ON THE STRONG MASSEY PROPERTY FOR NUMBER FIELDS

CHRISTIAN MAIRE, JÁN MINÁČ, RAVI RAMAKRISHNA, AND NGUYỄN DUY TÂN

In memory of Nigel Boston

ABSTRACT. Let $n \geqslant 3$. 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 property relative to p. Our work is based on an adapted version of the proof of the Theorem of Scholz-Reichardt.

Fix K a number field and an 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 a 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 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 [19, Chapter 2, §2.1]). This strategy has implications for Massey products as well.

Let $n \geqslant 3$ 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 $Z_{n+1} = \langle E_{1,n+1} \rangle$ 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 $\overline{U}_{n+1} := U_{n+1}/Z_{n+1}$ to be the quotient. To Γ a profinite group and a continuous homomorphism $\rho : \Gamma \to U_{n+1}$ with $1 \leqslant i < j \leqslant n+1$, we associate the functions $\rho_{i,j} : \Gamma \to \mathbb{F}_p$ giving the (i, j)-coordinate. We use similar notation for homomorphisms $\overline{\rho} : \Gamma \to \overline{U}_{n+1}$. Note that $\rho_{i,i+1}$ (resp., $\overline{\rho}_{i,i+1}$) is a group homomorphism. Set

$$\varphi := (\rho_{1,2}, \cdots, \rho_{n,n+1}) \text{ so } \varphi(U_{n+1}) = (\mathbb{Z}/p)^n$$

Date: August 31, 2024.

1991 *Mathematics Subject Classification.* 55S30, 11R32, 11R37,12G05.

Key words and phrases. Massey products, embedding problem, Scholz-Reichardt Theorem.

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. The first, seccond and third authors gratefully acknowledge the support of the 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.

and

$$\overline{\varphi} := (\overline{\rho}_{1,2}, \cdots, \overline{\rho}_{n,n+1}) \text{ so } \overline{\varphi}(U_{n+1}) = (\mathbb{Z}/p)^n.$$

We have the commutative diagram of groups:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & Z_{n+1} & \longrightarrow & U_{n+1} & \longrightarrow & \overline{U}_{n+1} & \longrightarrow & 1 \\ & & & & & \overset{\varphi}{\searrow} & \downarrow \overline{\varphi} & & \\ & & & & & & (\mathbb{Z}/p)^n & & \end{array}$$

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 original definition of the Massey product and instead use a consequence which characterizes the 'defined' and 'vanishing' conditions via group representations. below. For more details see [3] and also [10], [14] and [15]. Note that the definitions of Massey products in [3] and [15] differ from those in [10] and [14] by a sign.

Definition. *Let $\chi_1, \cdots, \chi_n \in H^1(\Gamma, \mathbb{Z}/p)$. The Massey product $\langle \chi_1, \cdots, \chi_n \rangle \subset H^2(\Gamma, \mathbb{Z}/p)$*

- *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 $\rho : \Gamma \to U_{n+1}$.*

These definitions depend crucially on the ordering of the characters. Also, we do not have *a priori*: $\rho' \equiv \rho$ modulo Z_{n+1}.

Definition. *The profinite group Γ satisfies the strong n-fold Massey 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

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

One has $A_n \subset B_n \subset C_n$. That $A_n \subset B_n$ follows from Definition 3.1. That $B_n \subset C_n$ follows from a simple argument - see [14, Remark 2.2]. For $n = 3$, $B_3 = C_3$. Other inclusions may be strict in general.

For $p = 2$ and Γ_K the absolute Galois group of a number field K, Hopkins and Wickelgren [11] have shown the remarkable result that the triple Massey product vanishes whenever it is defined. In [15] this is established for Γ_F the absolute Galois group of any field F. Harpaz and Wittenberg [10] have recently proved the Mináč-Tân Conjecture for number fields K: Γ_K satisfies the n-fold Massey property for p, that is $A_n = B_n$.

