb{Z}/p\mathbb{Z})$. Finally, by [MS82, Proposition 15.5], the sequence is also exact at $H^1(G, \mathbb{Z}/p\mathbb{Z})$. \square

Corollary 3.3. *Let (G, θ) be a p -oriented profinite group and let M be a Hilbert 90 module for (G, θ) . Let $a, b \in M^G$ be such that $\chi_a \cup \chi_b = 0$ in $H^2(G, \mathbb{Z}/p\mathbb{Z})$. Then there exists $\alpha \in M^{G_a}$ such that $N_{G/G_a}(\alpha) = b$ in M^G .*

Proof. By Proposition 3.2 applied to $\chi = \chi_a$, there exists $\psi \in H^1(G_a, \mathbb{Z}/p\mathbb{Z})$ such that $\text{Cor}_{G_a}^G(\psi) = \chi_b$. Let $\alpha' \in M^{G_a}$ be such that $\psi = \chi_{\alpha'}$. By Lemma 3.1, we have $N_{G/G_a}(\alpha') = b + pu$ for some $u \in M^G$. Define $\alpha := \alpha' - u \in M^{G_a}$. Then $N_{G/G_a}(\alpha) = b$, as desired. \square

4. PROOF OF THEOREM 1.5

Proof of Theorem 1.5. Suppose first that (G, θ) admits a Hilbert 90 module M . We have a commutative diagram of G -modules with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & S[p^n] & \longrightarrow & M & \xrightarrow{p^n} & M \longrightarrow 0 \\ & & \downarrow & & \downarrow^{p^{n-1}} & & \parallel \\ 0 & \longrightarrow & S[p] & \longrightarrow & M & \xrightarrow{p} & M \longrightarrow 0. \end{array}$$

Therefore, for every open subgroup H of G , we obtain a commutative diagram with exact rows

$$\begin{array}{ccccc} M^H & \longrightarrow & H^1(H, S[p^n]) & \longrightarrow & H^1(H, M) \\ \parallel & & \downarrow & & \downarrow^{p^{n-1}} \\ M^H & \longrightarrow & H^1(H, S[p]) & \longrightarrow & H^1(H, M). \end{array}$$

Since $H^1(H, M) = 0$, we deduce that the map $H^1(H, S[p^n]) \rightarrow H^1(H, S[p])$ is surjective, as desired.

Conversely, suppose that the pair (G, θ) satisfies formal Hilbert 90. Let H be an open subgroup of G , and fix $\sigma \in Z^1(H, S[p])$. By Lemma 2.3, we may find a sequence $(\sigma_n)_{n \geq 1}$, where $\sigma_n \in Z^1(H, S[p^n])$, $\sigma_1 = \sigma$ and the map $Z^1(H, S[p^n]) \rightarrow Z^1(H, S[p^{n-1}])$ sends σ_n to σ_{n-1} for all $n \geq 2$.

Lemma 4.1. *Write $\bar{\sigma}_n$ for the image of σ_n under $Z^1(H, S[p^n]) \rightarrow Z^1(H, S)$. For all $n \geq 1$ and all $x \in \mathbb{Z}_{(p)}$, we have $x\bar{\sigma}_n = px\bar{\sigma}_{n+1}$ in $Z^1(H, S)$.*

Proof. We have a commutative square H -modules

$$\begin{array}{ccc} S[p^n] & \hookrightarrow & S \\ \downarrow^p & & \downarrow^p \\ S[p^{n-1}] & \hookrightarrow & S. \end{array}$$

Passing to cocycles, we get a commutative square

$$\begin{array}{ccc} Z^1(H, S[p^n]) & \longrightarrow & Z^1(H, S) \\ \downarrow & & \downarrow^p \\ Z^1(H, S[p^{n-1}]) & \longrightarrow & Z^1(H, S), \end{array}$$

from which the conclusion follows. \square

Consider the uniquely divisible group $Q_H := \bigoplus_{\sigma} \mathbb{Q}u_{\sigma}$, where σ ranges over all elements of $Z^1(H, S[p])$ and the u_{σ} are formal symbols.

We now define an H -module M_H . As an abelian group, $M_H := S \oplus Q_H$. The group H acts on M_H as follows: for all $h \in H$, $\sigma \in Z^1(H, S[p])$, $s \in S$, $a \in \mathbb{Q}$, if n is a positive integer such that $p^n a \in \mathbb{Z}_{(p)}$, then

$$(4.1) \quad h(s, au_{\sigma}) := (\theta(h)s + p^n a \bar{\sigma}_n(h), au_{\sigma}).$$

By Lemma 4.1, this definition is independent on the choice of n . We have a short exact sequence of H -modules

$$(4.2) \quad 0 \rightarrow S \rightarrow M_H \rightarrow Q_H \rightarrow 0,$$

where the map $S \rightarrow M_H$ is the inclusion into the first factor and the map $M_H \rightarrow Q_H$ is the projection onto the second factor.

Lemma 4.2. *The map $H^1(H, S[p]) = H^1(H, M_H[p]) \rightarrow H^1(H, M_H)$ is trivial.*

Proof. Let $\sigma \in Z^1(H, S[p])$ be a 1-cocycle, and set $m_{\sigma} := (0, \frac{1}{p}u_{\sigma}) \in M_H$. By (4.1), for all $h \in H$ we have $(h-1)m_{\sigma} = (\bar{\sigma}_1(h), 0) = (\bar{\sigma}(h), 0)$, that is, the image of σ in $Z^1(H, M_H)$ is equal to the coboundary of m_{σ} . \square

Consider the following diagram of short exact sequence of G -modules

$$(4.3) \quad \begin{array}{ccccccc} 0 & \longrightarrow & \text{Ind}_H^G(S) & \longrightarrow & \text{Ind}_H^G(M_H) & \longrightarrow & \text{Ind}_H^G(Q_H) \longrightarrow 0 \\ & & \downarrow \nu & & \downarrow & & \parallel \\ 0 & \longrightarrow & S & \longrightarrow & \widetilde{M}_H & \longrightarrow & \text{Ind}_H^G(Q_H) \longrightarrow 0, \end{array}$$

where the top row is induced by (4.2), ν is the map of (1.2) for $A = S$, and \widetilde{M}_H is defined as the pushout of the left square. If N is an H -module, the induced G -module $\text{Ind}_H^G(N)$ is a G -module whose underlying abelian group is a direct sum of $[G : H]$ copies of N . In particular, the functor $\text{Ind}_H^G(-)$ is exact. This explains the exactness of the top row in (4.3).

Lemma 4.3. *The map $H^1(H, S[p]) = H^1(H, \widetilde{M}_H[p]) \rightarrow H^1(H, \widetilde{M}_H)$ is trivial.*

Proof. This follows from the fact that the inclusion of $S[p] = \widetilde{M}_H[p]$ into \widetilde{M}_H factors as the composition of the H -module homomorphisms

$$S[p] \rightarrow M_H \rightarrow \text{Ind}_H^G(M_H) \rightarrow \widetilde{M}_H$$

and the homomorphism $H^1(H, S[p]) \rightarrow H^1(H, M_H)$ is trivial by Lemma 4.2. \square

Consider the following diagram of G -modules with exact rows

$$(4.4) \quad \begin{array}{ccccccc} 0 & \longrightarrow & \bigoplus_{H \subset G} S & \longrightarrow & \bigoplus_{H \subset G} \widetilde{M}_H & \longrightarrow & \bigoplus_{H \subset G} \text{Ind}_H^G(Q_H) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \parallel \\ 0 & \longrightarrow & S & \longrightarrow & M & \longrightarrow & \bigoplus_{H \subset G} \text{Ind}_H^G(Q_H) \longrightarrow 0. \end{array}$$

Here H ranges over all open subgroups of G , the top row is the direct sum of the bottom rows in (4.3), the left vertical map is the identity on every summand, and M is defined so that the left square is a pushout.

Lemma 4.4. *The G -module M is a Hilbert 90 module for (G, θ) .*

Proof. By (4.4), the G -module M is an extension of a uniquely divisible G -module by the p -primary torsion G -module S . It follows that M is divisible and uniquely divisible by all primes $p' \neq p$. In particular, $M = pM$ and $M_{\text{tors}} = S$.

Let $H \subset G$ be an open subgroup. By (4.4), the embedding of S into M factors as $S \rightarrow \widetilde{M}_H \rightarrow M$. Therefore, by Lemma 4.3, the homomorphism

$$H^1(H, S[p]) = H^1(H, M[p]) \rightarrow H^1(H, M)$$

is trivial. The short exact sequence

$$0 \rightarrow S[p] \rightarrow M \xrightarrow{p} M \rightarrow 0$$

yields an exact sequence

$$H^1(H, S[p]) \rightarrow H^1(H, M) \xrightarrow{p} H^1(H, M).$$

Since the first homomorphism is trivial, this implies that $H^1(H, M)[p] = 0$. For all primes $p' \neq p$, the subgroup $H^1(H, M)[p']$ is trivial because M is uniquely p' -divisible. We conclude that $H^1(H, M) = 0$. This completes the proof. \square

By Lemma 4.4, the p -oriented profinite group (G, θ) admits a Hilbert 90 module. This completes the proof of Theorem 1.5. \square

Corollary 4.5. *Let (G, θ) be a p -oriented profinite group that satisfies formal Hilbert 90. Let $\chi : G \rightarrow \mathbb{Z}/p\mathbb{Z}$ be a character and set $H := \text{Ker}(\chi)$. Then the sequence*

$$H^1(H, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\text{Cor}} H^1(G, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\cup \chi} H^2(G, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\text{Res}} H^2(H, \mathbb{Z}/p\mathbb{Z})$$

is exact.

