Mathematische Annalen (2026) 395:102
https://doi.org/10.1007/s00208-026-03518-1

Mathematische Annalen

On the strong Massey vanishing property for number fields

Christian Maire[1] · Ján Mináč[2] · Ravi Ramakrishna[3] · Nguyễn Duy Tân[4]

Received: 12 August 2025 / Revised: 9 April 2026 / Accepted: 10 June 2026

Abstract
Let $n \geq 3$ and p be an odd prime. We show that for every number field K with $\zeta_p \notin K$, the absolute and tame Galois groups Γ_K and Γ_K^{ta} of K satisfy the strong n-fold Massey vanishing property relative to p. Our work is based on an adaptation of the proof of the Scholz–Reichardt theorem.

Mathematics Subject Classification 55S30 · 11R32 · 11R37 · 12G05

1 Introduction

Let K be a number field with a fixed algebraic closure $\overline{K}$. We set $K^{ta} \subset \overline{K}$ to be the maximal tamely ramified Galois extension of K, that is K^{ta} is the composite of all number fields $L \subset \overline{K}$ such that the ramification index $e_{\mathfrak{Q}}$ at all primes $\mathfrak{Q}$ of L is prime to the residue characteristic of $\mathfrak{Q}$. Set $\Gamma_K := Gal(\overline{K}/K)$, and $\Gamma_K^{ta} = Gal(K^{ta}/K)$.

Let p be an odd prime number such that ζ_p, a primitive pth root of unity, is not in K. In [9] the authors use embedding techniques to characterize finitely generated pro-p groups that can be realized as quotients of Γ_K^{ta}. They introduced the notion of

In memory of Nigel Boston

✉ Ravi Ramakrishna
ravi@math.cornell.edu

Christian Maire
christian.maire@univ-fcomte.fr

Ján Mináč
minac@uwo.ca

Nguyễn Duy Tân
tan.nguyenduy@hust.edu.vn

1 Université Marie et Louis Pasteur, CNRS, Institut FEMTO-ST, 25000 Besançon, France

2 Department of Mathematics, Western University, London, ON N6A 5B7, Canada

3 Department of Mathematics, Cornell University, Ithaca, NY 14853-4201, USA

4 Faculty of Mathematics and Informatics, Hanoi University of Science and Technology, 1 Dai Co Viet Road, Hanoi, Vietnam

Published online: 07 July 2026

locally inertially generated pro-p groups for which congruence subgroups of $\mathrm{SL}_m(\mathbb{Z}_p)$ are archetypes. This key notion provides compatibility with local tame liftings as used in the Scholz–Reichardt theorem (see [26, Chapter 2, §2.1]). This strategy has implications for Massey products as well.

Let $n \geq 3$ and U_{n+1} be the group of all upper-triangular unipotent $(n+1) \times (n+1)$-matrices with entries in $\mathbb{F}_p$. Let Z_{n+1} be the subgroup of all such matrices with all off-diagonal entries 0 except at position $(1, n+1)$; it is the center of U_{n+1}. Set $\overline{U}_{n+1} := U_{n+1}/Z_{n+1}$. Let W_{n+1} be the subgroup of U_{n+1} that is zero on the near diagonal, that is all $(i, i+1)$ entries are 0. It is also the p-Frattini subgroup of U_{n+1}. Let φ and $\bar{\varphi}$ be the natural projections to U_{n+1}/W_{n+1} and $\overline{U}_{n+1}/(W_{n+1}/Z_{n+1})$, both of which are isomorphic to $(\mathbb{Z}/p)^n$. We have the diagram of groups below:

$$\begin{tikzcd}
 & & & \Gamma \arrow[dl, dotted, "?\rho"'] \arrow[d, dotted, "?\rho'"] \arrow[dd, bend left=60, "\theta"] & \\
1 \arrow[r] & Z_{n+1} \arrow[r] & U_{n+1} \arrow[r, two heads] \arrow[dr, two heads, "\varphi"'] & \overline{U}_{n+1} \arrow[d, two heads, "\overline{\varphi}"] & \\
 & & & (\mathbb{Z}/p)^n &
\end{tikzcd}$$

Here Γ is a profinite group that we usually take to be Γ_K^{ta} or Γ_K. Let $\chi_1, \cdots, \chi_n \in H^1(\Gamma, \mathbb{Z}/p)$, and set

$$\theta := (\chi_1, \cdots, \chi_n) : \Gamma \to (\mathbb{Z}/p)^n.$$

The existence of a homomorphic lift of θ to $\overline{U}_{n+1}$ is related to the existence of a subset of $H^2(\Gamma, \mathbb{Z}/p)$, denoted $\langle \chi_1, \cdots, \chi_n \rangle$ and called the Massey product. We will bypass the definition of the Massey product and instead use a consequence which characterizes the 'defined' and 'vanishing' conditions via group representations. For more details see [3, §2] and also [11, §2], [16, §2.2] and [20, §2]. Note that the definitions of Massey products in [3, 20] differ from those in [11, 16] by a sign.

Definition 1.1 Let $\chi_1, \cdots, \chi_n \in H^1(\Gamma, \mathbb{Z}/p)$. The Massey product $\langle \chi_1, \cdots, \chi_n \rangle$

- is defined if θ lifts to $\overline{U}_{n+1}$, *i.e.* $\theta = \overline{\varphi} \circ \rho'$ for some homomorphism $\rho' : \Gamma \to \overline{U}_{n+1}$;
- vanishes if θ lifts to U_{n+1}, *i.e.* $\theta = \varphi \circ \rho$ for some homomorphism $\rho : \Gamma \to U_{n+1}$.

Actually, for any lift $\rho' \colon \Gamma \to \overline{U}_{n+1}$ of θ, one can define an element $[\Delta(\rho')]$ in $H^2(\Gamma, \mathbb{Z}/p)$ coming from the boundary map $H^1(\Gamma, \overline{U}_{n+1}(\mathbb{F}_p)) \xrightarrow{\partial} H^2(\Gamma, Z) \simeq H^2(\Gamma, \mathbb{Z}/p)$, and the Massey product $\langle \chi_1, \cdots, \chi_n \rangle$ itself is the subset of $H^2(\Gamma, \mathbb{Z}/p)$ consisting of all such elements $[\Delta(\rho')]$, see for example, [19, Definition 1.1]. Thus it is possible that some $\rho' : \Gamma \to \overline{U}_{n+1}$ may lift to a $\rho : \Gamma \to U_{n+1}$, while others may not have lifts. These definitions depend crucially on the ordering of the characters.

Definition 1.2 The profinite group Γ satisfies the n-fold Massey vanishing property (relative to p) if the Massey product being defined implies it vanishes.

Definition 1.3 The profinite group Γ satisfies the strong n-fold Massey vanishing property (relative to p) if for all $\chi_1, \cdots, \chi_n \in H^1(\Gamma, \mathbb{Z}/p)$ such that

$$\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = \cdots = \chi_{n-1} \cup \chi_n = 0,$$

the Massey product $\langle \chi_1, \cdots, \chi_n \rangle$ vanishes.

Set

$$\begin{aligned}
A_n &= \{(\chi_1, \ldots, \chi_n) \mid \langle \chi_1, \cdots, \chi_n \rangle \text{ vanishes}\},\\
B_n &= \{(\chi_1, \ldots, \chi_n) \mid \langle \chi_1, \cdots, \chi_n \rangle \text{ is defined}\},\\
C_n &= \{(\chi_1, \ldots, \chi_n) \mid \chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = \cdots = \chi_{n-1} \cup \chi_n = 0 \in H^2(\Gamma, \mathbb{Z}/p)\}.
\end{aligned}$$

One has $A_n \subset B_n \subset C_n$. That $A_n \subset B_n$ follows from Definition 1.1. That $B_n \subset C_n$ follows from a simple argument—see [16, Remark 2.2]. For $n = 3$, $B_3 = C_3$. Other inclusions may be strict in general.

In [20, Conjecture 16] and [22, Conjecture 1.1] Mináč-Tân proposed the n-Massey vanishing conjecture, first for all fields containing a primitive pth root of unity and then for all fields. If $n \geq 3$, p is any prime, and Γ is the absolute Galois group of a field, the conjecture asserts Γ satisfies the n-fold Massey conjecture, namely that $A_n = B_n$. See [19] for a survey of current work on the Mináč-Tân Conjecture including the recent work of Merkurjev and Scavia [16–18]. In [21, Proposition 4.1] it is shown that if Γ is a pro-p Demushkin group then for p any prime and $n \geq 3$ we have $B_n = C_n$. That $A_n = B_n$ in the pro-p Demushkin setting is [20, Theorem 1.2]. Therefore Demushkin groups satisfy the strong n-fold Massey vanishing property. For further related results see [25].

In [16, Theorem 1.6] Merkurjev and Scavia showed that for any field F_0 of characteristic different from 2, there exists a field extension (not necessarily algebraic) F/F_0 such that for $p = 2$ and Γ_F, we have $A_4 \subsetneq C_4$. In a subsequent paper [18, Theorem 1.3] they extend this result to all primes p.

Turning to the case where the base field K is a number field and $p = 2$, Hopkins and Wickelgren [12, 1.3 Theorem] have shown the remarkable result that the triple Massey product vanishes whenever it is defined. In [20, Theorems 1.2 and Example 4.1] this is established for Γ_F the absolute Galois group of any field F. In [4, 15, 22] this was proved for any field and any prime p. The last paper removed the hypothesis that the base field contained a primitive pth root of unity. Thus the 3-fold Massey vanishing conjecture holds for any field and any prime. Merkurjev and Scavia also proved the 4-fold Massey vanishing conjecture holds for all fields with $p = 2$.

Harpaz and Wittenberg [11, Theorem 1.3] have recently proved the Mináč-Tân Conjecture for number fields K.

If a primitive pth-root of unity is in a number field K, there are several known counterexamples to the strong n-fold Massey vanishing property for Γ_K, that is there are examples where $A_n \subsetneq C_n$ so we do not have $A_n = B_n = C_n$. In the appendix to [6] there is an interesting example discovered by Harpaz and Wittenberg. For $K = \mathbb{Q}$ and $p = 2$ the 4-fold Massey product $\langle 34, 2, 17, 34 \rangle$ is not defined despite the fact that the Hilbert symbols $(34, 2)$, $(2, 17)$, $(17, 34)$ are trivial (by Kummer theory we have replaced elements of $H^1(\Gamma_{\mathbb{Q}}, \mathbb{Z}/2)$ by elements of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ and the Hilbert symbols correspond to cup products). This however cannot happen in the nondegenerate case, that is when the span of the χ_i is 4-dimensional. See Theorem 6.2 and Remark 6.3 of [6]. This example was generalized by Merkurjev-Scavia [16, §5] in the context of 4-fold Massey products $\langle bc, b, c, bc\rangle$ for $p = 2$. Thus for $K = \mathbb{Q}$ and $p = 2$ the Massey product $\langle 13 \cdot 17, 13, 17, 13 \cdot 17\rangle$ is not defined: Γ_K^{ta} does not satisfy the strong 4-fold Massey vanishing property, i.e. $A_4 \subsetneq C_4$.