If a primitive pth-root of unity is in a number field K, there are counterexamples to the strong n-fold Massey property for Γ_K, that is there are examples where $B_n \subsetneq C_n$ so we do not have $A_n = B_n = C_n$. In Wittenberg's appendix to [5] there is an interesting example discovered by

Harpaz and Wittenberg. For $K = \mathbb{Q}$ and $p = 2$ the 4-fold Massey $\langle 34, 2, 17, 34\rangle$ is not defined despite the fact that Hilbert symbols $(34, 2), (2, 17), (17, 34)$ vanish (by Kummer theory we have replaced elements of $H^1(\Gamma_{\mathbb{Q}}, \mathbb{Z}/2)$ by elements of $\mathbb{Q}^\times$). 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 [5]. This example was generalized by Merkurjev-Scavia [14, §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 verify the strong fourfold Massey property, i.e. $B_4 \subsetneq C_4$.

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

Theorem 1. *Take $n \geqslant 3$, and suppose that $\zeta_p \notin K$. The profinite groups Γ_K and Γ_K^{ta} satisfy the strong n-fold Massey property relative to p, that is $A_n = B_n = C_n$.*

We obtain this theorem by giving a global lifting result (Theorem 2.2) in the spirit of the inverse Galois problem over number fields for p-groups U with local conditions, as developed in [18, IX, §5, Theorem 9.5.5] or [17, Main Theorem]. When compared to the main theorem of Neukirch in [17], 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 use Chebotarev's theorem repeatedly, usually applied simultaneously to a governing field and the part of the tower we have already constructed in our inductive process to provide us with the primes of K that we need. The hypothesis $\zeta_p \notin K$ is important throughout this paper. It implies our field extensions are linearly disjoint over K so we can choose primes of K to split in these fields as we need.

We can strengthen the theorem above by showing that θ lifts, for any $r \geqslant 1$, to a subgroup of $Gl_{n+1}(\mathbb{Z}/p^r)$. Let $\pi_r : Gl_{n+1}(\mathbb{Z}/p^r) \to Gl_{n+1}(\mathbb{F}_p)$ be the mod p reduction homomorphism.

Theorem 2. *Take $\Gamma = \Gamma_K^{ta}$ or Γ_K, and suppose $\zeta_p \notin K$. For $n \geqslant 3$, let $\theta : \Gamma \to (\mathbb{Z}/p)^n$ satisfy C_n. Let ρ be given by Theorem 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 $\zeta_p \notin K$. Let $\pi_r : Gl_{n+1}(\mathbb{Z}/p^r) \to GL_{n+1}(\mathbb{F}_p)$ be the natural projection.*
(i) Then for every $r \geqslant 1$, 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 $\rho_r(\Gamma) \subset U_{n+1}(\mathbb{Z}/p^r)$.

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. Almost all cohomology groups $H^i(G, \mathbb{Z}/p\mathbb{Z})$ have $\mathbb{Z}/p\mathbb{Z}$-coefficients with trivial action so in those cases we simply write $H^i(G)$.

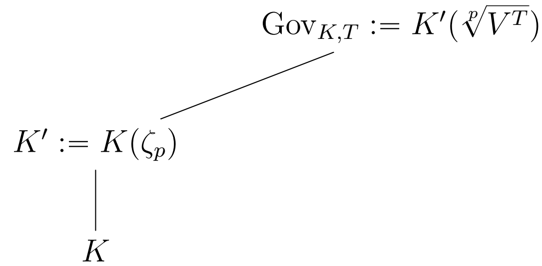
1. Tools for the Embedding problem

1.1. **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 [19, 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 1.7).

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

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

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



By Kummer theory we see $\mathrm{Gov}_{K,T}/K'$ is an elementary abelian p-extension. One easily computes it is unramified outside $T \cup \{\mathfrak{p}|p\}$. 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 on $Gal(K'/K)$ is given by Kummer duality: since $Gal(K'/K)$ acts trivially on V^T, it acts via the cyclotomic character (which is nontrivial 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 [6, Chapter I, Theorem 6.2].