Proof. Combine Theorem 1.5 and Proposition 3.2. \square

Remark 4.6. When $p = 2$ the sequence of Corollary 4.5 is exact for all profinite groups G , as it is part of the long exact sequence associated to

$$0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Ind}_H^G(\mathbb{Z}/2\mathbb{Z}) \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0.$$

5. MASSEY PRODUCTS IN GROUP COHOMOLOGY

5.1. Massey products. Let (A, ∂) be a differential graded ring, i.e. $A = \bigoplus_{i \geq 0} A^i$ is a non-negatively graded abelian group with an associative multiplication which respects the grading, and $\partial: A \rightarrow A$ is a group homomorphism of degree 1 such that $\partial \circ \partial = 0$ and $\partial(ab) = \partial(a)b + (-1)^i a\partial(b)$ for all $i \geq 0$, $a \in A^i$ and $b \in A$. We denote by $H^*(A) := \text{Ker } \partial / \text{Im } \partial$ the cohomology of (A, ∂) , and we write \cup for the multiplication (cup product) on $H^*(A)$.

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

- (1) $\partial(a_{i,i+1}) = 0$ and $a_{i,i+1}$ represents a_i in $H^1(A)$, and
- (2) $\partial(a_{ij}) = -\sum_{l=i+1}^{j-1} a_{il}a_{lj}$ for all $i < j - 1$.

It follows from (2) that $-\sum_{l=2}^n a_{1l}a_{l,n+1}$ is a 2-cocycle: we write $\langle a_1, \dots, a_n \rangle_M$ for its cohomology class in $H^2(A)$, called the *value* of $\langle a_1, \dots, a_n \rangle$ corresponding to M . By definition, the *Massey product* of a_1, \dots, a_n is the subset $\langle a_1, \dots, a_n \rangle$ of $H^2(A)$ consisting of the values $\langle a_1, \dots, a_n \rangle_M$ of all defining systems M . We say that the Massey product $\langle a_1, \dots, a_n \rangle$ is *defined* if it is non-empty, and that it *vanishes* if $0 \in \langle a_1, \dots, a_n \rangle$.

Lemma 5.1. *Let A be a differential graded ring and let $a_1, \dots, a_n \in H^1(A)$. Suppose that the Massey product $\langle a_1, \dots, a_n \rangle$ is defined and that $a_k = 0$ for at least one $k \in \{1, \dots, n\}$. Then the Massey product $\langle a_1, \dots, a_n \rangle$ vanishes.*

Proof. We follow the proof [Fen83, Lemma 6.2.4]. Let $(a_{ij})_{i,j}$ be a defining system for $\langle a_1, \dots, a_n \rangle$. Set $b_{ij} = a_{ij}$ if $i > k$ or $j < k$, and set $b_{ij} = 0$ if $i \leq k \leq j$. Then $(b_{ij})_{i,j}$ is a defining system for $\langle a_1, \dots, a_n \rangle$. Moreover, for all $2 \leq l \leq n$ we have $b_{1l}b_{l,n+1} = 0$, and hence $\sum_{l=2}^n b_{1l}b_{l,n+1} = 0$. Thus $\langle a_1, \dots, a_n \rangle$ vanishes. \square

5.2. Dwyer's Theorem. Let G be a profinite group and let p be a prime number. The complex $(C^*(G, \mathbb{Z}/p\mathbb{Z}), \partial)$ of mod p non-homogeneous continuous cochains of G with the standard cup product is a differential graded ring. Thus the cohomology ring $H^*(G, \mathbb{Z}/p\mathbb{Z}) = H^*(C^*(G, \mathbb{Z}/p\mathbb{Z}), \partial)$ is endowed with Massey products.

Let $U_{n+1} \subset \text{GL}_{n+1}(\mathbb{F}_p)$ be the subgroup of all upper-triangular unipotent matrices. For all $1 \leq i < j \leq n+1$, we denote by $u_{i,j}: U_{n+1} \rightarrow \mathbb{Z}/p\mathbb{Z}$ the (i, j) -th coordinate function on U_{n+1} . The functions $u_{i,j}$ are group homomorphisms only when $j = i+1$. The center Z_{n+1} of U_{n+1} is the subgroup of all matrices such that $u_{i,j} = 0$ when $(i, j) \neq (1, n+1)$. We fix an identification $Z_{n+1} \simeq \mathbb{Z}/p\mathbb{Z}$ by letting 1 correspond to the matrix in Z_{n+1} with 1 on the top-right corner. We obtain a commutative diagram

$$(5.1) \quad \begin{array}{ccccccc} 1 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & U_{n+1} & \longrightarrow & \bar{U}_{n+1} & \longrightarrow & 1 \\ & & & & & & \searrow & \downarrow & \\ & & & & & & & (\mathbb{Z}/p\mathbb{Z})^n & \end{array}$$

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

The following characterization of Massey products in group cohomology is due to Dwyer [Dwy75].

Theorem 5.2. *Let p be a prime number, let G be a profinite group, let χ_1, \dots, χ_n be in $H^1(G, \mathbb{Z}/p\mathbb{Z})$, write $\chi = (\chi_1, \dots, \chi_n): G \rightarrow (\mathbb{Z}/p\mathbb{Z})^n$ for the induced homomorphism, and consider the mod p Massey product $\langle \chi_1, \dots, \chi_n \rangle$.*

(i) *If $\tilde{\chi}: G \rightarrow \bar{U}_{n+1}$ is a continuous homomorphism lifting χ , then the collection of 1-cochains $M_{\tilde{\chi}} := \{u_{i,j} \circ \tilde{\chi}\}$ forms a defining system for $\langle \chi_1, \dots, \chi_n \rangle$.*

(ii) *There is a bijective correspondence between continuous lifts of χ and defining systems for $\langle \chi_1, \dots, \chi_n \rangle$, given by sending a lift $\tilde{\chi}: G \rightarrow \bar{U}_{n+1}$ to $M_{\tilde{\chi}}$.*

(iii) *Let $\tilde{\chi}: G \rightarrow \bar{U}_{n+1}$ be a continuous lift of χ . Then the value of $M_{\tilde{\chi}}$ is equal to $-\tilde{\chi}^*(u) \in H^2(G, \mathbb{Z}/p\mathbb{Z})$, where $u \in H^2(\bar{U}_{n+1}, \mathbb{Z}/p\mathbb{Z})$ is the class of the short exact sequence of (5.1)*

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

It follows from (iii) that $\tilde{\chi}$ lifts to U_{n+1} if and only if the class

$$h^*(u) = \left[\sum_{l=2}^n \tilde{\chi}_{1l} \tilde{\chi}_{l,n+1} \right] \in H^2(G, \mathbb{Z}/p\mathbb{Z}),$$

vanishes, where $\tilde{\chi}_{ij} := u_{ij} \circ \tilde{\chi}$. We will refer to $h^*(u)$ as the *obstruction* to lifting $\tilde{\chi}$ to U_{n+1} .

Proof. This result is originally due to Dwyer [Dwy75], with different sign conventions. For the version of Dwyer's Theorem with our sign conventions, see [Efr14, Proposition 8.3] or [HW23, Proposition 2.2]. \square

Let C_p be a cyclic group of order p , and fix a generator $\sigma \in C_p$. For every C_p -module A , we define a C_p -module endomorphism

$$\tilde{N}_{C_p}: A \rightarrow A, \quad \tilde{N}_{C_p}(a) = \sum_{l=0}^{p-2} (p-1-l)\sigma^l a \quad \text{for all } a \in A.$$

Now let G be a profinite group, let $\chi \in H^1(G, \mathbb{Z}/p\mathbb{Z})$ be a non-zero character, let H be the kernel of χ , and let $g \in G$ be such that $\chi(g) = 1$. For every G -module B on which H acts trivially, we define a G -module endomorphism $\tilde{N}_\chi: B \rightarrow B$ as \tilde{N}_{C_p} , where we view B as a G/H -module and identify G/H with C_p so that gH maps to σ . Explicitly:

$$\tilde{N}_\chi: B \rightarrow B, \quad \tilde{N}_\chi(b) = \sum_{l=0}^{p-2} (p-1-l)g^l b \quad \text{for all } b \in B.$$

A simple calculation shows that

$$(5.2) \quad (g-1)\tilde{N}_\chi(b) = N_{G/H}(b) - pb \quad \text{for all } b \in B.$$

For all $i \geq 0$, we have the induced maps $\tilde{N}_\chi: H^i(H, B) \rightarrow H^i(H, B)$.

Lemma 5.3. *Let p be a prime, let G be a profinite group, and let $\chi_1, \chi_2 \in H^1(G, \mathbb{Z}/p\mathbb{Z})$. Suppose that $\chi_1 \neq 0$, and set $H := \text{Ker}(\chi_1)$.*

(1) *Let $\psi \in H^1(H, \mathbb{Z}/p\mathbb{Z})$ be such that $\text{Cor}_H^G(\psi) = \chi_2$, and define*

$$\eta := \tilde{N}_{\chi_1}(\psi) \in H^1(H, \mathbb{Z}/p\mathbb{Z}).$$

Then there exists a continuous homomorphism $G \rightarrow U_3$ given by a matrix

$$(5.3) \quad \begin{bmatrix} 1 & \chi_1 & \rho \\ 0 & 1 & \chi_2 \\ 0 & 0 & 1 \end{bmatrix}$$

such that $\rho|_H = \eta$.

(2) Suppose that $p = 2$. For all $\psi \in H^1(H, \mathbb{Z}/2\mathbb{Z})$ such that $\text{Cor}_H^G(\psi) = \chi_2$, there exists a continuous homomorphism $G \rightarrow U_3$ as in (5.3) such that $\rho|_H = \psi$. Conversely, given a continuous homomorphism $G \rightarrow U_3$ as in (5.3) and setting $\psi := \rho|_H$, we have $\text{Cor}_H^G(\psi) = \chi_2$.