The main result of this paper is that when $\zeta_p \notin K$, the situation is much nicer:

Theorem 1.1 *Take $n \geq 3$, and suppose that $\zeta_p \notin K$. The profinite groups Γ_K and Γ_K^{ta} satisfy the strong n-fold Massey vanishing property relative to p, that is $A_n = B_n = C_n$.*

Remark 1.1 We build our ρ from θ inductively. In the tame situation, all additional ramified primes in our lift of θ to ρ can be chosen to have norm 1 modulo a suitably large power of p, usually taken to be the exponent of U_{n+1}. We use Chebotarev's theorem to choose these primes, usually applied simultaneously to a governing field, the part of the tower already constructed, and a cyclotomic extension of K. This hypothesis $\zeta_p \notin K$ is crucial as it implies linear disjointness of these fields over K. See Proposition 2.3.

We obtain this theorem by giving a global lifting result (Theorem 3.2) in the spirit of the inverse Galois problem over number fields for p-groups U with local conditions, as developed in [24, IX, §5, Theorem 9.5.5] or [23, Main Theorem]. When compared to the main theorem of Neukirch in [23], our proof is more explicit, constructive and streamlined to our specific Galois representations. The notion of local plans as used in [9] is central.

We can strengthen the theorem above by showing that θ lifts, for any $r \geq 1$, to a subgroup of $GL_{n+1}(\mathbb{Z}/p^r)$.

Theorem 1.2 *Take $\Gamma = \Gamma_K^{ta}$ or Γ_K, and suppose $\zeta_p \notin K$. For $n \geq 3$, let $\theta : \Gamma \to (\mathbb{Z}/p)^n$ satisfy C_n. Let ρ be given by Theorem 1.1, where we choose all tame primes $\mathfrak{q}'$ at which we will allow additional ramification to have norm 1 modulo $p^{m(r)}$, where $p^{m(r)}$ is the exponent of $U_{n+1}(\mathbb{Z}/p^r)$.*

Let $\pi_r : GL_{n+1}(\mathbb{Z}/p^r) \to GL_{n+1}(\mathbb{F}_p)$ and $i : U_{n+1}(\mathbb{F}_p) \to GL_{n+1}(\mathbb{F}_p)$ be the natural projection and inclusion maps.

(i) *Then for every $r \geq 1$, there exists a homomorphism $\rho_r : \Gamma \to GL_{n+1}(\mathbb{Z}/p^r)$ such that $\pi_r \circ \rho_r = i \circ \rho$. As the image of $\pi_r \circ \rho_r$ lies in $U_{n+1}(\mathbb{F}_p)$, we may apply i^{-1} to it and we also have $\theta = \varphi \circ i^{-1} \circ \pi_r \circ \rho_r$.*

(ii) *If moreover $\zeta_{p^r} \in K_{\mathfrak{q}}$ for every ramified prime $\mathfrak{q}$ in θ then ρ_r can be chosen such that $\rho_r(\Gamma) \subset U_{n+1}(\mathbb{Z}/p^r)$.*

We highlight two important points:
- This result is more involved than the proof of the Scholz–Reichardt theorem realizing every p-group as a Galois group over K. We proceed inductively as they do, but must start with a given θ rather than the trivial representation. This adds many complications.
- For some tamely ramified θ, a priori our theorems could have been false for Γ_K^{ta} but

true for Γ_K. In fact all new primes of ramification in our theorems are tame. See Sect. 3.

Given a prime number p, set $K' = K(\zeta_p)$. Since $-1 = \zeta_2 \in K$, we assume that p is odd. In particular, archimedean places play no role in our work. All cohomology groups in this paper have $\mathbb{Z}/p\mathbb{Z}$-coefficients with trivial action so we simply write $H^i(\Gamma)$ rather than $H^i(\Gamma, \mathbb{Z}/p\mathbb{Z})$. We write U_{n+1} to mean $U_{n+1}(\mathbb{F}_p)$. We include coefficient rings, e.g. $U_{n+1}(\mathbb{Z}/p^r)$, when there could be ambiguity. We freely identify $\mathbb{Z}/p$ with $\mathbb{F}_p$ when convenient.

2 Tools for the embedding problem

2.1 Realizing cyclic extensions with given ramification and splitting

The problem of realizing the group $G := (\mathbb{Z}/p)^d$ as a quotient of Γ_K which satisfies certain ramification conditions can be solved by induction as in [26, Chapter 2, §2.1] or [9, §2.1]. This involves a governing field $\mathrm{Gov}_{K,T}$ which controls the obstructions of our embedding problem (see Proposition 2.3).

Given a finite set T of finite primes of K, set

$$V^T = \{x \in K^\times; \mathfrak{q} \notin T \implies v_\mathfrak{q}(x) \equiv 0 \bmod p\}.$$

Denote by $\mathrm{Gov}_{K,T}$ the governing field $\mathrm{Gov}_{K,T} := K'(\sqrt[p]{V^T})$.

$$\begin{tikzcd}[column sep=small]
 & \mathrm{Gov}_{K,T} := K'(\sqrt[p]{V^T}) \arrow[dl, dash] \\
K' := K(\zeta_p) \arrow[d, dash] & \\
K &
\end{tikzcd}$$

We see $\mathrm{Gov}_{K,T}/K'$ is an elementary abelian p-extension. Moreover $\mathrm{Gov}_{K,T}/K$ is a Galois extension with Galois group isomorphic to the semi-direct product $Gal(K'(\sqrt[p]{V^T})/K') \rtimes Gal(K'/K)$, where the action of $Gal(K'/K)$ is given by Kummer duality: since $Gal(K'/K)$ acts trivially on V^T, it acts via the cyclotomic character (which is non-trivial as $\zeta_p \notin K$) on the Galois group over K' of each cyclic degree p extension M/K' in $K'(\sqrt[p]{V^T})/K'$. See [7, Chapter I, Theorem 6.2].

For a tame prime $\mathfrak{q} \notin T$ (that is, $\mathfrak{q} \nmid (p)$) it is easy to see $\mathfrak{q}$ is unramified in $\mathrm{Gov}_{K,T}/K$. We write $\sigma_\mathfrak{q}$ for the Frobenius in $Gal(\mathrm{Gov}_{K,T}/K')$ for a fixed prime $\mathfrak{Q}$ above $\mathfrak{q}$.

Remark 2.1 The Frobenius is actually associated to a prime $\mathfrak{Q}$ of $\mathrm{Gov}_{K,T}$ above $\mathfrak{q}$, but changing $\mathfrak{Q}$ changes the Frobenius by a nonzero scalar multiple. This follows from our description of $Gal(K'(\sqrt[p]{V^T})/K)$ above and does not affect the condition of Theorem 2.1 below. Hence we abuse notation and write $\sigma_{\mathfrak{q}}$.

One has (see [7, Chapter V, Corollary 2.4.2]):

Theorem 2.1 (Gras) *Let $S = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_s\}$ be a set of primes of K having absolute norm* 1 *mod p and coprime to T. There exists a $\mathbb{Z}/p$-extension L/K exactly ramified at S and splitting completely at T if and only if there exist $a_i \in \mathbb{F}_p^\times$, $i = 1, \cdots, s$, such that*

$$\sum_{i=1}^{s} a_i \sigma_{\mathfrak{q}_i} = 0 \in Gal(\mathrm{Gov}_{K,T}/K').$$

Hence, if a tame $\mathfrak{q}$ splits completely in $\mathrm{Gov}_{K,T}/K'$, there exists an $\mathbb{Z}/p$-extension L/K exactly ramified at $\mathfrak{q}$ and splitting completely at T.

2.2 Cohomology and embedding problems

Let G be a p-group and let $d(G) := \dim H^1(G)$ be its p-rank. Suppose $H \simeq \mathbb{Z}/p$ a normal subgroup of G is given such that $d(G/H) = d(G)$. Let Γ be a pro-p group, and let $\overline{\rho} : \Gamma \twoheadrightarrow G/H$ be a surjective morphism.

We consider the embedding problem $(\mathcal{E})$:

$$\begin{tikzcd} & & & \Gamma \arrow[dl, dotted, "?\rho"'] \arrow[d, two heads, "\overline{\rho}"] \\ 1 \arrow[r] & H \arrow[r] & G \arrow[r, two heads, "\pi"'] & G/H \end{tikzcd}$$

where π is the natural projection.

Let ε be the element in $H^2(G/H)$ corresponding to the (equivalence class of the) group extension:

$$1 \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow 1. \tag{1}$$

As $d(G) = d(G/H)$, we have $\varepsilon \neq 0$. Consider the inflation map $Inf : H^2(G/H) \to H^2(\Gamma)$. The action of Γ on $H = \mathbb{Z}/p$ is induced by $\overline{\rho}$ and is thus trivial.

Theorem 2.2 *With hypotheses as above, the embedding problem $(\mathcal{E})$ has a solution if and only if $Inf(\varepsilon) = 0$. Moreover, any solution is always proper, that is ρ is surjective. If a solution exists, the set of solutions (modulo equivalence) of $(\mathcal{E})$ is a principal homogeneous space under $H^1(\Gamma)$.*

Proof See Propositions 3.5.9 and 3.5.11 of [24]. □

Remark 2.2 For a prime $\mathfrak{q}$ of K, denote by $\Gamma_{\mathfrak{q}}$ the maximal pro-p quotient of the absolute Galois group of $K_{\mathfrak{q}}$. We need to study the local embedding problems attached to local maps $\iota_{\mathfrak{q}} : \Gamma_{\mathfrak{q}} \to \Gamma$. Let $\overline{D}_{\mathfrak{q}} \subset G/H$ be the image of $\overline{\rho_{\mathfrak{q}}} := \overline{\rho} \circ \iota_{\mathfrak{q}}$, and $M_{\mathfrak{q}} \subset G$ be the inverse image $\pi^{-1}(\overline{D}_{\mathfrak{q}})$. We have the local embedding problem $(\mathcal{E}_{\mathfrak{q}})$:

$$\begin{tikzcd}
 & & & \Gamma_{\mathfrak{q}} \arrow[dl, dotted, "?\rho_{\mathfrak{q}}"'] \arrow[d, two heads, "\overline{\rho_{\mathfrak{q}}}"] \\
1 \arrow[r] & H_{\mathfrak{q}} \arrow[r] & M_{\mathfrak{q}} \arrow[r, two heads, "\pi_{\mathfrak{q}}"'] & \overline{D}_{\mathfrak{q}}
\end{tikzcd}$$

If a solution exists, the set of solutions (modulo equivalence) of $(\mathcal{E}_{\mathfrak{q}})$ is a principal homogeneous space under $H^1(\Gamma_{\mathfrak{q}})$.

2.3 Trivializing the Shafarevich group

Let X be a finite set of places of K. Let K_X be the maximal pro-p extension of K unramified outside X and set $\Gamma_X := Gal(K_X/K)$.