For a tame prime $\mathfrak{q} \notin T$ (that is $\mathfrak{q} \nmid (p)$), we write $\sigma_\mathfrak{q}$ for the Frobenius in $Gal(\mathrm{Gov}_{K,T}/K')$ for a fixed prime $\mathfrak{Q}$ above $\mathfrak{q}$. One has (see [6, Chapter V, Corollary 2.4.2]):

Theorem 1.1 (Gras)**.** *Let $S = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_s\}$ be a set of primes of K coprime to T and p. There exists a cyclic degree 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*

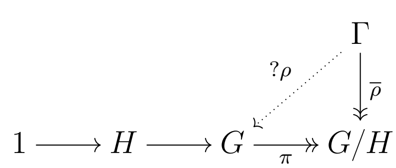
$$\sum_{i=1}^{s} a_i \sigma_{\mathfrak{q}_i} = 0 \in Gal(\mathrm{Gov}_{K,T}/K').$$

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.

Remark 1.2. *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 power that is not a multiple of p. This follows from our description of $Gal(K'(\sqrt[p]{V^T})/K)$ above and does not affect the condition of Theorem 1.1. Hence we abuse notation and write $\sigma_\mathfrak{q}$. Later we will also use the governing field $K'(\sqrt[p]{V_N})$ where $V_N = \{x \in K^\times; v_\mathfrak{q}(x) \equiv 0 \bmod p;\ \mathfrak{q} \in N \implies x \in (K_\mathfrak{q}^\times)^p\}$.*

1.2. **Cohomology and embedding problems.** Let G be a p-group of p-rank d. Suppose given $H \simeq \mathbb{Z}/p$ a normal subgroup of G such that G/H also has p-rank d. Let Γ be a pro-p group, and let $\overline{\rho} : \Gamma \twoheadrightarrow G/H$ be a surjective morphism.

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



where π is the natural projection. That G and G/H have the same p-rank implies $H \subset G^p[G,G]$, so every solution of $(\mathscr{E})$ is *proper*, that is if ρ exists, it is surjective.

Let ε be the element in $H^2(G/H, H) = H^2(G/H, \mathbb{Z}/p) = H^2(G/H)$ corresponding to the group extension:

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

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

Theorem 1.3. *The embedding problem $(\mathscr{E})$ has a solution if and only if $Inf(\varepsilon) = 0$. Moreover, any solution is always proper. The set of solutions (modulo equivalence) of $(\mathscr{E})$ is a principal homogeneous space under $H^1(\Gamma)$.*

Proof. Proposition 3.5.9 and 3.5.11 of [18]. ∎

Remark 1.4. *For a prime $\mathfrak{q}$ of K, denote by $\Gamma_{\mathfrak{q}}$ the absolute pro-p 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 $(\mathscr{E}_{\mathfrak{q}})$:*

$$\begin{array}{ccccccc} & & & & & & \Gamma_{\mathfrak{q}} \\ & & & & & {\scriptstyle ?\rho_{\mathfrak{q}}} \swarrow & \downarrow{\scriptstyle \overline{\rho_{\mathfrak{q}}}} \\ 1 & \longrightarrow & H_{\mathfrak{q}} & \longrightarrow & M_{\mathfrak{q}} & \xrightarrow[\pi_{\mathfrak{q}}]{} & \overline{D}_{\mathfrak{q}} \end{array}$$

The set of solutions (modulo equivalence and if it exists) of $(\mathscr{E}_{\mathfrak{q}})$ is a principal homogeneous space under $H^1(\Gamma_{\mathfrak{q}})$.