Proof. (1) We have $U_3 = V \rtimes C$, where

$$V = \begin{bmatrix} 1 & 0 & * \\ & 1 & * \\ & & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & * & 0 \\ & 1 & 0 \\ & & 1 \end{bmatrix}.$$

We let C act on V by conjugation. We identify C and $\mathbb{Z}/p\mathbb{Z}$ via the coordinate map $u_{1,2}$, and we write V_1 for the twist of V by $\chi_1: G \rightarrow C = \mathbb{Z}/p\mathbb{Z}$.

Let $g \in G$ be such that $\chi_1(g) = 1$. We define $j: V_1 \rightarrow \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z})$ by sending

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

to the constant function 1 and the function mapping $g^i H$ to $i-1$ for $i = 0, \dots, p-1$, respectively. We have the following commutative diagram:

$$(5.4) \quad \begin{array}{ccccc} & & \tilde{N}_{\chi_1} & & \\ & & \curvearrowright & & \\ \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z}) & \xrightarrow{\mu} & V_1 & \xleftarrow{j} & \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z}) \\ & \parallel & \downarrow \pi & & \downarrow g^{-1} \\ \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z}) & \xrightarrow{\nu} & \mathbb{Z}/p\mathbb{Z} & \xleftarrow{i} & \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z}), \\ & & \curvearrowright & & \\ & & N_{G/H} & & \end{array}$$

where μ is defined by the commutativity of the top triangle, and i and ν are the maps of (1.1) and (1.2) for $A = \mathbb{Z}/p\mathbb{Z}$. Indeed, the bottom triangle commutes by a direct calculation, the outer rectangle commutes by (5.2), the right square commutes by a direct calculation, and by the injectivity of the right horizontal maps this implies the commutativity of the left square.

Let $q: \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z}) \rightarrow \mathbb{Z}/p\mathbb{Z}$ be given by evaluation at the identity of G : it is a homomorphism of trivial H -modules. The Faddeev–Shapiro isomorphism

$$\varphi: H^1(G, \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z})) \xrightarrow{\text{Res}} H^1(H, \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z})) \xrightarrow{q_*} H^1(H, \mathbb{Z}/p\mathbb{Z})$$

fits into a commutative square

$$(5.5) \quad \begin{array}{ccc} H^1(G, \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z})) & \xrightarrow{\varphi} & H^1(H, \mathbb{Z}/p\mathbb{Z}) \\ \downarrow \nu_* & & \downarrow \text{Cor}_H^G \\ H^1(G, \mathbb{Z}/p\mathbb{Z}) & \xlongequal{\quad} & H^1(G, \mathbb{Z}/p\mathbb{Z}); \end{array}$$

see [NSW08, Proposition (1.6.5)]. Let $\psi_0 := \varphi^{-1}(\psi)$ and $\eta_0 := \varphi^{-1}(\eta)$, so that $\tilde{N}_{\chi_1}(\psi_0) = \eta_0$. The homomorphism $H^1(G, \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z})) \rightarrow H^1(G, V_1)$ coming from (5.4) sends ψ_0 to a class

$$h_0 := \begin{bmatrix} 1 & 0 & \rho \\ 0 & 1 & \chi \\ 0 & 0 & 1 \end{bmatrix} \in H^1(G, V_1).$$

The commutativity of the right square of (5.4) implies that $\chi = \pi_*(h_0) = \nu_*(\eta_0)$, and by (5.5) we have $\nu_*(\psi_0) = \text{Cor}_H^G(\psi) = \chi_2$. Therefore $\chi = \chi_2$. We have a commutative square of H -modules with trivial action

$$(5.6) \quad \begin{array}{ccc} V_1 & \xleftarrow{j} & \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z}) \\ \downarrow u_{1,3} & & \downarrow q \\ \mathbb{Z}/p\mathbb{Z} & \xlongequal{\quad} & \mathbb{Z}/p\mathbb{Z}, \end{array}$$

where the top horizontal map comes from (5.4). We obtain the commutative square

$$(5.7) \quad \begin{array}{ccc} H^1(G, V_1) & \xrightarrow{j_*} & H^1(G, \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z})) \\ \downarrow \text{Res} & & \downarrow \text{Res} \\ H^1(H, V_1) & \xrightarrow{j_*} & H^1(H, \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z})) \\ \downarrow (u_{1,3})_* & & \downarrow q_* \\ H^1(H, \mathbb{Z}/p\mathbb{Z}) & \xlongequal{\quad} & H^1(H, \mathbb{Z}/p\mathbb{Z}), \end{array} \quad \left. \begin{array}{l} \phantom{H^1(H, \mathbb{Z}/p\mathbb{Z})} \\ \phantom{H^1(H, \mathbb{Z}/p\mathbb{Z})} \\ \phantom{H^1(H, \mathbb{Z}/p\mathbb{Z})} \end{array} \right\} \varphi$$

where the bottom square is induced by (5.6). We know from (5.4) that the map $j_*: H^1(G, V_1) \rightarrow H^1(G, \text{Ind}_H^G(\mathbb{Z}/p\mathbb{Z}))$ sends h_0 to $\tilde{N}_{\chi_1}(\psi_0) = \eta_0$. On the other hand, $\varphi(\eta_0) = \eta$ and the composition of the left vertical maps sends h_0 to $\rho|_H$. Thus $\rho|_H = \eta$.

By [KMRT98, Proposition (28.8)], the twisting map $Z^1(G, V_1) \rightarrow Z^1(G, U_3)$ sends h_0 to

$$\begin{bmatrix} 1 & 0 & \rho \\ 0 & 1 & \chi_2 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & \chi_1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \chi_1 & \rho \\ 0 & 1 & \chi_2 \\ 0 & 0 & 1 \end{bmatrix}.$$

This matrix defines a continuous homomorphism $G \rightarrow U_3$ such that $\rho|_H = \eta$.

(2) Since $\tilde{N}_{\chi_1}(\psi) = \psi$ when $p = 2$, the first part of (2) follows from an application of (1) to $\eta = \psi$. We now prove the second part of (2). Let $g \in G - H$. The map $g - 1: \text{Ind}_H^G(\mathbb{Z}/2\mathbb{Z}) \rightarrow \text{Ind}_H^G(\mathbb{Z}/2\mathbb{Z})$ factors through $\nu: \text{Ind}_H^G(\mathbb{Z}/2\mathbb{Z}) \rightarrow \mathbb{Z}/2\mathbb{Z}$. Therefore the right square of (5.4) yields a commutative square

$$\begin{array}{ccc} V_1 & \xrightarrow{j} & \text{Ind}_H^G(\mathbb{Z}/2\mathbb{Z}) \\ \downarrow \pi & & \downarrow \nu \\ \mathbb{Z}/2\mathbb{Z} & \xlongequal{\quad} & \mathbb{Z}/2\mathbb{Z}. \end{array}$$

We obtain a commutative diagram

$$\begin{array}{ccccc} H^1(G, V_1) & \xrightarrow{j_*} & H^1(G, \text{Ind}_H^G(\mathbb{Z}/2\mathbb{Z})) & \xrightarrow{\varphi} & H^1(H, \mathbb{Z}/2\mathbb{Z}) \\ \downarrow \pi_* & & \downarrow \nu_* & & \downarrow \text{Cor}_H^G \\ H^1(G, \mathbb{Z}/2\mathbb{Z}) & \xlongequal{\quad} & H^1(G, \mathbb{Z}/2\mathbb{Z}) & \xlongequal{\quad} & H^1(G, \mathbb{Z}/2\mathbb{Z}), \end{array}$$

where the right square is (5.5). Consider the class

$$h := \begin{bmatrix} 1 & 0 & \rho \\ 0 & 1 & \chi_2 \\ 0 & 0 & 1 \end{bmatrix} \in H^1(G, V_1).$$

We deduce that $\chi_2 = \pi_*(h) = \text{Cor}_H^G(\varphi(j_*(h)))$. By (5.7), we have $\varphi(j_*(h)) = \psi$, and hence $\chi_2 = \text{Cor}_H^G(\psi)$, as desired. \square

6. PROOF OF THEOREM 1.3

Proof of Theorem 1.3. It is clear that (3) implies (2), and it follows from the definition of triple Massey products that (1) and (2) are equivalent. It thus suffices to show that (2) implies (3).

Define $G' := \theta^{-1}(1 + p\mathbb{Z}_p)$. Then G' is an open subgroup of G , the index $[G : G']$ divides $p - 1$ and $(G', \theta|_{G'})$ is cyclotomic. Suppose that (2) implies (3) for all triple Massey products in $H^2(G', \mathbb{Z}/p\mathbb{Z})$. Then, as p does not divide $[G : G']$, by [MT16, Proposition 4.14] we deduce that (2) implies for (3) for all triple Massey products in $H^2(G, \mathbb{Z}/p\mathbb{Z})$. Replacing (G, θ) by $(G', \theta|_{G'})$, we may thus assume that (G, θ) is cyclotomic. Moreover, by Lemma 5.1 we may suppose that $\chi_1 \neq 0$ and $\chi_3 \neq 0$.

By Theorem 1.5, the pair (G, θ) admits a Hilbert 90 module M . Fix an inclusion $\iota: \mathbb{Z}/p\mathbb{Z} \hookrightarrow M$, and let $a, b, c \in M^G$ such that $\chi_1 = \chi_a$, $\chi_2 = \chi_b$ and $\chi_3 = \chi_c$; see below (2.2) for the notation. Since $\chi_a \cup \chi_b = 0$, by Corollary 3.3 there exists $\alpha \in M^{G_a}$ such that $b = N_{G/G_a}(\alpha)$.