Let Ш^2_X be the kernel of the localization map

$$H^2(\Gamma_X) \longrightarrow \prod_{\mathfrak{q}\in X} H^2(\Gamma_{\mathfrak{q}}).$$

Set $V_X := \{x \in K^\times; v_{\mathfrak{q}}(x) \equiv 0 \bmod p\ \forall \mathfrak{q},\ \text{and } \mathfrak{q} \in X \implies x \in (K_{\mathfrak{q}}^\times)^p\}$. Note that V_X is qualitatively different from V^T defined earlier, e.g. as X increases, V_X never increases in size, but can decrease. In contrast, while T increases, V^T never decreases in size, but can increase. By the work of Koch and Shafarevich (see [13, Chapter 11, Theorem 11.3]), we have that

$$\text{Ш}^2_X \hookrightarrow \text{Б}_X := (V_X/(K^\times)^p)^\vee,$$

where the superscript $^\vee$ indicates the Pontryagin dual.

Lemma 2.1 *One can choose a set N of primes of K whose norms are 1 mod p such that Б_N (and therefore Ш^2_N) is trivial.*

Proof From the definition of V_X we have that $K'(\sqrt[p]{V_X})/K'$ is unramified outside $\{p\}$ and completely split at X. Since the maximal elementary p-extension of K' unramified outside $\{\mathfrak{p}|p\}$ is finitely generated (see [13, §11.3]), we see for a finite set N of primes of K whose Frobenius elements span $Gal(K'(\sqrt[p]{V_\emptyset})/K')$ (which exists by Chebotarev's theorem) that $K'(\sqrt[p]{V_N}) = K'$. Thus $\forall x \in V_N$ we have $x \in (K'^\times)^p$. By taking the norm of x in K'/K and using the fact that $([K' : K], p) = 1$, we conclude that $x \in (K^\times)^p$. Thus $V_N/(K^\times)^p = 1$ which implies $\text{Ш}^2_N = 0$. The primes of N necessarily split completely in $K' := K(\zeta_p)$ and thus have norm 1 mod p. □

It is an easy exercise to see that for any sets Y, Z that $V_{Y\cup Z} \subset V_Y$ so $\text{Б}_Y \twoheadrightarrow \text{Б}_{Y\cup Z}$. Thus $V_{N\cup Y}/(K^\times)^p$ and $\text{Ш}^2_{N\cup Y}$ are trivial for any set Y.

Henceforth we assume that $\text{Ш}^2_N = 0$ and $\overline{\rho} : \Gamma_N \to G/H$ is given. Thus if at every $\mathfrak{q} \in N$ there is no local obstruction to lift $\overline{\rho_{\mathfrak{q}}}$ to $\rho_{\mathfrak{q}} : \Gamma_q \to G$, then the embedding problem $(\mathcal{E})$ with $\Gamma = \Gamma_N$ has a solution in K_N/K. We have reduced solving the obstruction problem to purely local problems. It is interesting to note that when we work with local plans at $\mathfrak{q} \in N$ (see Sect. 2.5) we can choose them to be unramified at these $\mathfrak{q}$. Thus the primes of N force the obstruction problem to be local, but they need not be ramified in our resolution of the Massey problem!

The question is: How do we create a situation for which there are no local obstructions for every quotient of G? We address this in the next two subsections.

2.4 The local-global principle

Let X be a finite set of primes of K. Given another finite set R of primes of K, denote by ψ_R the localization map:

$$\psi_R : H^1(\Gamma_{X \cup R}) \longrightarrow \prod_{\mathfrak{q} \in X} H^1(\Gamma_{\mathfrak{q}}).$$

We will control the image of ψ_R in the case where $R = \{\tilde{\mathfrak{q}}\}$, $\tilde{\mathfrak{q}}$ being a *tame* prime. Set $N(\tilde{\mathfrak{q}})$ to be the absolute norm of $\tilde{\mathfrak{q}}$.

The condition $\zeta_p \notin K$ is needed at this point, in particular the following lemma is crucial for Proposition 2.3.

Lemma 2.2 *Let F/K be Galois with $Gal(F/K)$ a p-group. If $\zeta_p \notin K$, then $F(\zeta_p) \cap K'(\sqrt[p]{V^X}) = K'$.*

Proof The intersection clearly contains K'. If it was larger, there would exist a $\mathbb{Z}/p$-extension M/K', Galois over K with $M \subset F(\zeta_p)$. Then $Gal(K'/K)$ would act on $Gal(M/K')$ in two different ways: trivially by viewing M in $F(\zeta_p)/K'$, and via the mod p cyclotomic character by viewing M in $K'(\sqrt[p]{V^X})/K'$. As these actions are incompatible when $\zeta_p \notin K$, the result follows. □

Below we recall Proposition 1.4 of [9]. The statement there requires the set of primes N (X in Proposition 2.3 below) to be tame. That proof in fact is valid word for word for *any* finite set of primes N - the authors of [9] were working in the tame setting and stated things accordingly. Also note that Proposition 1.3 of [9], on which Proposition 1.4 relies, is valid for *any* finite set of primes.

Proposition 2.3 *Let X be a finite set of primes, and let $(f_{\mathfrak{q}})_{\mathfrak{q} \in X} \in \prod_{\mathfrak{q} \in X} H^1(\Gamma_{\mathfrak{q}})$. There exist infinitely many finite primes $\tilde{\mathfrak{q}}$ such that $(f_{\mathfrak{q}})_{\mathfrak{q} \in X} \in Im(\psi_{\{\tilde{\mathfrak{q}}\}})$. Moreover, when $\zeta_p \notin K$, the primes $\tilde{\mathfrak{q}}$ can be chosen such that:*

(i) *$\tilde{\mathfrak{q}}$ splits completely in F/K, where F/K is a given finite p-extension,*
(ii) *For a given $m \in \mathbb{N}$, one can choose $\tilde{\mathfrak{q}}$ such that $v_p(N(\tilde{\mathfrak{q}}) - 1) \geq m$.*

Remark 2.3 Take $m \geq 1$. In the proof of Proposition 2.3 given in [9], the tame prime $\tilde{\mathfrak{q}}$ is characterized by its Frobenius in $K'(\zeta_{p^m}, \sqrt[p]{V^X})/K'$; in this case we can choose $v_p(N(\tilde{\mathfrak{q}}) - 1) \geq m$. Using effective versions of Chebotarev's theorem, one can give an upper bound for the absolute norm of the smallest such $\tilde{\mathfrak{q}}$.

Let $d_{X,m}$ be the absolute value of the absolute discriminant of the number field $K'(\zeta_{p^m}, \sqrt[p]{V^X})$. Then, assuming the GRH, $N(\tilde{\mathfrak{q}}) \ll (\log(d_{X,m}))^2$. See [14]. One can give unconditional estimates, but they are much weaker and more complicated to write down.

2.5 Local plans

Previously, we had considered the problem $(\mathcal{E})$ where $H \simeq \mathbb{Z}/p$. To prove our main theorem we need to lift

$$\begin{tikzcd} & & & \Gamma \arrow[dl, dotted, "?\rho"'] \arrow[d, two heads, "\overline{\rho}"] \\ 1 \arrow[r] & V \arrow[r] & U \arrow[r, two heads, "\pi"'] & U/V \end{tikzcd}$$

where V is some normal subgroup of the p-group U. Of course we will do this one step at a time where each kernel is isomorphic to $\mathbb{Z}/p$, but at each step we will need more ramified primes. As we introduce a new ramified prime, we need a *local plan* for it, that is a local solution to the *overall* lifting problem above.

As before, N is taken so that $Ш^2_N = 0$. We suppose given a sub-extension F/K of K_N/K with Galois group isomorphic to U/V, that is we have a homomorphism $\overline{\rho} : \Gamma_N \twoheadrightarrow U/V$.

Given $\mathfrak{q} \in N$, let $\overline{\rho}_\mathfrak{q} : \Gamma_\mathfrak{q} \longrightarrow \overline{D}_\mathfrak{q} \subset U/V$ be the restriction of $\overline{\rho}$, where $\overline{D}_\mathfrak{q}$ is the decomposition group of $\mathfrak{q}$ in $U/V = Gal(F/K)$ (after fixing a prime $\mathfrak{Q}|\mathfrak{q}$).

We seek a lift $\rho_\mathfrak{q}$ of $\overline{\rho}_\mathfrak{q}$ in U, in the setting where $\overline{\rho}_\mathfrak{q}$ is ramified:

$$\begin{tikzcd} & \Gamma_\mathfrak{q} \arrow[dl, dotted, "?\rho_\mathfrak{q}"'] \arrow[d, "\overline{\rho}_\mathfrak{q}"] \\ U \arrow[r, two heads] & U/V \end{tikzcd}$$

If $\rho_\mathfrak{q}$ does not exist, our problem has no local solution and thus no global solution. If $\rho_\mathfrak{q}$ exists, we call it a *local plan* for $\Gamma_\mathfrak{q}$ into U.

Recall that the pro-p group $\Gamma_\mathfrak{q}$ is
- free when $\zeta_p \notin K_\mathfrak{q}$,
- and Demushkin when $\zeta_p \in K_\mathfrak{q}$.

Let us be more precise.

Consider $\mathfrak{q} \nmid p$. We suppose that $\zeta_p \in K_\mathfrak{q}$ (if not, $\Gamma_\mathfrak{q} \simeq \mathbb{Z}_p$). Recall that in this case $\Gamma_\mathfrak{q} \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p$ is Demushkin. Indeed, let $\tau_\mathfrak{q} \in \Gamma_\mathfrak{q}$ be a generator of inertia and $\sigma_\mathfrak{q}$ a lift of the Frobenius. One has the unique relation: $\sigma_\mathfrak{q}\tau_\mathfrak{q}\sigma_\mathfrak{q}^{-1} = \tau_\mathfrak{q}^{N(\mathfrak{q})}$. See [13, Chapter 10, §10.2 and §10.3].

We now consider $\mathfrak{p}|p$ and set $n_\mathfrak{p} = [K_\mathfrak{p} : \mathbb{Q}_p]$. If $\zeta_p \notin K_\mathfrak{p}$, then $\Gamma_\mathfrak{p}$ is free pro-p on $n_\mathfrak{p} + 1$ generators and $\bar{\rho}_\mathfrak{p}$ obviously lifts to a $\rho_\mathfrak{p}$. If $\zeta_p \in K_\mathfrak{p}$, then $\Gamma_\mathfrak{p}$ is a Demushkin on $n_\mathfrak{p} + 2$ generators $x_1, \cdots, x_{n_\mathfrak{p}+2}$; in this case the unique relation is $x_1^{p^s}[x_1, x_2] \cdots [x_{n_\mathfrak{p}+1}, x_{n_\mathfrak{p}+2}]$, where p^s is the largest power of p such that $K_\mathfrak{p}$ contains the p^s-roots of the unity. See [24, Theorems 7.5.11, 7.5.12].

We give examples of local plans.