1.3. **Trivializing the Shafarevich group.** Let X be a finite set of places of K. Let K_X 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 $V_X := \{x \in K^\times; v_{\mathfrak{q}}(x) \equiv 0 \bmod p,\ \forall \mathfrak{q}; x \in (K_{\mathfrak{q}}^\times)^p,\ \forall \mathfrak{q} \in X\}$. By the work of Koch and Shafarevich (see [12, Chapter 11, Theorem 11.3]), we have that

$$Ш^2_X \hookrightarrow Б_X := (V_X/(K^\times)^p)^\wedge,$$

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

Lemma 1.5. *One can choose N 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, by Hermite-Minkowski, finitely generated, we see for a finite set N whose Frobenius elements span $Gal(K'(\sqrt[p]{V_\varnothing})/K')$ (which exists by Chebotarev's theorem) that $K'(\sqrt[p]{V_N}) = K'$. Thus $\forall x \in V_N$ we have $x \in (K')^p$. By taking the norm of x in K'/K and using the fact that $([K' : K], p) = 1$, we conclude that $x \in K^p$. Thus $V_N/(K^\times)^p = 1$ which implies $Ш^2_N = 1$. ∎

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

Henceforth we assume that $Ш^2_N = 1$ 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 $(\mathscr{E})$ 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 §1.5) 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 two next subsections.

1.4. **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 to for Proposition 1.7.

Lemma 1.6. *Let F/K be a p-extension. 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 degree 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 cyclotomic character by viewing M in $K'(\sqrt[p]{V^X})/K'$. These actions are incompatible when $\zeta_p \notin K$. □

Recall Proposition 1.4 of [9].

Proposition 1.7. *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 p-extension,
(ii) the p-adic valuation of $N(\tilde{\mathfrak{q}}) - 1$ is given in advance.

Proof. See §1.2 of [9]. □

Remark 1.8. *Take $m \geqslant 1$. In the proof of Proposition 1.7 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 $v_p(N(\tilde{\mathfrak{q}}) - 1) = m$. Thus 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 absolue discriminant of the number field $K(\zeta_{p^{m+1}}, \sqrt{V^X})$. Then, assuming the GRH, $N(\tilde{\mathfrak{q}}) \ll (\log(d_{X,m}))^2$. See* [13].

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

$$\begin{array}{ccccccc} & & & & & & \Gamma \\ & & & & & \overset{?\rho}{\swarrow} & \downarrow \overline{\rho} \\ 1 & \longrightarrow & V & \longrightarrow & U & \underset{\pi}{\twoheadrightarrow} & U/V \end{array}$$

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 $\mathbb{Z}/p$, 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 set N is taken so that $Ш^2_N = 1$. 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:

$$\begin{array}{ccc} & & \Gamma_{\mathfrak{q}} \\ & \overset{?\rho_{\mathfrak{q}}}{\swarrow} & \downarrow \overline{\rho}_{\mathfrak{q}} \\ U & \twoheadrightarrow & U/V \end{array}$$

If $\rho_{\mathfrak{q}}$ exists, we say that $\rho_{\mathfrak{q}}$ is a *local plan* for $\Gamma_{\mathfrak{q}}$ into U.

Recall that the pro-p group $\Gamma_{\mathfrak{q}}$ is

- free when $\zeta_p \notin K_{\mathfrak{q}}$,
- 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 [12, 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. 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-root of the unity.

We give examples of local plans.

Example 1.9. *[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 $v_p(N(\mathfrak{q})-1) = m$ - this is possible as $\zeta_p \notin K$. 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.*

Example 1.10. *[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.
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 works in this case as well.

Example 1.11. *[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 $N(\mathfrak{q}) \equiv 1 \pmod{p^k}$ with $k \geqslant \ell$. 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 $\overline{\rho}_{\mathfrak{q}}(\tau_{\mathfrak{q}}) = \overline{y}$. 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.*

There is another important local plan in the context of Massey products coming from results of Mináč-Tân ([16, Proposition 4.1] and [15, Theorem 4.3]). We call these *Massey local plans* and use them in the proof of Theorem 3.1.