By Lemma 5.3(1), letting $\eta := \tilde{N}_{\chi_a}(\alpha) \in M^{G_a}$, there exists a continuous homomorphism $G \rightarrow U_3$ given by a matrix

$$\begin{bmatrix} 1 & \chi_a & \rho \\ 0 & 1 & \chi_b \\ 0 & 0 & 1 \end{bmatrix}$$

such that $\rho|_{G_a} = \chi_\eta$. Similarly, since $\chi_b \cup \chi_c = 0$ there exists $\gamma \in M^{G_c}$ such that $N_{G/G_c}(\gamma) = b$. Letting $\mu := \tilde{N}_{\chi_a}(\gamma) \in M^{G_a}$, there exists a continuous homomorphism $G \rightarrow U_3$ given by a matrix

$$\begin{bmatrix} 1 & \chi_b & \pi \\ 0 & 1 & \chi_c \\ 0 & 0 & 1 \end{bmatrix}$$

such that $\pi|_{G_c} = \chi_\mu$. The matrix

$$\begin{bmatrix} 1 & \chi_a & \rho & \square \\ 0 & 1 & \chi_b & \pi \\ 0 & 0 & 1 & \chi_c \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

defines a continuous homomorphism $G \rightarrow \overline{U}_4$. The obstruction to lifting this homomorphism to U_4 is given by

$$\varepsilon := \chi_a \cup \pi + \rho \cup \chi_c \in H^2(G, \mathbb{Z}/p\mathbb{Z}).$$

Suppose first that χ_a and χ_c are linearly dependent in $H^1(G, \mathbb{Z}/p\mathbb{Z})$. In this case $\text{Res}_{G_a}^G(\varepsilon) = 0$, and so by Proposition 3.2 we have $\varepsilon = \chi_a \cup \chi_u$ for some $u \in M$. Consider the continuous homomorphism $G \rightarrow \overline{U}_4$ defined by the matrix

$$\begin{bmatrix} 1 & \chi_a & \rho & \square \\ 0 & 1 & \chi_b & \pi - \chi_u \\ 0 & 0 & 1 & \chi_c \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The obstruction to lifting this homomorphism to U_4 is given by

$$\chi_a \cup (\pi - \chi_u) + \rho \cup \chi_c = \varepsilon - \chi_a \cup \chi_u = 0,$$

and hence this homomorphism lifts to U_4 . The conclusion follows from Theorem 5.2.

Suppose now that χ_a and χ_c are linearly independent in $H^1(G, \mathbb{Z}/p\mathbb{Z})$. Then $G_a \neq G_c$, and hence

$$N_{G_{a+c}/G_a \cap G_c}(\alpha - \gamma) = N_{G/G_a}(\alpha) - N_{G/G_c}(\gamma) = b - b = 0.$$

Let $g \in G_{a+c}$ such that $\chi_a(g) = 1$. By Lemma 2.5, M is a Hilbert 90 module for $(G_a, \theta|_{G_a})$, and hence by Lemma 2.6 we have an exact sequence

$$M^{G_a \cap G_c} \xrightarrow{g-1} M^{G_a \cap G_c} \xrightarrow{N_{G/G_c}} M^{G_a}.$$

Therefore there exists $\omega \in M^{G_a \cap G_c}$ such that $(g-1)\omega = \alpha - \gamma$. Set

$$e := \eta + N_{G/G_c}(\omega) \in M^{G_a}.$$

Then

$$\begin{aligned} (g-1)e &= (g-1)\eta + (g-1)(N_{G/G_c}(\omega)) \\ &= (N_{G/G_a} - p)(\alpha) + N_{G/G_c}((g-1)\omega) \\ &= b - p\alpha + N_{G/G_c}(\alpha - \gamma) \\ &= b - p\alpha + p\alpha - b \\ &= 0, \end{aligned}$$

which proves that $e \in M^G$. We have

$$\text{Res}_{G_a}^G(\varepsilon) = \rho|_{G_a} \cup \chi_c = \chi_\eta \cup \chi_c = \chi_e \cup \chi_c \quad \text{in } H^2(G_a, \mathbb{Z}/p\mathbb{Z}),$$

that is, $\text{Res}_{G_a}^G(\varepsilon - \chi_e \cup \chi_c) = 0$ in $H^2(G_a, \mathbb{Z}/p\mathbb{Z})$. By Proposition 4.5 applied to $\chi = \chi_a$, there exists $f \in M^G$ such that $\varepsilon - \chi_e \cup \chi_c = \chi_a \cup \chi_f$ in $H^2(G, \mathbb{Z}/p\mathbb{Z})$, and hence

$$\varepsilon = \chi_a \cup \chi_f + \chi_e \cup \chi_c \quad \text{in } H^2(G, \mathbb{Z}/p\mathbb{Z}).$$

Consider the continuous homomorphism $G \rightarrow \overline{U}_4$ given by the matrix

$$\begin{bmatrix} 1 & \chi_a & \rho - \chi_e & \square \\ 0 & 1 & \chi_b & \pi - \chi_f \\ 0 & 0 & 1 & \chi_c \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The obstruction to lifting this homomorphism to U_4 is given by

$$\chi_a \cup (\pi - \chi_f) + (\rho - \chi_e) \cup \chi_c = \varepsilon - \chi_a \cup \chi_f - \chi_e \cup \chi_c = 0,$$

and hence this homomorphism lifts to U_4 . By Theorem 5.2, the Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle$ vanishes, as desired. \square

Remark 6.1. When $p > 2$, it is proved in [LLSWW23, Proposition 6.1.4, Theorem 6.2.1] that if the sequence of Corollary 4.5 is exact at $H^1(G, \mathbb{Z}/p\mathbb{Z})$ for a profinite group G , then the conclusion of Theorem 1.3 holds for G . On the other hand, when $p = 2$, the exactness of the sequence of Corollary 4.5 is satisfied by all profinite groups G (see Remark 4.6), and so it cannot imply the conclusion of Theorem 1.3.

We emphasize that, even when p is odd, Theorem 1.3 does not follow from [LLSWW23, Theorem 6.2.1]. Indeed, the proof of Theorem 1.3 relies on the construction of a Hilbert 90 module given by Theorem 1.5. Moreover, our proof of Theorems 1.3 and 1.5 is uniform in p and applies to $p = 2$ as well.

Remark 6.2. Theorem 1.3 proves the first half of a conjecture of Quadrelli [Qua21, Conjecture 1.5], which predicts that Theorem 1.3 might be true under the further assumption that $\text{Im}(\theta) \subset 1 + 4\mathbb{Z}_2$ when $p = 2$. The second half of [Qua21, Conjecture 1.5] predicts that, under the same assumptions, a fourfold Massey product $\langle \chi_1, \chi_2, \chi_3, \chi_4 \rangle \subset H^2(G, \mathbb{Z}/p\mathbb{Z})$ vanishes as soon as $\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = \chi_3 \cup \chi_4 = 0$. This is false in general; see [MS22, Theorem 1.6].

Remark 6.3. Consider the group G given by the following presentation:

$$G := \langle x_1, x_2, x_3, x_4, x_5 : [[x_1, x_2], x_3][x_4, x_5] = 1 \rangle.$$

Let p be a prime number, and write \hat{G} for the pro- p completion of G . By [MT17, Example 7.2], there is a triple Massey product $\langle \chi_1, \chi_2, \chi_3 \rangle \subset H^2(\hat{G}, \mathbb{Z}/p\mathbb{Z})$ which is defined but non-vanishing. By Theorem 1.3, we conclude that (\hat{G}, θ) does not satisfy formal Hilbert 90 for any orientation θ . When p is odd, this fact already been proved by Quadrelli [Qua21, Theorem 1.5].

7. PROOF OF THEOREM 1.4

Proposition 7.1. *Let (G, θ) be a p -oriented profinite group satisfying formal Hilbert 90, and let $\chi_1, \chi_2, \chi_3 \in H^1(G, \mathbb{Z}/2\mathbb{Z})$. Suppose that $\chi_1 \neq 0$ and let $H := \text{Ker}(\chi_1)$.*

(1) *The Massey product $\langle \chi_1, \chi_2, \chi_3, \chi_1 \rangle$ vanishes if and only if there exist φ and ψ in $H^1(H, \mathbb{Z}/2\mathbb{Z})$ such that $\text{Cor}_H^G(\varphi) = \chi_2$, $\text{Cor}_H^G(\psi) = \chi_3$, $\varphi \cup \psi = 0$ and $\varphi \cup \text{Res}_H^G(\chi_3) = 0$.*

(2) *The Massey product $\langle \chi_1, \chi_2, \chi_3, \chi_1 \rangle$ is defined if and only if there exist φ and ψ in $H^1(H, \mathbb{Z}/2\mathbb{Z})$ such that $\text{Cor}_H^G(\varphi) = \chi_2$, $\text{Cor}_H^G(\psi) = \chi_3$, $\varphi \cup \psi$ belongs to the image of $\text{Res}: H^2(G, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(H, \mathbb{Z}/2\mathbb{Z})$ and $\varphi \cup \text{Res}_H^G(\chi_3) = 0$.*

Proof. Let P be the normal subgroup of $U_5 \subset \text{GL}_5(\mathbb{F}_2)$ given by

$$P := \begin{bmatrix} 1 & 0 & 0 & * & * \\ & 1 & 0 & * & * \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix}.$$

Note that P is the kernel of the surjective homomorphism $U_5 \rightarrow U_3 \times U_3$ which forgets the 2×2 upper-right square of a unitriangular matrix. We write \bar{P} for the

quotient of P by the center of U_5 . We obtain a commutative diagram

$$(7.1) \quad \begin{array}{ccccccc} & & 1 & & 1 & & \\ & & \downarrow & & \downarrow & & \\ & & \mathbb{Z}/2\mathbb{Z} & \xlongequal{\quad} & \mathbb{Z}/2\mathbb{Z} & & \\ & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & P & \longrightarrow & U_5 & \longrightarrow & U_3 \times U_3 \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \parallel \\ 1 & \longrightarrow & \bar{P} & \longrightarrow & \bar{U}_5 & \longrightarrow & U_3 \times U_3 \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \\ & & 1 & & 1 & & \end{array}$$

where the rows and columns are short exact sequences. Since P is abelian, the rows endow P and \bar{P} with the structure of $(U_3 \times U_3)$ -modules, and the quotient map $P \rightarrow \bar{P}$ is $(U_3 \times U_3)$ -equivariant.