Example 2.1 *(S-R plan)* Recall the principle of the proof of the Scholz–Reichardt theorem. Suppose that U contains an element y of order p^m. Take a prime $\mathfrak{q}$ such that $v_p(N(\mathfrak{q})-1) \geq m$ - just choose $\mathfrak{q}$ to split completely in $K(\zeta_{p^m})/K$. Suppose we are given a homomorphism $\overline{\rho}_\mathfrak{q} : \Gamma_\mathfrak{q} \longrightarrow U/V$ defined by $\overline{\rho}_\mathfrak{q}(\sigma_\mathfrak{q}) = \overline{1}$ and $\overline{\rho}_\mathfrak{q}(\tau_\mathfrak{q}) = \bar{y}$. Since $y^{N(\mathfrak{q})-1} = 1$, the map $\rho_\mathfrak{q} : \Gamma_\mathfrak{q} \to U$ given by $\rho_\mathfrak{q}(\sigma_\mathfrak{q}) = 1$ and $\rho_\mathfrak{q}(\tau_\mathfrak{q}) = y$ is a homomorphic lift of $\overline{\rho}_\mathfrak{q}$ from U/V to U. This local plan is used for the primes $\mathfrak{q}'_i$ in the proof of Theorem 3.2.

Example 2.2 *(Trivial plan)* There are two trivial plans.

1) Suppose F/K unramified at $\mathfrak{q}$, *i.e.* let $\overline{\rho}_\mathfrak{q} : \Gamma_\mathfrak{q} \longrightarrow U/V$ be a homomorphism defined by $\overline{\rho}_\mathfrak{q}(\sigma_\mathfrak{q}) = \overline{x}$ for some $\overline{x} \in U/V$ and $\overline{\rho}_\mathfrak{q}(\tau_\mathfrak{q}) = \overline{1}$. Let $x \in U$ be any lift of $\overline{x}$. The map $\rho_\mathfrak{q} : \Gamma_\mathfrak{q} \to U$ given by $\rho_\mathfrak{q}(\sigma_\mathfrak{q}) = x$ and $\rho_\mathfrak{q}(\tau_\mathfrak{q}) = 1$ is a homomorphic lift of $\overline{\rho}_\mathfrak{q}$ from U/V to U. This local plan is used for the primes of $N_2 \setminus S_2$ in the proof of Theorem 3.2.

2) The previous unramified setting is a special case of the situation where $\Gamma_\mathfrak{q}$ is pro-p free, e.g. if $\mathfrak{q} \mid p$ and $\zeta_p \notin K_\mathfrak{q}$. Any lift gives a local plan in this case as well.

Example 2.3 *(Abelian plan)* Suppose that U contains two elements x and y satisfying $xy = yx$. Let p^ℓ be the order of y. Take a prime $\mathfrak{q}$ such that $v_p(N(\mathfrak{q})-1) = k \geq \ell$. The pro-$p$ part of the abelianization of $\Gamma_\mathfrak{q}$ is $\mathbb{Z}_p \times \mathbb{Z}/p^k$. Suppose given $\overline{\rho}_\mathfrak{q} : \Gamma_\mathfrak{q} \longrightarrow U/V$ defined by $\overline{\rho}_\mathfrak{q}(\sigma_\mathfrak{q}) = \overline{x}$ and $\overline{\rho}_\mathfrak{q}(\tau_\mathfrak{q}) = \bar{y}$. The map $\rho_\mathfrak{q} : \Gamma_\mathfrak{q} \to U$ given by $\rho_\mathfrak{q}(\sigma_\mathfrak{q}) = x$ and $\rho_\mathfrak{q}(\tau_\mathfrak{q}) = y$ is a homomorphic lift of $\overline{\rho}_\mathfrak{q}$ from U/V to U. We use this local plan in our alternative proof of the main theorem of this paper in the case $p > n$. See Corollary 4.1 and Sect. 4.2.

We use various other local plans in this paper:

- The results of Mináč-Tân ([21, Proposition 4.1] and [20, Theorem 4.3]) which we call *Massey local plans* and use in the proof of Theorem 4.1.
- We also use local plans from the work of Böckle [1, Theorem 1.3], Emerton-Gee [5, Theorem 6.4.4] and Conti-Demarche-Florence [2] (the corollary of the main theorem in the introduction) in the proof of Theorem 4.2.

3 A global lifting result

The main result of this section is Theorem 3.2, a variant of the Scholz–Reichardt theorem. We start with a proposition useful in proving the theorem when $d(U) > d(U/V)$, that is when U has more generators than U/V. In the context of the strong Massey vanishing property, it is useful for the *degenerate case*, e.g. if

$$U/V \simeq \theta(\Gamma) \subsetneq (\mathbb{Z}/p)^n \twoheadleftarrow U_{n+1} = U.$$

Proposition 3.1 *Suppose that $\zeta_p \notin K$. Let F/K be a finite p-extension and let S be a finite set of primes of K. Let $k, m \geq 1$ and for $\mathfrak{q} \in S$ and $i = 1, \cdots, k$, let $\chi_{\mathfrak{q},i} \in H^1(\Gamma_\mathfrak{q})$. Then for $i = 1, \cdots, k$*

(i) *there exist a non-trivial $\chi_i \in H^1(\Gamma_K)$ such that for every $\mathfrak{q} \in S$, $\chi_{i|\Gamma_\mathfrak{q}} = \chi_{\mathfrak{q},i}$. Let M_i/K be the $\mathbb{Z}/p$-extension fixed by $Ker(\chi_i)$;*

(ii) *the extension* M_i/K *is unramified outside* $S \cup \{\mathfrak{q}'_i\}$, *where* $\mathfrak{q}'_i$ *is a new tame prime such that* $v_p(N(\mathfrak{q}'_i) - 1) \geq m$;
(iii) *the extension* M_i/K *is totally ramified at* $\mathfrak{q}'_i$,
(iv) *for every* i, $\mathfrak{q}'_i$ *splits completely in* F/K.
(v) *for every* $j \neq i$, $\mathfrak{q}'_j$ *splits completely in* M_i/K.

Proof Establishing (v) requires Gras' Theorem 2.1. It is the crucial ingredient that allows us to define local plans used in Theorem 3.2 for the primes $\mathfrak{q}'_i$.

• By Proposition 2.3, there exists a tame prime $\mathfrak{q}'$ and $\chi_1 \in H^1(\Gamma_{S\cup\{\mathfrak{q}'\}})$ such that $\chi_1 |_{\Gamma_\mathfrak{q}} = \chi_{\mathfrak{q},1}$ for each $\mathfrak{q} \in S$. Moreover, since $\zeta_p \notin K$, using that $\mathrm{Gov}_{K,S}/K'$ and $F(\zeta_{p^m})/K'$ are linearly disjoint, we can choose $\mathfrak{q}'$ such that $v_p(N(\mathfrak{q}') - 1) \geq m$ and $\mathfrak{q}'$ splits completely in F/K. Let M be the extension of K fixed by the kernel of χ_1.

- If χ_1 is ramified at $\mathfrak{q}'$, then we set $M_1 := M$ and $\mathfrak{q}'_1 := \mathfrak{q}'$ and (i)-(iv) hold and (v) does not yet apply. We can move on to χ_2.

- If χ_1 is unramified at $\mathfrak{q}'$ there are two possibilities: χ_1 is trivial or non-trivial. In either case choose a tame prime $\mathfrak{q}'_1$ that splits completely in $\mathrm{Gov}_{K,S}F(\zeta_{p^m})/K$. By Theorem 2.1 there exists a $\mathbb{Z}/p$-extension M'_1/K exactly ramified at $\mathfrak{q}'_1$ in which the places of S split completely.

(a) if χ_1 is trivial then each $\chi_{\mathfrak{q},1}$ is trivial and $M = K$. Choose $M_1 := M'_1$. We have (i)–(iv) immediately, (v) does not yet apply, and we can move on to χ_2.

(b) if χ_1 is unramified at $\mathfrak{q}'$ and non-trivial, then $Gal(M'_1M/K) \simeq \mathbb{Z}/p \times \mathbb{Z}/p$. We choose M_1 to be any intermediate extension other than M and M'_1. We have (i) as the primes of S have the same splitting behavior in M and M_1, (ii) by construction, (iii) automatically and (iv) by the choice of $\mathfrak{q}'_1$ and (v) does not yet apply. We can move on to χ_2.

• Set $S_1 = S \cup \{\mathfrak{q}'_1\}$. Set $\chi_{\mathfrak{q}'_1,2} \in H^1(\Gamma_{\mathfrak{q}'_1})$ to be trivial. By Proposition 2.3, there is a tame prime $\mathfrak{q}'$ and $0 \neq \chi_2 \in H^1(\Gamma_{S_1})$ with $\chi_2|_{\Gamma_\mathfrak{q}} = \chi_{\mathfrak{q},2}$ for every $\mathfrak{q} \in S_1$. This is (i). Moreover, since $\zeta_p \notin K$, the prime $\mathfrak{q}'$ can be chosen such that $v_p(N(\mathfrak{q}') - 1) \geq m$, and such that $\mathfrak{q}'$ splits completely in FM_1/K (indeed $\mathrm{Gov}_{K,S}/K'$ and $FM_1(\zeta_{p^m})/K'$ are linearly disjoint). As before, set M to be the $\mathbb{Z}/p$-extension of K corresponding to χ_2. By the choice of $\chi_{\mathfrak{q}'_1,2}$, we see that $\mathfrak{q}'_1$ splits completely in M/K.

- If χ_2 is ramified at $\mathfrak{q}'$, set $M_2 = M$ and $\mathfrak{q}'_2 := \mathfrak{q}'$.

- If χ_2 is unramified we proceed as we did above to get $\mathfrak{q}'_2$ and M_2.

Then, in all cases, one has $(i) - (iv)$.

Note that the splitting choices for $\mathfrak{q}'_1$ and $\mathfrak{q}'_2$ give (v) as well.

Repeat this process with $S_2 = S_1 \cup \{\mathfrak{q}'_2\}$ to find $\mathfrak{q}'_3$ and M_3 etc. to finish the proof. □

Theorem 3.2 is the key result we need to establish the strong n-fold Massey vanishing property for Γ_K and Γ_K^{ta}. The proof of Theorem 3.2 is more involved than the corresponding argument of [9] or the proof of Scholz–Reichardt for U_{n+1}. This is because in those situations one starts with a trivial homomorphism and inductively builds the entire group. The local plans are much easier to introduce and maintain. In §4.1 we *start* with a homomorphism $\theta : \Gamma \to (\mathbb{Z}/p)^n$ and must lift that to $\overline{U}_{n+1}$ and U_{n+1}, rather than build θ at our convenience.

Theorem 3.2 *Suppose that $\zeta_p \notin K$. Let U be a p-group, and $V \lhd U$ be a normal subgroup of U. Let F/K satisfy*

- *F/K is unramified outside a set of primes $S = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_t\}$;*
- *for each $\mathfrak{q} \in S$ the decomposition group $\overline{D}_\mathfrak{q}$ in F/K respects a local plan $\rho_\mathfrak{q} : \Gamma_\mathfrak{q} \to U$. In other words, $\overline{D}_\mathfrak{q} \equiv \rho_\mathfrak{q}(\Gamma_\mathfrak{q})$ modulo V.*
- *$Gal(F/K) \simeq U/V$.*

Then there exists a Galois extension L/K in $\overline{K}/K$ (ramified at S and a finite set of tame primes not in S) such that:

(i) *L/K contains F/K;*
(ii) *$Gal(L/K) \simeq U$;*
(iii) *$\rho_\mathfrak{q}(\Gamma_\mathfrak{q}) \simeq D_\mathfrak{q} := Gal(L_\mathfrak{q}/K_\mathfrak{q})$, for every $\mathfrak{q} \in S$.*

Moreover, if $F \subset K^{ta}$ then L can be chosen in K^{ta}.

Proof Let p^m be the exponent of U. Since $\zeta_p \notin K$, Lemma 2.2 implies $F(\zeta_p) \cap \mathrm{Gov}_{K,S} = K'$. This will allow us to use Chebotarev's theorem to choose primes that split as we need in $K(\zeta_{p^m})$, F and $\mathrm{Gov}_{K,S}$.

For a p-group H set $FrQ(H) := H/[H,H]H^p$, the Frattini quotient of H. This is an $\mathbb{F}_p$-vector space. From the group extension $1 \to V \overset{i}{\to} U \overset{\pi}{\to} U/V \to 1$ we see i and π induce maps $\tilde{i} : FrQ(V) \to FrQ(U)$ and $\tilde{\pi} : FrQ(U) \to FrQ(U/V)$ with the latter map being surjective. The former map need not be injective - the Heisenberg group of order p^3 provides an example. Set $d(U) := \dim FrQ(U)$ and $d(U/V) := \dim FrQ(U/V)$.

• We first consider the case $d(U/V) < d(U)$. Let $\tilde{y}_1, \cdots, \tilde{y}_{d(U/V)}$ be lifts to $FrQ(U)$ of a basis of $FrQ(U/V)$. They form an independent set in $FrQ(U)$. It is an exercise to show the sum of their span with $\tilde{i}(FrQ(V))$ is $FrQ(U)$. Let $\tilde{x}_1, \cdots, \tilde{x}_k$ be elements of $\tilde{i}(FrQ(V))$ that together with $\tilde{y}_1, \cdots, \tilde{y}_{d(U/V)}$ form a basis of $FrQ(U)$. Let y_i and x_j be lifts to U and V of $\tilde{y}_i$ and $\tilde{x}_j$. Set $A := ([U,U]U^p) \cdot \langle y_1, \cdots, y_{d(U/V)} \rangle \subset U$ so $VA = U$. Then U/A is a quotient of $FrQ(U)$ of dimension k and

$$\frac{U}{V \cap A} \hookrightarrow \frac{U}{V} \times \frac{U}{A} \text{ and } 1 \to \frac{V}{V \cap A} \to \frac{U}{V \cap A} \to \frac{U}{V} \to 1,$$

so

$$\#\frac{U}{V \cap A} = \#\frac{U}{V} \cdot \#\frac{V}{V \cap A} = \#\frac{U}{V} \cdot \#\frac{VA}{A} = \#\frac{U}{V} \cdot \#\frac{U}{A} = \#\frac{U}{V} \cdot p^k.$$

We see

$$\frac{U}{V \cap A} \overset{\simeq}{\hookrightarrow} \frac{U}{V} \times \frac{U}{A} \simeq \frac{U}{V} \times (\mathbb{Z}/p)^k.$$

For $i = 1, \cdots, k$, let $\eta_i \in H^1\left(\frac{U}{V \cap A}\right)$ be defined by $\eta_i(x_j) = \delta_{i,j}$, and η_i is trivial on U/V. We have a local plan for each $\mathfrak{q} \in S$, so $\rho_\mathfrak{q}(\Gamma_\mathfrak{q}) \subset U \twoheadrightarrow \frac{U}{V \cap A}$ and the restriction $\eta_{i\,|\rho_\mathfrak{q}(\Gamma_\mathfrak{q})}$ can be viewed as an element of $H^1(\Gamma_\mathfrak{q})$ and thus an input of Proposition 3.1 for each $\mathfrak{q} \in S$.

By Proposition 3.1, there exist non-trivial $\chi_i \in H^1(\Gamma_K)$ for $i = 1, \cdots, k$ such that

(i) for every $\mathfrak{q} \in S$, $\chi_{i\,|\Gamma_\mathfrak{q}} = \eta_{i\,|\rho_\mathfrak{q}(\Gamma_\mathfrak{q})}$;
(ii) for each i let M_i the $\mathbb{Z}/p$-extension fixed by $Ker(\chi_i)$. The extension M_i/K is unramified outside $S \cup \{\mathfrak{q}'_i\}$ where $\mathfrak{q}'_i$ is a new tame prime satisfying $v_p(N(\mathfrak{q}'_i) - 1) \geq m$.
(iii) the extension M_i/K is totally ramified at $\mathfrak{q}'_i$,
(iv) for every i, $\mathfrak{q}'_i$ splits completely in F/K.
(v) for every $j \neq i$, $\mathfrak{q}'_j$ splits completely in M_i/K.

Put $K_2 := FM_1 \cdots M_k$. Then

$$h : Gal(K_2/K) \xrightarrow{\simeq} Gal(F/K) \times (\mathbb{Z}/p)^k \xrightarrow{\simeq} \frac{U}{V} \times (\mathbb{Z}/p)^k \xrightarrow{\simeq} \frac{U}{V \cap A}.$$

Condition (i) above implies the isomorphism h respects the initial local plans $\rho_\mathfrak{q}$ for every $\mathfrak{q} \in S$: the image of $\rho_\mathfrak{q}(\Gamma_\mathfrak{q}) \subset U$ projects to $D_\mathfrak{q}(K_2/K)$ in $\dfrac{U}{V \cap A} \simeq Gal(K_2/K)$. Moreover, for the other ramified primes $\mathfrak{q}'_i$, one has $v_p(N(\mathfrak{q}'_i) - 1) \geq m$, and $D_{\mathfrak{q}'_i}(K_2/K) = I_{\mathfrak{q}'_i}(K_2/K) \simeq \mathbb{Z}/p$, $i = 1, \cdots, k$. The extension K_2/K is unramified outside $S_2 := S \cup \{\mathfrak{q}'_1, \cdots, \mathfrak{q}'_k\}$. We have a local plan for each of these primes: the one given by the hypothesis for those in S, and the S-R local plan of Example 2.1 for the $\mathfrak{q}'_i$.

We have realized $\dfrac{U}{V \cap A}$ as $Gal(K_2/K)$ respecting all local plans for $\mathfrak{q} \in S$. For the additional primes of ramification we have created new local plans. As

$$d\left(\frac{U}{V \cap A}\right) = k + d\left(\frac{U}{V}\right) = d(U),$$

we can proceed to the next case.

• Now suppose $d(U/V) = d(U)$. Set $\Gamma = \Gamma_K$ or Γ_K^{ta}.

$$\begin{tikzcd}
 & & & \Gamma \arrow[dl, dotted, "?\rho"'] \arrow[d, two heads, "\bar{\rho}"] \\
1 \arrow[r] & V \arrow[r] & U \arrow[r, two heads, "\pi"'] & U/V
\end{tikzcd}$$

The map $\tilde{\pi} : FrQ(U) \to FrQ(U/V)$ is an isomorphism so if ρ exists it is surjective. As U is a p-group, we can filter V by normal subgroups of U whose successive quotients are $\mathbb{Z}/p$ (intersect a filtration of normal subgroups of U with the normal subgroup V).

Thus it suffices to solve the embedding problem above for $V = \mathbb{Z}/p$ and induct.

Let N_2 be a finite set of primes containing those ramified in K_2/K (*i.e.* $S_2 \subset N_2$) and such that $Ш^2_{N_2} = 0$.

At each stage of the induction we will:

(i) solve the *nonsplit* embedding problem above;

(ii) adjust the solution by an element of H^1 (adding ramification at a new prime if needed) such that the new solution is on all local plans, including at the new prime of ramification. There is then no local obstruction for the next step of the induction.

– There is no obstruction to lift the decomposition group $D_{\mathfrak{q}}$ of $\mathfrak{q}$ in U/V to U: for each $\mathfrak{q}$, one has a local plan. (If $\mathfrak{q} \in N_2 \backslash S_2$ take the trivial plan (1) of Example 2.2.) As $Ш^2_{N_2} = 0$ there is no global obstruction. There exists a $\mathbb{Z}/p$-extension of K_3/K_2, unramified outside N_2, Galois over K, solving the lifting problem to U. That is (i) of the strategy.

– If we are on all local plans in N_2, we proceed with the induction. The problem now is that the decomposition group $D_{\mathfrak{q}}$ at some $\mathfrak{q} \in N_2$ in K_3/K may be off the local plan and therefore it may not be liftable for the next stage of the induction.

Assume now that we are not on all local plans. As $H^1(\Gamma_{\mathfrak{q}})$ acts as a principal homogeneous spaces on the solutions to our local embedding problem, the existence of a local plan implies the existence of $f_{\mathfrak{q}} \in H^1(\Gamma_{\mathfrak{q}})$ by which we can adjust our solution to be on the local plan.

We now use Proposition 2.3 to find a tame prime $\mathfrak{r}$ such that for $R_2 = \{\mathfrak{r}\}$

$$(f_{\mathfrak{q}})_{\mathfrak{q} \in N_2} \in Im(\psi_{R_2}), \quad v_p(N(\mathfrak{r}) - 1) \geq m,$$

and $\mathfrak{r}$ splits completely in K_2/K. Hence there exists an element of $H^1(\Gamma_{N_2 \cup R_2})$ that puts us on the local plan for all $\mathfrak{q} \in N_2$. As $\mathfrak{r}$ splits completely in K_2/K, we can use an S-R local plan for $\mathfrak{r}$. Set $S_3 = S_2 \cup \{\mathfrak{r}\}$. We are on the local plan at all $\mathfrak{q} \in S_3$ and can proceed by induction.

As in the split case, all new primes of ramification are tame, so if $F \subset K^{ta}$, then our final field $L \subset K^{ta}$. □

4 Applications

4.1 The main result

In this section we prove:

Theorem 4.1 *Let p be an odd prime, $n \geq 3$ and K be a number field such that $\zeta_p \notin K$. Then the profinite groups Γ_K^{ta} and Γ_K satisfy the strong n-fold Massey vanishing property (relative to p).*

We use the cup product condition C_n as follows:

- We invoke it when we use that the local Galois groups $\Gamma_{\mathfrak{q}}$ satisfy the strong n-fold Massey vanishing property for $n \geq 3$.
- In Sect. 4.2 we present a proof when $p > n$ that uses the local triviality of $\chi_i \cup \chi_{i+1}$ and that $Ш^2_N = 0$.