Lemma 7.2. *Let $\varphi, \psi \in H^1(H, \mathbb{Z}/2\mathbb{Z})$ be such that $\text{Cor}_H^G(\varphi) = \chi_2$ and $\text{Cor}_H^G(\psi) = \chi_3$, and let $h, h' : G \rightarrow U_3$ be continuous homomorphisms given by matrices*

$$(7.2) \quad \begin{bmatrix} 1 & \chi_1 & \rho \\ 0 & 1 & \chi_2 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & \chi_3 & \rho' \\ 0 & 1 & \chi_1 \\ 0 & 0 & 1 \end{bmatrix},$$

where $\rho|_H = \varphi$ and $(\rho')|_H = \psi$.

(1) *The homomorphism $(h, h') : G \rightarrow U_3 \times U_3$ lifts to a continuous homomorphism $G \rightarrow U_5$ if and only if $\varphi \cup \psi = \varphi \cup \text{Res}_H^G(\chi_3) = 0$.*

(2) *The homomorphism $(h, h') : G \rightarrow U_3 \times U_3$ lifts to a continuous homomorphism $G \rightarrow \bar{U}_5$ if and only if $\varphi \cup \psi$ belongs to the image of $H^2(G, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(H, \mathbb{Z}/2\mathbb{Z})$ and $\varphi \cup \text{Res}_H^G(\chi_3) = 0$.*

Proof. Consider the following normal subgroups of U_3 :

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

We have an isomorphism of $(U_3 \times U_3)$ -modules $N \otimes N' \rightarrow P$ given by

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

We obtain a homomorphism

$$H^1(U_3, N) \otimes H^1(U_3, N') \xrightarrow{\cup} H^2(G, P).$$

The natural projections $t : U_3 \rightarrow N$ and $t' : U_3 \rightarrow N'$ are 1-cocycles, and a direct calculation shows that the class of the middle row of (7.1) in $H^2(U_3 \times U_3, P)$ is

equal to $t \cup t'$. Consider the commutative diagram

$$\begin{array}{ccc}
H^1(U_3, N) \otimes H^1(U_3, N') & \xrightarrow{\cup} & H^2(U_3 \times U_3, P) \\
\downarrow h^* \otimes (h')^* & & \downarrow (h, h')^* \\
H^1(G, N) \otimes H^1(G, N') & \xrightarrow{\cup} & H^2(G, P) \\
\downarrow \text{Res} \otimes \text{Res} & & \downarrow \text{Res} \\
H^1(H, N) \otimes H^1(H, N') & \xrightarrow{\cup} & H^2(H, P).
\end{array}$$

It follows that the map $H^1(U_3 \times U_3, P) \rightarrow H^2(H, P)$ sends

$$(7.3) \quad t \cup t' \mapsto \begin{bmatrix} 1 & 0 & 0 & \varphi \cup \text{Res}_H^G(\chi_3) & \varphi \cup \psi \\ & 1 & 0 & \text{Res}_H^G(\chi_2 \cup \chi_3) & \text{Res}_H^G(\chi_2) \cup \psi \\ & & 1 & 0 & 0 \\ & & & 1 & 0 \\ & & & & 1 \end{bmatrix}.$$

(1) The homomorphism $(h, h'): G \rightarrow U_3 \times U_3$ lifts to U_5 if and only if the image of $t \cup t'$ in $H^2(G, P)$ vanishes. Since

$$P \simeq N \otimes N' \simeq \text{Ind}_H^G(\mathbb{Z}/2\mathbb{Z})^{\otimes 2} \simeq \text{Ind}_H^G((\mathbb{Z}/2\mathbb{Z})^{\oplus 2}),$$

we have the Faddeev–Shapiro isomorphism

$$H^2(G, P) \xrightarrow{\text{Res}} H^2(H, P) \rightarrow H^2(H, (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}),$$

and hence the restriction $H^2(G, P) \rightarrow H^2(H, P)$ is injective. Therefore, (h, h') lifts to U_5 if and only if the image of $t \cup t'$ in $H^2(H, P)$ vanishes. In view of (7.3), this is equivalent to

$$\varphi \cup \psi = \varphi \cup \text{Res}_H^G(\chi_3) = \text{Res}_H^G(\chi_2) \cup \psi = \text{Res}_H^G(\chi_2 \cup \chi_3) = 0.$$

This implies that $\varphi \cup \psi = \varphi \cup \text{Res}_H^G(\chi_3) = 0$ in $H^2(H, \mathbb{Z}/2\mathbb{Z})$, but it is in fact equivalent to this. Indeed, if $\varphi \cup \psi = \varphi \cup \text{Res}_H^G(\chi_3) = 0$, then by the projection formula we have

$$\chi_2 \cup \chi_3 = \text{Cor}_H^G(\varphi) \cup \chi_3 = \text{Cor}_H^G(\varphi \cup \text{Res}_H^G(\chi_3)) = 0,$$

and hence $\text{Res}_H^G(\chi_2 \cup \chi_3) = 0$. Moreover, letting $g \in G - H$, we have

$$\varphi \cup g(\psi) = \varphi \cup \text{Res}_H^G(\chi_3) + \varphi \cup \psi = 0 + 0 = 0,$$

and hence

$$\text{Res}_H^G(\chi_2) \cup \psi = \varphi \cup \psi + g(\varphi) \cup \psi = \varphi \cup \psi + g(\varphi \cup g(\psi)) = 0 + 0 = 0.$$

(2) The left vertical sequence in (7.1) induces an exact sequence

$$(7.4) \quad H^2(G, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(G, P) \rightarrow H^2(G, \bar{P}).$$

The homomorphism $(h, h'): G \rightarrow U_3 \times U_3$ lifts to a homomorphism $G \rightarrow \bar{U}_5$ if and only if the pullback of the middle row of (7.1) along (h, h') splits, that is, if and only if the corresponding element in $H^2(G, \bar{P})$ is trivial. In view of (7.4), this

happens if and only if the image of $t \cup t'$ in $H^2(G, P)$ belongs to the image of $H^2(G, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(G, P)$. We have a commutative square

$$\begin{array}{ccc} H^2(G, \mathbb{Z}/2\mathbb{Z}) & \longrightarrow & H^2(G, P) \\ \downarrow \text{Res} & & \downarrow \text{Res} \\ H^2(H, \mathbb{Z}/2\mathbb{Z}) & \longrightarrow & H^2(H, P), \end{array}$$

where, as explained earlier, the right vertical map is injective by the Faddeev–Shapiro lemma. Therefore the image of $t \cup t'$ in $H^2(G, P)$ belongs to the image of $H^2(G, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(G, P)$ if and only if the image of $t \cup t'$ in $H^2(H, P)$ belongs to the image of the composition $H^2(G, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(H, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(H, P)$. By (7.3), this is equivalent to the existence of $u \in H^2(G, \mathbb{Z}/2\mathbb{Z})$ such that

$$\varphi \cup \psi = u, \quad \varphi \cup \text{Res}_H^G(\chi_3) = \text{Res}_H^G(\chi_2) \cup \psi = \text{Res}_H^G(\chi_2 \cup \chi_3) = 0.$$

This implies that $\varphi \cup \psi$ comes from $H^2(G, \mathbb{Z}/2\mathbb{Z})$ and that $\varphi \cup \text{Res}_H^G(\chi_3) = 0$, but it is in fact equivalent to this. Indeed, given $u \in H^2(G, \mathbb{Z}/2\mathbb{Z})$ such that $\varphi \cup \psi = u$ and $\varphi \cup \text{Res}_H^G(\chi_3) = 0$, by the projection formula we have $\chi_2 \cup \chi_3 = 0$, and hence $\text{Res}_H^G(\chi_2 \cup \chi_3) = 0$. Moreover, letting $g \in G - H$, we have

$$\varphi \cup g(\psi) = \varphi \cup \text{Res}_H^G(\chi_3) + \varphi \cup \psi = 0 + u = u,$$

and hence

$$\text{Res}_H^G(\chi_2) \cup \psi = \varphi \cup \psi + g(\varphi) \cup \psi = \varphi \cup \psi + g(\varphi \cup g(\psi)) = u + g(u) = 0. \quad \square$$

Using Lemma 7.2, we complete the proof of Proposition 7.1 as follows. Suppose first that the Massey product $\langle \chi_1, \chi_2, \chi_3, \chi_1 \rangle$ vanishes (resp. is defined). By Theorem 5.2, the homomorphism $(\chi_1, \chi_2, \chi_3, \chi_1): G \rightarrow (\mathbb{Z}/2\mathbb{Z})^4$ lifts to a homomorphism $G \rightarrow U_5$ (resp. $G \rightarrow \bar{U}_5$) and hence to a homomorphism $(h, h'): G \rightarrow U_3 \times U_3$ given by matrices as in (7.2). We let $\varphi, \psi \in H^1(H, \mathbb{Z}/2\mathbb{Z})$ be such that $\rho|_H = \varphi$ and $(\rho')|_H = \psi$. By Lemma 5.3(2), we have $\text{Cor}_H^G(\varphi) = \chi_2$ and $\text{Cor}_H^G(\psi) = \chi_3$ in $H^1(G, \mathbb{Z}/2\mathbb{Z})$. By construction, (h, h') lifts to U_5 (resp. \bar{U}_5), hence Lemma 7.2 implies that $\varphi \cup \psi = \varphi \cup \text{Res}_H^G(\chi_3) = 0$ in $H^1(H, \mathbb{Z}/2\mathbb{Z})$ (resp. $\varphi \cup \psi$ comes from $H^2(G, \mathbb{Z}/2\mathbb{Z})$ and $\varphi \cup \text{Res}_H^G(\chi_3) = 0$ in $H^1(H, \mathbb{Z}/2\mathbb{Z})$).

Conversely, let $\varphi, \psi \in H^1(H, \mathbb{Z}/2\mathbb{Z})$ be such that $\text{Cor}_H^G(\varphi) = \chi_2$, $\text{Cor}_H^G(\psi) = \chi_3$, and $\varphi \cup \psi = \varphi \cup \text{Res}_H^G(\chi_3) = 0$ in $H^1(H, \mathbb{Z}/2\mathbb{Z})$ (resp. $\varphi \cup \psi$ comes from $H^2(G, \mathbb{Z}/2\mathbb{Z})$ and $\varphi \cup \text{Res}_H^G(\chi_3) = 0$ in $H^1(H, \mathbb{Z}/2\mathbb{Z})$). By Lemma 5.3(2), there exist homomorphisms $h, h': G \rightarrow U_3$ as in (7.2) such that $\rho|_H = \varphi$ and $(\rho')|_H = \psi$. By Lemma 7.2, the homomorphism (h, h') lifts to U_5 (resp. \bar{U}_5). On the other hand, the homomorphism $(h, h'): G \rightarrow U_3 \times U_3$ is a lift of $(\chi_1, \chi_2, \chi_3, \chi_1): G \rightarrow (\mathbb{Z}/2\mathbb{Z})^4$. Therefore $(\chi_1, \chi_2, \chi_3, \chi_1)$ lifts to U_5 (resp. \bar{U}_5). By Theorem 5.2, the Massey product $\langle \chi_1, \chi_2, \chi_3, \chi_1 \rangle$ is defined. \square

Proposition 7.3. *Let (G, θ) be a 2-oriented profinite group, let M be a Hilbert 90 module for (G, θ) , let $a, b \in M^G$, and suppose that $\chi_a \neq 0$ and $\chi_b \neq 0$. Let $\alpha \in M^{G_a}$ be such that $N_{G/G_a}(\alpha) = b$ and $\beta \in M^{G_b}$ such that $N_{G/G_b}(\beta) = a$.*

Then we have an exact sequence of G -modules

$$M^{(G_a)\alpha} \oplus M^{G_b} \xrightarrow{\pi} M^{G_a} \xrightarrow{\lambda} H^2(G, M) \xrightarrow{\text{Res}} H^2((G_b)_\beta, M),$$

where

$$\pi(\zeta, \eta) = N_{G_a/(G_a)\alpha}(\zeta) - N_{G/G_b}(\eta)$$

and $\lambda(\delta)$ is the image of $\text{Cor}_{G_a}^G(\chi_\alpha \cup \chi_\delta) \in H^2(G, \mathbb{Z}/2\mathbb{Z})$ in $H^2(G, M)$.

Proof. We define the following elements of U_3 :

$$\sigma_1 := \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \sigma_2 := \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \tau := [\sigma_1, \sigma_2] = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

We have the following exact sequence of U_3 -modules:

$$(7.5) \quad 0 \rightarrow \mathbb{Z}[U_3/\langle \sigma_2, \tau \rangle] \xrightarrow{f} \mathbb{Z}[U_3/\langle \sigma_2 \rangle] \oplus \mathbb{Z}[U_3/\langle \sigma_1, \tau \rangle] \xrightarrow{g} \mathbb{Z}[U_3/\langle \sigma_1 \rangle] \oplus \mathbb{Z} \xrightarrow{k} \mathbb{Z} \rightarrow 0,$$

where

$$\begin{aligned} f(1) &= (1 + \tau, -1 - \sigma_2), \\ g(1, 0) &= (1 + \sigma_2, -1), \\ g(0, 1) &= (1 + \tau, -1), \\ k(1, 0) &= 1, \\ k(0, 1) &= 2. \end{aligned}$$

By Lemma 5.3(2), there exists a continuous homomorphism $h: G \rightarrow U_3$ given by a matrix (5.3) such that $\rho|_{G_a} = \chi_\alpha$. Since χ_a and χ_b are non-zero, either h is surjective or the image of h is the subgroup of U_3 generated by $\sigma_1\sigma_2$. In either case, we have

$$(7.6) \quad [G : G_a] = [G : G_b] = 2, \quad [G : (G_a)_\alpha] = [G : (G_b)_\beta] = 4.$$

We regard (7.5) as an exact sequence of G -modules via h . In view of (7.6), an application of the functor $\text{Hom}_{\mathbb{Z}}(-, M)$ yields the exact sequence of G -modules

$$(7.7) \quad 0 \rightarrow M \xrightarrow{\mu} \text{Ind}_{(G_b)_\beta}^G(M) \oplus M \xrightarrow{\varepsilon} \text{Ind}_{(G_a)_\alpha}^G(M) \oplus \text{Ind}_{G_b}^G(M) \xrightarrow{\pi} \text{Ind}_{G_a}^G(M) \rightarrow 0,$$

where

$$\pi(\zeta, \eta) = N_{G_a/(G_a)_\alpha}(\zeta) - N_{G/G_b}(\eta).$$

Let $T = \text{Ker}(\pi) = \text{Coker}(\mu)$. Since M is a Hilbert 90 module for G , by Lemma 2.5 it is also a Hilbert 90 module for the open subgroups $(G_a)_\alpha$, G_b and $(G_b)_\beta$, and hence by Faddeev–Shapiro’s lemma

$$\begin{aligned} H^1(G, \text{Ind}_{(G_b)_\beta}^G(M) \oplus M) &= H^1((G_b)_\beta, M) \oplus H^1(G, M) = 0, \\ H^1(G, \text{Ind}_{(G_a)_\alpha}^G(M) \oplus \text{Ind}_{G_b}^G(M)) &= H^1((G_a)_\alpha, M) \oplus H^1(G_b, M) = 0. \end{aligned}$$

Thus (7.7) yields the exact sequences

$$M^{(G_a)_\alpha} \oplus M^{G_b} \xrightarrow{\pi} M^{G_a} \rightarrow H^1(G, T) \rightarrow 0$$

and

$$0 \rightarrow H^1(G, T) \rightarrow H^2(G, M) \xrightarrow{\text{Res}} H^2((G_b)_\beta, M).$$

We obtain an exact sequence of G -modules

$$M^{(G_a)_\alpha} \oplus M^{G_b} \xrightarrow{\pi} M^{G_a} \xrightarrow{\lambda'} H^2(G, M) \xrightarrow{\text{Res}} H^2((G_b)_\beta, M),$$

where λ' is defined as the composition $M^{G_a} \rightarrow H^1(G, T) \rightarrow H^2(G, M)$. It remains to show that $\lambda' = \lambda$.

Let $\delta \in M^{G_a}$. By Lemma 2.8, the homomorphism $H^2(G_a, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(G_a, M)$ sends $\chi_\alpha \cup \chi_\delta$ to $\omega_\alpha \cup \delta$, where $\omega_\alpha \in H^2(G_a, \mathbb{Z})$ is defined as the Bockstein of $\chi_\alpha \in H^1(G_a, \mathbb{Z}/2\mathbb{Z})$. Thus $\lambda(\delta) = \text{Cor}_{G_a}^G(\omega_\alpha \cup \delta)$.

Consider the following commutative diagram

$$(7.8) \quad \begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}[U_3/\langle\sigma_2, \tau\rangle] & \xrightarrow{f} & \mathbb{Z}[U_3/\langle\sigma_2\rangle] \oplus \mathbb{Z}[U_3/\langle\sigma_1, \tau\rangle] & \xrightarrow{g} & \mathbb{Z}[U_3/\langle\sigma_1\rangle] \oplus \mathbb{Z} & \xrightarrow{k} & \mathbb{Z} & \longrightarrow & 0 \\ & & \parallel & & \downarrow (1,0) & & \downarrow l & & \downarrow 1+\sigma_1 & & \\ 0 & \longrightarrow & \mathbb{Z}[U_3/\langle\sigma_2, \tau\rangle] & \xrightarrow{1+\tau} & \mathbb{Z}[U_3/\langle\sigma_2\rangle] & \xrightarrow{1-\tau} & \mathbb{Z}[U_3/\langle\sigma_2\rangle] & \xrightarrow{1} & \mathbb{Z}[U_3/\langle\sigma_2, \tau\rangle] & \longrightarrow & 0, \end{array}$$

where the top row is (7.5) and

$$\begin{aligned} l(1, 0) &= 1 + \sigma_1, \\ l(0, 1) &= 1 + \sigma_1 + \tau + \sigma_1\tau. \end{aligned}$$

The commutativity of (7.8) is easily verified using the explicit descriptions of the arrows. By applying the functor $\text{Hom}_{\mathbb{Z}}(-, M)$ to each term of (7.8), we obtain the following commutative diagram with exact rows:

$$(7.9) \quad \begin{array}{ccccccccc} 0 & \longrightarrow & \text{Ind}_{G_a}^G(M) & \longrightarrow & \text{Ind}_{(G_a)_\alpha}^G(M) & \xrightarrow{1-\tau} & \text{Ind}_{(G_a)_\alpha}^G(M) & \xrightarrow{\nu'} & \text{Ind}_{G_a}^G(M) & \longrightarrow & 0 \\ & & \downarrow \nu & & \downarrow & & \downarrow (1,0) & & \parallel & & \\ 0 & \longrightarrow & M & \xrightarrow{\mu} & \text{Ind}_{(G_b)_\beta}^G(M) \oplus M & \xrightarrow{\varepsilon} & \text{Ind}_{(G_a)_\alpha}^G(M) \oplus \text{Ind}_{G_b}^G(M) & \xrightarrow{\pi} & \text{Ind}_{G_a}^G(M) & \longrightarrow & 0. \end{array}$$

Here ν is the map of (1.2) for $H = G_a$ and $A = M$, and ν' is obtained by applying the functor $\text{Ind}_{G_a}^G$ to the map of (1.2) for the profinite group G_a , the open subgroup $H = (G_a)_\alpha$ and the G_a -module $A = \text{Ind}_{G_a}^G(M)$.