Proof We have $\theta := (\chi_1, \cdots, \chi_n) : \Gamma \to (\mathbb{Z}/p)^n$. For every $\mathfrak{q} \in S$, denote by $\theta_{\mathfrak{q}} : \Gamma_{\mathfrak{q}} \to (\mathbb{Z}/p)^n$ the restriction of θ to $\Gamma_{\mathfrak{q}}$. For $\mathfrak{q}$ ramified in θ, recall that $\Gamma_{\mathfrak{q}}$ is either a Demushkin group or free pro-p. By [21, Proposition 4.1] and [20, Theorem 4.3] Demushkin groups satisfy the strong n-fold Massey vanishing property for $n \geq 3$. Recall U_{n+1} is the unipotent subgroup of $GL_{n+1}(\mathbb{F}_p)$ and $\varphi : U_{n+1} \twoheadrightarrow (\mathbb{Z}/p)^n$ is a natural quotient map. The lifts of $\theta_\mathfrak{q}$ to homomorphisms $\rho_\mathfrak{q} : \Gamma_\mathfrak{q} \to U_{n+1}$ whose existence is guaranteed by [20, 21] necessarily have image in $\varphi^{-1}(\theta(\Gamma)) \subset U_{n+1}$. These are the Massey local plans referred to at the end of Sect. 2.5.

$$\begin{tikzcd}
 & & \varphi^{-1}(\theta(\Gamma)) \arrow[r, hook] \arrow[d, two heads, "\varphi"'] & U_{n+1} \arrow[d, two heads, "\varphi"'] \\
\Gamma_\mathfrak{q} \arrow[r] \arrow[urr, "\rho_\mathfrak{q}"] \arrow[rr, bend right, "\theta_\mathfrak{q}"'] & \Gamma \arrow[r, two heads, "\theta"'] \arrow[ur, "?\rho"'] & \theta(\Gamma) \arrow[r, hook] & (\mathbb{Z}/p)^n
\end{tikzcd}$$

We simply apply Theorem 3.2 with $U = \varphi^{-1}(\theta(\Gamma))$ and $V = ker\varphi|_U$ to get the existence of ρ which we then compose with the injection $\varphi^{-1}(\theta(\Gamma)) \hookrightarrow U_{n+1}$ to establish the result. As Theorem 3.2 only introduces tame ramification, if θ is tamely ramified, then ρ is tamely ramified. $\square$

Remark 4.1 The method shows that each embedding problem can be solved by a tame prime $\mathfrak{q}$ that is given via the Chebotarev density theorem. One needs at most $n(n-1)/2$ such primes. Using GRH effective versions of Chebotarev's theorem, one can bound the absolute norms. See Remark 2.3.

4.2 Abelian plans

Let $\theta = (\chi_1, \cdots, \chi_n) : \Gamma_K^{ta} \to (\mathbb{Z}/p)^n$ be a homomorphism in C_n:

$$\chi_1 \cup \chi_2 = \chi_2 \cup \chi_3 = \cdots = \chi_{n-1} \cup \chi_n = 0.$$

In the proof of Theorem 4.1 above, we used the condition C_n only in the local results we cite from [21, Proposition 4.1] and [20, Theorem 4.3]. In this section we give another proof that uses local triviality of cup products for these primes when $p > n$ and highlights condition C_n.

Let S be the set of ramification of θ, which is by the choice of Γ_K^{ta} tame. Then for $\mathfrak{q} \in S$ we have $\zeta_p \in K_\mathfrak{q}$. For $\psi \in H^1(\Gamma_K^{ta})$, set $\psi_\mathfrak{q} := \psi|_{\Gamma_\mathfrak{q}}$.

Lemma 4.1 *Let p be odd and $\mathfrak{q}$ have norm 1 mod p. Set $\chi_{i,\mathfrak{q}} := \chi_i|_{\Gamma_\mathfrak{q}}$ and suppose $\chi_{i,\mathfrak{q}} \neq 0$. Then there exists $\lambda_{\mathfrak{q},i} \in \mathbb{Z}/p$ such that $\chi_{i+1,\mathfrak{q}} = \lambda_{\mathfrak{q},i}\chi_{i,\mathfrak{q}}$.*

Proof The arguments below are standard in local Galois cohomology. Using the local Euler-Poincaré characteristic and that $\zeta_p \in K_\mathfrak{q}$ one has

$$\dim H^i(\Gamma_\mathfrak{q}, \mathbb{Z}/p) = \dim H^i(\Gamma_\mathfrak{q}, \mu_p) = \begin{cases} 1 & \text{if } i = 0 \\ 2 & \text{if } i = 1 \\ 1 & \text{if } i = 2 \end{cases}.$$

As $\mu_p \simeq \mathbb{Z}/p$ (non-canonically) in $K_\mathfrak{q}$, the perfect local pairing becomes

$$H^1(\Gamma_\mathfrak{q}, \mathbb{Z}/p) \times H^1(\Gamma_\mathfrak{q}, \mathbb{Z}/p) \to H^2(\Gamma_\mathfrak{q}, \mathbb{Z}/p).$$

By the alternating property of cup products, each $\chi_{i,\mathfrak{q}}$ annihilates itself.

The annihilator of $\chi_{i,\mathfrak{q}}$ is codimension one in $H^1(\Gamma_\mathfrak{q})$ so the fact that $\dim H^1(\Gamma_\mathfrak{q}) = 2$ implies that the space spanned by $\chi_{i,\mathfrak{q}}$ is its own exact annihilator under the local pairing. The result follows from localizing $\chi_i \cup \chi_{i+1} = 0$ at $\mathfrak{q}$. □

We need to lift $\theta : \Gamma_K^{ta} \to (\mathbb{Z}/p)^n \twoheadleftarrow U_{n+1}$ to a homomorphism $\Gamma_K^{ta} \to U_{n+1}$. We will do this in separate blocks of (local) nonzero characters. Each trivial $\chi_{j,\mathfrak{q}}$ marks the end of a block at row j.

For a block with nonzero local characters, $\chi_{j,\mathfrak{q}}, \chi_{j+1,\mathfrak{q}}, \cdots, \chi_{j+k,\mathfrak{q}}$, we have by Lemma 4.1

$$\begin{aligned}
\chi_{j+1,\mathfrak{q}} &= \lambda_{j,\mathfrak{q}}\chi_{j,\mathfrak{q}}, \\
\chi_{j+2,\mathfrak{q}} &= \lambda_{j+1,\mathfrak{q}}\chi_{j+1,\mathfrak{q}}, \\
&\cdots \\
\chi_{j+k,\mathfrak{q}} &= \lambda_{j+k-1,\mathfrak{q}}\chi_{j+k-1,\mathfrak{q}}.
\end{aligned}$$

On this block we set $\rho_\mathfrak{q}(\sigma_\mathfrak{q})$ and $\rho_\mathfrak{q}(\tau_\mathfrak{q})$ to be elements of U_{n+1} that are nonzero only on the diagonal and on the 'near-diagonal', that is at (i, i) and $(i, i+1)$ entries. For example, with $n = 3$ and $\theta = (\chi_1, \chi_2, \chi_3)$ and $\chi_{2,\mathfrak{q}} = \lambda_{1,\mathfrak{q}}\chi_{1,\mathfrak{q}}$ and $\chi_{3,\mathfrak{q}} = \lambda_{2,\mathfrak{q}}\chi_{2,\mathfrak{q}}$ our local plan is, for $\gamma \in \{\sigma_\mathfrak{q}, \tau_\mathfrak{q}\}$:

$$\rho_\mathfrak{q}(\gamma) := \begin{pmatrix} 1 & \chi_{1,\mathfrak{q}}(\gamma) & 0 & 0 \\ 0 & 1 & \lambda_{1,\mathfrak{q}}\chi_{1,\mathfrak{q}}(\gamma) & 0 \\ 0 & 0 & 1 & \lambda_{1,\mathfrak{q}}\lambda_{2,\mathfrak{q}}\chi_{1,\mathfrak{q}}(\gamma) \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

From the definition of $\Lambda_\mathfrak{q}$ below, we have $\Lambda_\mathfrak{q}^{n+1} = 0$.

We first show $\rho_\mathfrak{q}(\sigma_\mathfrak{q})$ and $\rho_\mathfrak{q}(\tau_\mathfrak{q})$ commute. In our example with $n = 3$,

$$\Lambda_\mathfrak{q} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & \lambda_{1,\mathfrak{q}} & 0 \\ 0 & 0 & 0 & \lambda_{1,\mathfrak{q}}\lambda_{2,\mathfrak{q}} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

so

$$\begin{aligned}
\rho_\mathfrak{q}(\sigma_\mathfrak{q})\rho_\mathfrak{q}(\tau_\mathfrak{q})\rho_\mathfrak{q}(\sigma_\mathfrak{q})^{-1} &= \left(I + \chi_{1,\mathfrak{q}}(\sigma_\mathfrak{q})\Lambda_\mathfrak{q}\right)\left(I + \chi_{1,\mathfrak{q}}(\tau_\mathfrak{q})\Lambda_\mathfrak{q}\right)\left(I + \chi_{1,\mathfrak{q}}(\sigma_\mathfrak{q})\Lambda_\mathfrak{q}\right)^{-1} \\
&= I + \chi_{1,\mathfrak{q}}(\tau_\mathfrak{q})\Lambda_\mathfrak{q} \\
&= \rho_\mathfrak{q}(\tau_\mathfrak{q}).
\end{aligned}$$

We need to check that $\rho_{\mathfrak{q}}$ respects the relation $\sigma_{\mathfrak{q}}\tau_{\mathfrak{q}}\sigma_{\mathfrak{q}}^{-1} = \tau_{\mathfrak{q}}^{N(\mathfrak{q})}$, that is that $\rho_{\mathfrak{q}}(\tau_{\mathfrak{q}}) = \rho_{\mathfrak{q}}(\tau_{\mathfrak{q}})^{N(\mathfrak{q})}$ or equivalently, recalling that $N(\mathfrak{q}) - 1 = pb$ for some $b \in \mathbb{N}$, that

$$\rho_{\mathfrak{q}}(\tau_{\mathfrak{q}})^{pb} = (I + \chi_{1,\mathfrak{q}}(\tau_{\mathfrak{q}})\Lambda_{\mathfrak{q}})^{pb} \overset{?}{=} I.$$

This follows as in characteristic p we have $(I+\chi_{1,\mathfrak{q}}(\tau_{\mathfrak{q}})\Lambda_{\mathfrak{q}})^p = I+\chi_{1,\mathfrak{q}}^p(\tau_{\mathfrak{q}})\Lambda_{\mathfrak{q}}^p = I$ as $p > n$ and $\Lambda_{\mathfrak{q}}^{n+1} = 0$. Having local plans and invoking Theorem 3.2 we have proved:

Corollary 4.1 *Let $n \geq 3$, $p > n$ and $\zeta_p \notin K$. Then the strong Massey vanishing property holds for θ and Γ_K^{ta} with $\rho_{\mathfrak{q}}$ as above constructed in blocks. The element $\rho_{\mathfrak{q}}(\tau_{\mathfrak{q}})$ has order p in the lift $\rho : \Gamma_K^{ta} \to U_{n+1}$ of θ.*

4.3 More liftings

Set $r \geq 1$. Let $GL_{n+1}(\mathbb{Z}/p^r)$ be the group of invertible $(n+1) \times (n+1)$-matrices with entries in $\mathbb{Z}/p^r$ and $U_{n+1}(\mathbb{Z}/p^r) \subset GL_{n+1}(\mathbb{Z}/p^r)$ be the subgroup of all upper-triangular unipotent matrices. Let $\pi_r : GL_{n+1}(\mathbb{Z}/p^r) \to GL_{n+1}(\mathbb{Z}/p)$ be the mod p reduction homomorphism. It is well known that $Ker(\pi_r)$ is a p-group. Let $U \subset GL_{n+1}(\mathbb{Z}/p^r)$ be a p-group. The Scholz–Reichardt Theorem gives the existence of a Galois extension K over $\mathbb{Q}$ such that $Gal(K/\mathbb{Q}) \simeq U$. In this case, if p^m is the exponent of U, we can guarantee every ramified prime $\mathfrak{q}$ satisfies $N(\mathfrak{q}) \equiv 1$ modulo p^m and so all ramification is tame.