Let $N := \langle\sigma_2, \tau\rangle$. The bottom row of (7.8) is induced from the exact sequence of N -modules

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Z}[N/\langle\sigma_2\rangle] \xrightarrow{1-\tau} \mathbb{Z}[N/\langle\sigma_2\rangle] \rightarrow \mathbb{Z} \rightarrow 0.$$

This sequence may be viewed as a sequence of $N/\langle\sigma_2\rangle$ -modules. As $N/\langle\sigma_2\rangle$ is cyclic of order 2, by [GS17, Proposition 3.4.11] the induced map $\mathbb{Z} \rightarrow H^2(N/\langle\sigma_2\rangle, \mathbb{Z})$ sends 1 to the generator of $H^2(N/\langle\sigma_2\rangle, \mathbb{Z}/2\mathbb{Z})$, that is, to the Bockstein of the generator of $H^1(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$. It follows that the map $M^G \rightarrow H^2(G_a, M)$ induced by the top row of (7.9) is given by cup product with the Bockstein of χ_a , that is, with ω_a . Therefore (7.9) gives a commutative square

$$(7.10) \quad \begin{array}{ccc} M^{G_a} & \xrightarrow{(-) \cup \omega_a} & H^2(G_a, M) \\ \parallel & & \downarrow \text{Cor}_{G_a}^G \\ M^{G_a} & \xrightarrow{\lambda'} & H^2(G, M). \end{array}$$

We conclude that $\lambda'(\delta) = \text{Cor}_{G_a}^G(\omega_a \cup \delta) = \lambda(\delta)$, as desired. \square

Proof of Theorem 1.4. By Lemma 5.1, we may assume that $\chi_1 \neq 0$ and $\chi_2 \neq 0$. By Theorem 1.5, there exists a Hilbert 90 module M for (G, θ) . Let $\iota: \mathbb{Z}/2\mathbb{Z} \hookrightarrow M$ be the unique injective homomorphism, and let $a, b, c \in M^G$ be such that $\chi_1 = \chi_a$, $\chi_2 = \chi_b$ and $\chi_3 = \chi_c$; see below (2.2) for the notation. Since χ_a and χ_b are non-trivial, by Proposition 7.1(2) there exist $\alpha, \delta \in M^{G_a}$ such that $\text{Cor}_{G/G_a}(\chi_\alpha) = \chi_b$, $\text{Cor}_{G/G_a}(\chi_\delta) = \chi_c$, $\chi_\alpha \cup \chi_\delta$ belongs to the image of $H^2(G, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(G_a, \mathbb{Z}/2\mathbb{Z})$ and $\chi_\alpha \cup \chi_c = 0$ in $H^2(G_a, \mathbb{Z}/2\mathbb{Z})$.

Since $\chi_\alpha \cup \chi_\delta$ comes from $H^2(G, \mathbb{Z}/2\mathbb{Z})$, we have $\text{Cor}_{G_a}^G(\chi_\alpha \cup \chi_\delta) = 0$. As χ_a and χ_b are non-trivial, Proposition 7.3 implies that $\lambda(\delta) = 0$. It follows that δ belongs to the image of the map π appearing in Proposition 7.3, that is, $\delta = N_{G_a/(G_a)_\alpha}(\zeta) -$

$N_{G/G_b}(\eta)$ for some $\zeta \in M^{(G_a)_\alpha}$ and $\eta \in M^{G_b}$. Letting $z := N_{G/G_b}(\eta) \in M^G$, we obtain

$$\chi_\alpha \cup \chi_\delta = \chi_\alpha \cup \text{Cor}_{(G_a)_\alpha}^{G_a}(\zeta) + \chi_\alpha \cup \chi_z = \chi_\alpha \cup \chi_z \quad \text{in } H^2(G_a, \mathbb{Z}/2\mathbb{Z}).$$

It follows that $\chi_\alpha \cup \chi_{\delta+z} = 0$ in $H^2(G_a, \mathbb{Z}/2\mathbb{Z})$. Moreover,

$$N_{G/G_a}(\delta + z) = N_{G/G_a}(\delta) + 2z = c + 0 = c,$$

and so $\text{Cor}_{G_a}^G(\chi_{\delta+z}) = \chi_c$. We already know that $\chi_a \neq 0$, $\text{Cor}_{G_a}^G(\chi_\alpha) = \chi_b$ and $\chi_\alpha \cup \chi_c = 0$ in $H^1(G_a, \mathbb{Z}/p\mathbb{Z})$, the elements α and $\delta + z$ satisfy the conditions of Proposition 7.1(2). By Proposition 7.1(2), the Massey product $\langle \chi_1, \chi_2, \chi_3, \chi_1 \rangle$ vanishes. \square

8. AN EXAMPLE

In this section, we illustrate Theorem 1.3 with an example. Consider the group G given by the following presentation by generators and relations:

$$(8.1) \quad G := \langle a, b : a^2b = ba^2 \rangle.$$

As in the proof of Proposition 7.3, we define the following elements of $U_3 \subset \text{GL}_3(\mathbb{F}_2)$:

$$\sigma_1 := \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \sigma_2 := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad \tau := [\sigma_1, \sigma_2] = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The group G fits into the diagram with exact rows

$$(8.2) \quad \begin{array}{ccccccc} 1 & \longrightarrow & H & \longrightarrow & G & \xrightarrow{f} & \mathbb{Z}/2\mathbb{Z} \longrightarrow 1 \\ & & \downarrow \varphi|_H & & \downarrow \varphi & & \parallel \\ 1 & \longrightarrow & N' & \longrightarrow & U_3 & \xrightarrow{u_{2,3}} & \mathbb{Z}/2\mathbb{Z} \longrightarrow 1, \end{array}$$

where φ is determined by $\varphi(a) = \sigma_1$ and $\varphi(b) = \sigma_2$, the subgroup $H \subset G$ is defined as the kernel of f , and the subgroup $N' \subset U_3$ as the kernel of the coordinate map $u_{2,3}$.

Proposition 8.1. *Let \hat{G} be the pro-2 completion of G defined in (8.1) and let $\hat{H} \subset \hat{G}$ be the pro-2 completion of the subgroup $H \subset G$ considered in (8.2).*

(1) *The reduction maps $H^1(\hat{G}, \mathbb{Z}/2^n\mathbb{Z}) \rightarrow H^1(\hat{G}, \mathbb{Z}/2\mathbb{Z})$ are surjective for all $n \geq 1$.*

(2) *The reduction map $H^1(\hat{H}, \mathbb{Z}/4\mathbb{Z}) \rightarrow H^1(\hat{H}, \mathbb{Z}/2\mathbb{Z})$ is not surjective.*

(3) *There exist $\chi_1, \chi_2, \chi_3 \in H^1(\hat{G}, \mathbb{Z}/2\mathbb{Z})$ such that $\langle \chi_1, \chi_2, \chi_3 \rangle$ is defined but does not vanish.*

Proof of Proposition 8.1(1) and (2). (1) We have $G/[G, G] \simeq \mathbb{Z} \times \mathbb{Z}$, and hence the reduction maps $H^1(G, \mathbb{Z}/2^n\mathbb{Z}) \rightarrow H^1(G, \mathbb{Z}/2\mathbb{Z})$ are surjective for all $n \geq 1$. By the universal property of pro-2 completion, the canonical map $G \rightarrow \hat{G}$ induces isomorphisms $H^1(\hat{G}, \mathbb{Z}/2^n\mathbb{Z}) \rightarrow H^1(G, \mathbb{Z}/2^n\mathbb{Z})$ for all $n \geq 1$. It follows that the reduction maps $H^1(\hat{G}, \mathbb{Z}/2^n\mathbb{Z}) \rightarrow H^1(\hat{G}, \mathbb{Z}/2\mathbb{Z})$ are also surjective for all $n \geq 1$.

(2) We have $N' \simeq (\mathbb{Z}/2\mathbb{Z})^2$ and the map $u_{1,3}: N' \rightarrow \mathbb{Z}/2\mathbb{Z}$ is a homomorphism. Define $\chi := u_{1,3} \circ \varphi|_H \in H^1(H, \mathbb{Z}/2\mathbb{Z})$. Suppose by contradiction that χ lifts to some $\tilde{\chi} \in H^1(H, \mathbb{Z}/4\mathbb{Z})$.