On the other hand, by following the Massey product philosophy, starting with $\theta : \Gamma \to (\mathbb{Z}/p)^n$ in C_n, one can ask if θ lifts to a $\rho_r : \Gamma \to GL_{n+1}(\mathbb{Z}/p^r)$ such that the diagram below commutes:

$$\begin{tikzcd}
 & \pi_r^{-1}\left(U_{n+1}(\mathbb{F}_p)\right) \subset GL_{n+1}(\mathbb{Z}/p^r) \arrow[d, "\pi_r"] \\
 & U_{n+1}(\mathbb{F}_p) \arrow[d, "\varphi"] \\
\Gamma \arrow[uur, "?\rho_r"] \arrow[ur, "\rho"'] \arrow[r, "\theta"'] & (\mathbb{Z}/p)^n
\end{tikzcd}$$

Here ρ is a lift given by Theorem 4.1. Since $Ker(\pi_r)$ is a p-group, our putative $\rho_r(\Gamma)$ is also a p-group.

Theorem 4.2 *Take $\Gamma = \Gamma_K^{ta}$ or Γ_K, and suppose $\zeta_p \notin K$. For $n \geq 3$, let $\theta : \Gamma \to (\mathbb{Z}/p)^n$ satisfy C_n. Let ρ be given by Theorem 4.1, where we choose all tame primes $\mathfrak{q}'$ from that proof to satisfy $N(\mathfrak{q}') \equiv 1$ modulo $p^{m(r)}$, where $p^{m(r)}$ is the exponent of $U_{n+1}(\mathbb{Z}/p^r)$. This is possible as $\zeta_p \notin K$.*

(i) *Then for every $r \geq 1$, there exists a homomorphism $\rho_r : \Gamma \to GL_{n+1}(\mathbb{Z}/p^r)$ such that $\pi_r \circ \rho_r = \rho$ and $\theta = \varphi \circ \pi_r \circ \rho_r$.*

(ii) *If moreover $\zeta_{p^r} \in K_{\mathfrak{q}}$ for every ramified prime $\mathfrak{q}$ in θ then ρ_r can be taken such that $\rho_r(\Gamma) \subset U_{n+1}(\mathbb{Z}/p^r)$.*

Proof (i) Let S be the set of ramified primes of θ. By [21, Proposition 4.1] and [20, Theorem 4.3], we may choose for each prime $\mathfrak{q} \in S$ a lift $\rho_{\mathfrak{q}} : \Gamma_{\mathfrak{q}} \to U_{n+1}(\mathbb{F}_p)$. Using Theorem 4.1 we realize a global lift $\rho : \Gamma \to U_{n+1}(\mathbb{F}_p)$ of θ whose local plans for all $\mathfrak{q} \in S$ are $\rho_{\mathfrak{q}}$.

We have to add many new ramified primes $\mathfrak{q}'$ to obtain ρ. As $\zeta_p \notin K$, they can be chosen such that $N(\mathfrak{q}') \equiv 1$ modulo $p^{m(r)}$, where $p^{m(r)}$ is the exponent of $U_{n+1}(\mathbb{Z}/p^r)$. We give each such prime $\mathfrak{q}'$ the [S-R] local plan for lifts of ρ to $GL_{n+1}(\mathbb{Z}/p^r)$, that is

- $\rho_{r,\mathfrak{q}'}(\sigma_{\mathfrak{q}'}) = 1$, and
- $\rho_{r,\mathfrak{q}'}(\tau_{\mathfrak{q}'})$ is any lift of $\rho_{\mathfrak{q}'}(\tau_{\mathfrak{q}'}) = \overline{x} \in U_{n+1}$, to $U_{n+1}(\mathbb{Z}/p^r)$. This element is killed by $p^{m(r)}$ and by local class field theory the image of τ in $\Gamma_{\mathfrak{q}}^{ab}$ has order at least $p^{m(r)}$.

It remains to show the existence, for $\mathfrak{q} \in S$, of local plans $\rho_{r,\mathfrak{q}} : \Gamma_{\mathfrak{q}} \to GL_{n+1}(\mathbb{Z}/p^r)$ whose reductions modulo p are $\rho_{\mathfrak{q}}$.

First, there is the trivial local plan: when $\mathfrak{q}|p$ and $\zeta_p \notin K_{\mathfrak{q}}$. As $\Gamma_{\mathfrak{q}}$ is free pro-p, any lift of $\rho_{\mathfrak{q}}(\Gamma_{\mathfrak{q}})$ in $U_{n+1}(\mathbb{Z}/p^r)$ works.

For the other primes $\mathfrak{q} \in S$ one needs more local lifting results. One uses the local plans for lifts of ρ to $GL_{n+1}(\mathbb{Z}/p^r)$ given by:

- Böckle [1, Theorem 1.3] for the tame primes ($\mathfrak{q} \nmid p$),
- Emerton and Gee [5, Theorem 6.4.4] for the wild primes ($\mathfrak{q}|p$).

In [1, 5], the authors prove the existence of lifts $\rho_{\infty,\mathfrak{q}}$ into $GL_{n+1}(\mathbb{Z}_p)$ for every representation $\Gamma_{\mathfrak{q}} \to GL_{n+1}(\mathbb{F}_p)$. Applying these results to $\rho_{\mathfrak{q}} : \Gamma_{\mathfrak{q}} \to U_{n+1}(\mathbb{F}_p)$, $\mathfrak{q} \in S$ and reducing modulo p^r gives the desired local plans. Now (i) follows by Theorem 3.2 with $U := \pi_r^{-1}(\rho(\Gamma))$ and $V = Ker(\pi_r) \cap U$.

For (ii), assume that $\zeta_{p^r} \in K_{\mathfrak{q}}$ and since $\rho_{\mathfrak{q}}(\Gamma_{\mathfrak{q}}) \subset U_{n+1}(\mathbb{F}_p)$, a recent result of Conti, Demarche and Florence [2] (the corollary of the main theorem in the introduction of that paper) shows that there exist local lifts $\rho_{r,\mathfrak{q}}$ of $\rho_{\mathfrak{q}}$ to $GL_{n+1}(\mathbb{Z}/p^r)$, that can be taken with image in $U_{n+1}(\mathbb{Z}/p^r)$. This result holds even if the residue characteristic of $\mathfrak{q}$ is p. Set $U := \pi_r^{-1}(\rho(\Gamma)) \cap U_{n+1}(\mathbb{Z}/p^r)$ and $V = Ker(\pi_r) \cap U$. Since $\rho(\Gamma) \simeq U/V$, and $\rho(\Gamma)$ and V are p-groups, we see U is also a p-group. We apply Theorem 3.2 with U, U/V, and the above local plans $\rho_{r,\mathfrak{q}}$. □

Our construction does not allow us to pass to the projective limit to get a lift in $GL_{n+1}(\mathbb{Z}_p)$. This is because $m(\infty) = \infty$ and we would need to choose primes $\mathfrak{q}'$ with $N(\mathfrak{q}') \equiv 1$ modulo p^∞.

Remark 4.2 Observe that in the nondegenerate case (the χ_i are independent in $H^1(\Gamma)$), it is an exercise to show $\rho(\Gamma) = U_{n+1}(\mathbb{F}_p)$ and then another exercise to show, in case (ii) of Theorem 4.2, that $\rho_r(\Gamma) = U_{n+1}(\mathbb{Z}/p^r)$.

To conclude we show why the condition '$\zeta_{p^r} \in K_{\mathfrak{q}}$' given in [2] is necessary in many cases.

Proposition 4.3 *Let $\mathfrak{q}$ be a tame prime. Suppose given a homomorphism $\rho_\mathfrak{q} : \Gamma_\mathfrak{q} \to U_{n+1}(\mathbb{F}_p)$, and a lift $\rho_{\mathfrak{q},r}$ of $\rho_\mathfrak{q}$ to $U_{n+1}(\mathbb{Z}/p^r)$:*

$$\begin{tikzcd} & U_{n+1}(\mathbb{Z}/p^r) \arrow[d, "\pi_r"] \\ \Gamma_\mathfrak{q} \arrow[ur, "\rho_{\mathfrak{q},r}"] \arrow[r, "\rho_\mathfrak{q}"'] & U_{n+1}(\mathbb{F}_p) \end{tikzcd}$$

If a character θ_i on the near diagonal of $U_{n+1}(\mathbb{F}_p)$ is ramified, then $\zeta_{p^r} \in K_\mathfrak{q}$. That is, if $\theta_i(\tau_\mathfrak{q}) \neq 0$, then $N(\mathfrak{q}) \equiv 1$ modulo p^r.

Proof By hypothesis there exists $\theta_i \in H^1(\Gamma_\mathfrak{q}, \mathbb{Z}/p)$ such that $\theta_i(\tau_\mathfrak{q}) \neq 0$. But this homomorphism lifts to $\theta_{i,r} \in H^1(\Gamma_\mathfrak{q}, \mathbb{Z}/p^r)$. The two corresponding extensions are *cyclic extensions*, the first included in the second, and since θ_i is ramified (at $\mathfrak{q}$), it forces the cyclic degree p^r extension associated to $\theta_{i,r}$ to be totally ramified, which implies $\zeta_{p^r} \in K_\mathfrak{q}$ by class field theory. □

4.4 Further remarks on strong Massey vanishing and Gras' Conjecture.

In this subsection we allow $p = 2$. Let S be a finite set of primes of K and set K_S to be the maximal pro-p extension of K unramified outside S. When $p = 2$, we assume that the real archimedean places remain real in every subfield of K_S. Set $\Gamma_S := Gal(K_S/K)$. Shafarevich and Koch showed the pro-p group Γ_S is finitely generated.

4.4.1 Free groups

Let S_p be the set of p-adic primes of K. As first observed by Shafarevich, Γ_{S_p} can be a free noncommutative pro-p group. For instance, when $K = \mathbb{Q}(\zeta_p)$ and p is regular, then Γ_{S_p} is free on $(p+1)/2$ generators. When Γ_{S_p} is free, it obviously satisfies the strong n-fold Massey vanishing property for every $n \geq 2$. We state a Conjecture of Gras [8, Conjecture 7.11]:

Conjecture 1 (Gras) *Fix a number field K. For $p \gg 0$ the pro-p group Γ_{S_p} is free on $r_2 + 1$ generators, where $2r_2$ is the number of complex embeddings of K.*

4.4.2 Deep relations

When $S \cap S_p = \emptyset$, the pro-p group Γ_S is FAB: every open subgroup has finite abelianization.

Observe first that Γ_S can be trivial: take $K = \mathbb{Q}$, and $S = \emptyset$. It can also be cyclic of order p^m: take $K = \mathbb{Q}$, p odd, and ℓ a prime such that $v_p(\ell - 1) = m$. Set $S = \{\ell\}$; then $\Gamma_S \simeq \mathbb{Z}/p^m$. In this situation, it is not difficult to see that Γ_S satisfies the strong n-fold Massey vanishing property if and only if $n + 1 \leq p^m$. In the cyclic setting,

Γ_S is presented by one generator x and one relation $r := x^{p^m}$ of depth p^m (using the Zassenhaus filtration).

Vogel has the following general result [27, Corollary 1.2.9]:

Theorem 4.4 *Let G be a finitely generated pro-p group described by generators and a set R of relations. If all elements of R are of at least depth $n+1$, then G satisfies the strong k-fold Massey vanishing property for $2 \leq k \leq n$.*

Theorem 4.4 follows immediately from Lemma 4.2 below. While we have not previously used the language and notation of Massey products, we do so in its proof.

Lemma 4.2 *We use the terminology as in [28]. Let G be a pro-p group and $n \geq 2$ an integer. Suppose that $G = F/R$ where F is a free pro-p group on generators $x_1, \ldots, x_n$, and $R \subseteq F^p[F, F]$. The following are equivalent:*

i) $R \subseteq F_{(n+1)}$.
ii) *All k-fold Massey products are strictly and uniquely defined and equal to 0, for $2 \leq k \leq n$.*
iii) *G satisfies the strong k-fold Massey vanishing property for $2 \leq k \leq n$.*
iv) *G satisfies the k-fold Massey vanishing property for $2 \leq k \leq n$.*

Proof The implication from i) to ii) follows from [28, Theorem A3].

The implications from ii) to iii) and from iii) to iv) are clear.

Now we suppose that iv) holds. Let $\chi_1, \ldots, \chi_n \in H^1(F, \mathbb{F}_p) = H^1(G, \mathbb{F}_p)$ be the dual basis to $x_1, \ldots, x_n$. That G satisfies the 2-fold Massey vanishing property means that all cup products $\chi_{i_1} \cup \chi_{i_2}$ are zero, for $1 \leq i_1, i_2 \leq n$. By [28, Theorem A3], for every $f \in R$ and every $1 \leq i_1, i_2 \leq n$, $I = (i_1, i_2)$, one has

$$\epsilon_{I,p}(f) = (-1)^{2-1}\mathrm{tr}_f\langle \chi_{i_1}, \chi_{i_2}\rangle = 0.$$

This implies that $f \in F_{(3)}$ by [28, Lemma 2.19], and hence $R \subseteq F_{(3)}$.

Now because $R \subseteq F_{(3)}$, we see that for all $1 \leq i_1, i_2, i_3 \leq n$, triple Massey products $\langle \chi_{i_1}, \chi_{i_2}, \chi_{i_3}\rangle$ are well-defined, by [28, Theorem A3]. Thus $\langle \chi_{i_1}, \chi_{i_2}, \chi_{i_3}\rangle = 0$ because G satisfies the 3-fold Massey vanishing property. Also by [28, Theorem A3], for every $f \in R$ and every $1 \leq i_1, i_2, i_3 \leq n$, $I = (i_1, i_2, i_3)$, one has

$$\epsilon_{I,p}(f) = (-1)^{3-1}\mathrm{tr}_f\langle \chi_{i_1}, \chi_{i_2}, \chi_{i_3}\rangle = 0.$$

This implies that $f \in F_{(4)}$ by [28, Lemma 2.19]. Hence $R \subseteq F_{(4)}$. Continuing in this way, we show that $R \subseteq F_{(k+1)}$ for all $2 \leq k \leq n$. In particular, $R \subseteq F_{(n+1)}$. □

To conclude, we give another situation where we can apply Theorem 4.4 . Take T a finite set of primes of K, disjoint from S. Let K_S^T be the maximal pro-p extension of K unramified outside S, with the primes of T splitting completely in K_S^T. Set $\Gamma_S^T := Gal(K_S^T/K)$.

Corollary 4.2 *Take $n \geq 3$. Let K be a number field, not totally real, satisfying Gras' conjecture. Then for $p \gg 0$, there exists a set T of primes of K, coprime to p, such that the pro-p group $\Gamma_{S_p}^T$ is infinite, has finite abelianization and satisfies the strong n-fold Massey vanishing property.*

Proof We apply the strategy of [10]: We may take the quotient of the free pro-p group Γ_{S_p} (Gras' conjecture) by any Frobenius elements whose depth in the Zassenhaus filtration is greater than $n+1$, by p^n-powers of Frobenius elements that generate Γ_{S_p}, and apply Theorem 4.4. Chebotarev's theorem gives a positive density of such primes for our set T. □

Acknowledgements The authors thank Alexander Merkurjev and Federico Scavia for related discussions with Christian Maire and Jan Mináč during the *Workshop on Galois Cohomology and Massey Products* in June 2024. In particular, we are grateful to Federico Scavia for bringing our attention to related work in progress of Peter Koymans. We are also grateful to Koymans for subsequent discussion of these topics. We thank the anonymous referee for numerous helpful suggestions. The first, second, and third authors gratefully acknowledge the support of the Western Academy for Advanced Research (WAFAR) during the year 2022/23 and for support during a summer 2023 visit. The first author was also partially supported by the EIPHI Graduate School (contract "ANR-17-EURE-0002") and by the Bourgogne-Franche-Comté Region. The second author was partially supported by the Natural Sciences Engineering and Research Council of Canada (NSERC), Grant R0370A01. The third author was partially supported by Simons Collaboration Grant #524863. The fourth author was partially supported by the Vietnam National Foundation for Science and Technology Development (NAFOSTED) under Grant number 101.04-2023.21.

Data availability This manuscript has no associated data.

Declarations

Conflict of interest On behalf of all the authors, the corresponding author states there is no conflict of interest.

References

1. Böckle, G.: Lifting mod p representations to characteristics p^2. J. Number Theory **101**(2), 310–337 (2003)
2. Conti, A., Demarche, C., Florence, M.: Lifting Galois representations via Kummer flags. arXiv:2403.08888 (2026)
3. Dwyer, W.G.: Homology, Massey products and maps between groups. J. Pure Appl. Algebra **6**(2), 177–190 (1975)
4. Efrat, I., Matzri, E.: Triple Massey products and absolute Galois groups. J. Eur. Math. Soc. (JEMS) **19**(12), 3629–3640 (2017)
5. Emerton, M., Gee, T.: Moduli stacks of étale (φ, Γ)-modules and the existence of crystalline lifts. Ann. Math Stud. **215**, 175–177 (2023)
6. Guillot, P., Mináč, J., Harpaz, A.: Four-fold Massey products in Galois cohomology, With an appendix by Olivier Wittenberg. Compos. Math. **154**(9), 1921–1959 (2018)
7. Gras, G.: Class Field Theory: from Theory to Practice, Corr., Springer Monographs in Mathematics, 2nd edn. Springer (2005)

8. Gras, G.: Les Θ-régulateurs locaux d'un nombre algébrique:Conjectures p-adiques. Can. J. Math. **68**, 571–624 (2016)
9. Hajir, F., Larsen, M., Maire, C., Ramakrishna, R.: On tamely ramified infinite Galois extensions. J. Lond. Math. Soc. (2) **112**(1), 70209, 27 (2025)
10. Hajir, F., Maire, C., Ramakrishna, R.: Cutting towers of number fields. Ann. Math. Qué. **45**, 321–345 (2021)
11. Harpaz, Y., Wittenberg, O.: The Massey vanishing conjecture for number fields. Duke Math. J. **172**(1), 1–41 (2023)
12. Hopkins, J.M., Wickelgren, K.G.: Splitting varieties for triple Massey products. J. Pure Appl. Algebra **219**(5), 1304–1319 (2015)
13. Koch, H.: Galois Theory of p-Extensions. Springer, Berlin (2002)
14. Lagarias, J.C., Odlyzko, A.M.: Effective versions of the Chebotarev density theorem, Algebraic number fields: L-functions and Galois properties. In: Proceedings of the Symposium, University of Durham, Durham, pp. 409–464. Academic Press, London (1975)
15. Matzri, E.: Massey products in Galois cohomology. arXiv:1609.07927
16. Merkurjev, A., Scavia, F.: Degenerate fourfold Massey products over arbitrary field. J. Eur. Math. Soc. (JEMS). **28**(8), 3499–3537 (2026)
17. Merkurjev, A., Scavia, F.: The Massey vanishing conjecture for fourfold Massey products modulo 2. Ann. Sci. Éc. Norm. Supér. (4) **58**(3), 589–606 (2025)
18. Merkurjev, A., Scavia, F.: Non-formality of Galois cohomology modulo all primes. Compos. Math. **161**(4), 831–858 (2025)
19. Merkurjev, A., Scavia, F.: Lectures on the Massey vanishing conjecture. In: Gille, S., Zaynullin, K. (eds.) Proceedings of Workshop on Galois Cohomology and Massey Products, Ottawa, June 13–16, 2024 **(to appear)**
20. Mináč, J., Tân, N.D.: Triple Massey product and Galois theory. J. Eur. Math. Soc. (JEMS) **19**(1), 255–284 (2017)
21. Mináč, J., Tân, N.D.: Counting Galois $U_4(\mathbb{F}_p)$-extensions using Massey products. J. Number Theory **176**, 76–112 (2017)
22. Mináč, J., Tân, N.D.: Triple Massey products vanish over all fields. J. Lond. Math. Soc. (2) **94**(3), 909–932 (2016)
23. Neukirch, J.: On solvable number fields. Invent. Math. **53**(2), 135–164 (1979)
24. Neukirch, J., Schmidt, A., Wingberg, K.: Cohomology of Number Fields, Corrected Second Printing, GMW 323, 2nd edn. Springer, Berlin (2013)
25. Pál, A., G.: Quick A_3-formality for Demushkin groups at odd primes. arXiv:2601.07551
26. Serre, J.-P.: Topics in Galois Theory, Research Notes in Mathematics, 2nd edn. A K Peters Ltd, Wellesley (2008)
27. Vogel, D.: Massey products in the Galois cohomology of number fields. PhD Heidelberg (2004)
28. Vogel, D.: On the Galois group of 2-extensions with restricted ramification. J. Reine Angew. Math. **581**, 117–150 (2005)