Let $h := aba^{-1}b^{-1} \in H$. Then $\varphi(h) = \tau$ in N' , and hence $\chi(h) = 1$ in $\mathbb{Z}/2\mathbb{Z}$. Note that a belongs to H , and let $c := bab^{-1} \in H$, so that we have the identities $h = ac^{-1}$ and $c^2 = ba^2b^{-1} = a^2$ in H . Since the group $\mathbb{Z}/4\mathbb{Z}$ is abelian, we have $\tilde{\chi}(h^2) = \tilde{\chi}(a^2c^{-2}) = 0$ in $\mathbb{Z}/4\mathbb{Z}$. It follows that $\tilde{\chi}(h)$ belongs to $2\mathbb{Z}/4\mathbb{Z}$, and hence $\chi(h) = 0$, a contradiction. \square

Lemma 8.2. *Let p be a prime and $n \geq 3$ be an integer. Let $N \in \text{Mat}_{n+1}(\mathbb{F}_p)$ be such that $N_{i,j} = 1$ if $j = i + 1$ and $N_{i,j} = 0$ elsewhere.*

(1) *The U_{n+1} -centralizer of $I + N$ consists of all upper unitriangular matrices which are constant on all upper diagonals.*

(2) *The U_{n+1} -conjugacy class of $I + N$ consists of all upper unitriangular matrices M with entry 1 at $(i, i + 1)$ for all i .*

Proof. (1) A matrix M is in the U_{n+1} -centralizer of $I + N$ if and only if $MN = NM$. This is equivalent to $M_{i,j+1} = M_{i-1,j}$ for all i, j .

(2) The size of the U_{n+1} -conjugacy class of $I + N$ is equal to the index of the centralizer of $I + N$ in U_{n+1} . The order of U_{n+1} is $p^{\frac{n(n+1)}{2}}$. By (1), the order of the centralizer of $I + N$ is equal to p^n , thus the size of the U_{n+1} -conjugacy class of $I + N$ is equal to $p^{\frac{n(n-1)}{2}}$.

If M is conjugate to $I + N$, then the image of M in $U_{n+1}/[U_{n+1}, U_{n+1}]$ is equal to the image of $I + N$. This implies that $M_{i,i+1} = (I + N)_{i,i+1} = 1$ for all i . This restricts the possible conjugates of $I + N$ to at most $p^{\frac{n(n-1)}{2}}$ elements, hence by the previous paragraph they must form the conjugacy class of $I + N$. \square

Proof of Proposition 8.1(3). Let

$$A := I + N = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \in U_4,$$

so that

$$A^2 = I + N^2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

We write \bar{A} for the image of A in \bar{U}_4 . Let

$$B = \begin{bmatrix} 1 & B_{1,2} & B_{1,3} & B_{1,4} \\ 0 & 1 & B_{2,3} & B_{2,4} \\ 0 & 0 & 1 & B_{3,4} \\ 0 & 0 & 0 & 1 \end{bmatrix} \in U_4.$$

Then

$$BN^2 = \begin{bmatrix} 0 & 0 & 1 & B_{1,2} \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad N^2B = \begin{bmatrix} 0 & 0 & 1 & B_{3,4} \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Since $A^2 = I + N^2$, we deduce that:

- (i) \bar{A}^2 belongs to the center of \bar{U}_4 , and
- (ii) A^2 commutes with B in U_4 if and only if $B_{1,2} = B_{3,4}$.

In view of Theorem 5.2 and the universal property of pro-2 completion, in order to prove (3) it suffices to find a homomorphism $G \rightarrow (\mathbb{Z}/2\mathbb{Z})^3$ which lifts to \overline{U}_4 but not to U_4 . If S is a group, to give a homomorphism $G \rightarrow S$ is the same as giving two elements $s_a, s_b \in S$ such that $s_b s_a^2 = s_a^2 s_b$.

Consider the homomorphism $\chi: G \rightarrow (\mathbb{Z}/2\mathbb{Z})^3$ given by sending a to $(1, 1, 1)$ and b to $(1, 0, 0)$. By (i), sending

$$a \mapsto \overline{A}, \quad b \mapsto \begin{bmatrix} 1 & 1 & 0 & \square \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

defines a lift of χ to \overline{U}_4 .

Suppose that χ lifts to a group homomorphism $f: G \rightarrow U_4$. By Lemma 8.2(2), $f(a)$ is U_4 -conjugate to A , and so, replacing f by a U_4 -conjugate if necessary, we may suppose that $f(a) = A$. On the other hand, we have

$$f(b) = \begin{bmatrix} 1 & 1 & x_1 & x_3 \\ 0 & 1 & 0 & x_2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

for some $x_1, x_2, x_3 \in \mathbb{Z}/2$. Since $f(b)_{1,2} = 1 \neq 0 = f(b)_{3,4}$, we deduce from (i) that $f(b)$ does not commute with $A^2 = f(a^2)$, contradicting the fact that b commutes with a^2 . Therefore χ does not lift to U_4 . \square

REFERENCES

- [BCQ23] Simone Blumer, Alberto Cassella, and Claudio Quadrelli. Groups of p -absolute Galois type that are not absolute Galois groups. *J. Pure Appl. Algebra*, 227(4):Paper No. 107262, 35, 2023. [2](#)
- [CE56] Henri Cartan and Samuel Eilenberg. *Homological algebra*. Princeton University Press, Princeton, N. J., 1956. [7](#)
- [DCF22] Charles De Clercq and Mathieu Florence. Lifting low-dimensional local systems. *Math. Z.*, 300(1):125–138, 2022. [2](#)
- [Dwy75] William G. Dwyer. Homology, Massey products and maps between groups. *J. Pure Appl. Algebra*, 6(2):177–190, 1975. [13](#)
- [Efr14] Ido Efrat. The Zassenhaus filtration, Massey products, and representations of profinite groups. *Adv. Math.*, 263:389–411, 2014. [13](#)
- [EM17] Ido Efrat and Eliyahu Matzri. Triple Massey products and absolute Galois groups. *J. Eur. Math. Soc. (JEMS)*, 19(12):3629–3640, 2017. [1](#)
- [Fen83] Roger A. Fenn. Techniques of geometric topology. *London Mathematical Society Lecture Note Series*, 57. Cambridge University Press, Cambridge, 1983. [12](#)
- [GMT18] Pierre Guillot, Ján Mináč, and Adam Topaz. Four-fold Massey products in Galois cohomology. *Compos. Math.*, 154(9):1921–1959, 2018. With an appendix by Olivier Wittenberg. [1](#), [2](#)
- [GS17] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. Second edition. [8](#), [23](#)
- [HW15] Michael J. Hopkins and Kirsten G. Wickelgren. Splitting varieties for triple Massey products. *J. Pure Appl. Algebra*, 219(5):1304–1319, 2015. [1](#)
- [HW19] Christian Haesemeyer and Charles A. Weibel. *The norm residue theorem in motivic cohomology*, volume 200 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2019. [1](#)
- [HW23] Yonatan Harpaz and Olivier Wittenberg. The Massey vanishing conjecture for number fields. *Duke Math. J.*, 172(1):1–41, 2023. [2](#), [13](#)

- [KMRT98] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The book of involutions*, volume 44 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1998. With a preface in French by J. Tits. [15](#)
- [Koc02] Helmut Koch. *Galois theory of p -extensions*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002. With a foreword by I. R. Shafarevich, Translated from the 1970 German original by Franz Lemmermeyer, With a postscript by the author and Lemmermeyer. [6](#)
- [Kra66] David Kraines. Massey higher products. *Trans. Amer. Math. Soc.*, 124:431–449, 1966.
- [LLSWW23] Yeuk Hay Joshua Lam, Yuan Liu, Romyar Sharifi, Preston Wake, and Jiuya Wang. Generalized Bockstein maps and Massey products. *Forum Math. Sigma*, 11:Paper No. e5, 41, 2023. [18](#)
- [Mat18] Eliyahu Matzri. Triple Massey products of weight $(1, n, 1)$ in Galois cohomology. *J. Algebra*, 499:272–280, 2018. [1](#)
- [MS82] A. S. Merkurjev and A. A. Suslin. K -cohomology of Severi-Brauer varieties and the norm residue homomorphism. *Izv. Akad. Nauk SSSR Ser. Mat.*, 46(5):1011–1046, 1135–1136, 1982. [9](#)
- [MS22] Alexander Merkurjev and Federico Scavia. Degenerate fourfold Massey products over arbitrary fields. *arXiv:2208.13011*, 2022. [2](#), [3](#), [18](#)
- [MS23] Alexander Merkurjev and Federico Scavia. The Massey Vanishing Conjecture for fourfold Massey products modulo 2. *arXiv:2301.09290*, 2023. [1](#), [3](#)
- [MT16] Ján Mináč and Nguyen Duy Tân. Triple Massey products vanish over all fields. *J. Lond. Math. Soc. (2)*, 94(3):909–932, 2016. [1](#), [16](#)
- [MT17] Ján Mináč and Nguyen Duy Tân. Triple Massey products and Galois theory. *J. Eur. Math. Soc. (JEMS)*, 19(1):255–284, 2017. [1](#), [18](#)
- [NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008. [6](#), [7](#), [8](#), [15](#)
- [Qua21] Claudio Quadrelli. Chasing maximal pro- p Galois Groups via 1-cyclotomicity. *arXiv:2106.00335*, 2021. [2](#), [18](#)
- [Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. [7](#)
- [Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002. Translated from the French by Patrick Ion and revised by the author. Corrected reprint of the 1997 English edition. [4](#)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, LOS ANGELES, CA 90095, UNITED STATES OF AMERICA

Email address: merkurev@math.ucla.edu

Email address: scavia@math.ucla.edu