2. A global lifting result

The main result of this section is Theorem 2.2, a variation of the Scholz-Reichardt theorem. We start with a proposition useful in proving this theorem in the split case, that is when $d(U) > d(U/V)$. In the context of the strong Massey property, it is useful for the *degenerate case.*

Proposition 2.1. *Suppose that $\zeta_p \notin K$. Let F/K be a p-extension and let S be a finite set of primes of K. Let $k, m \geqslant 1$ and for $i = 1, \cdots, k$ let $(\chi_{\mathfrak{q},i})_{\mathfrak{q}\in S} \in H^1(\Gamma_{\mathfrak{q}})$. Then for $i = 1, \cdots, k$*

- (i) *there exist a $\chi_i \in H^1(\Gamma_K)$ 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 $v_p(N(\mathfrak{q}'_i) - 1) = m$;*
- (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. Given Proposition 1.7, (i), (ii) and (iv) are perhaps not surprising and (iv) involves a straightforward trick. Establishing (v) is crucial for our results and this requires Gras' result, Theorem 1.1.

• By Proposition 1.7, there exists a tame prime $\mathfrak{q}'$ such that there exists a $\chi_1 \in H^1(\Gamma_{S\cup\{\mathfrak{q}'\}})$ that $\chi_1 \mid_{\Gamma_{\mathfrak{q}}} = \chi_{\mathfrak{q},1}$ for each $\mathfrak{q} \in S$. This is (i). Moreover, since $\zeta_p \notin K$, using that $\mathrm{Gov}_{K,S}/K'$ and $F(\zeta_{p^{m+1}})/K'$ are linearly disjoint, we can choose $\mathfrak{q}'$ such that $v_p(N(\mathfrak{q}') - 1) = m$ and $\mathfrak{q}'$ splits completely in F/K. Set M to be the $\mathbb{Z}/p$-extension of K fixed by χ_1.
If χ_1 is ramified at $\mathfrak{q}'$, then we set $M_1 := M$ and $\mathfrak{q}'_1 := \mathfrak{q}'$.
If χ_1 is unramified at $\mathfrak{q}'$, we choose a tame prime $\mathfrak{q}'_1$ that splits completely in $\mathrm{Gov}_{K,S}F(\zeta_{p^m})/K$ but does not split completely in $K(\zeta_{p^{m+1}})/K$. By Theorem 1.1 there exists a $\mathbb{Z}/p$-extension M'_1/K exactly ramified at $\mathfrak{q}'_1$ in which the places of S split completely. Then $Gal(M'_1M/K) \simeq \mathbb{Z}/p \times \mathbb{Z}/p$, we choose M_1 to be any intermediate extension other than than M and M'_1. The field M'_1 satisfies (ii), (iii), and (iv), but we must exclude it get (i). We have established $(i) - (iv)$.

• Set $S_1 = S \cup \{\mathfrak{q}_1'\}$. Set $\chi_{\mathfrak{q}_1'} \in H^1(\Gamma_{\mathfrak{q}_1'})$ to be trivial. By Proposition 1.7, there is a tame prime $\mathfrak{q}'$ such that there exists a $\chi \in H^1(\Gamma_{S_1 \cup \{\mathfrak{q}'\}})$ with $\chi|_{\Gamma_\mathfrak{q}} = \chi_{\mathfrak{q},2}$ 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 $v_p(N(\mathfrak{q}') - 1) = m$, and such that $\mathfrak{q}'$ splits completely in FM_1/K (indeed $\mathrm{Gov}_{K,S}/K'$ and $FM_1(\zeta_{p^{m+1}})/K'$ are linearly disjoint). As before, set M to be the $\mathbb{Z}/p$-extension of K corresponding to χ. By the choice of $\chi_{\mathfrak{q}_1'}$, observe that $\mathfrak{q}_1'$ splits completely in M/K.
If χ is ramified at $\mathfrak{q}'$, set $M_2 = M$ and $\mathfrak{q}_2' := \mathfrak{q}'$.
If χ is unramified we proceed as did above to get $\mathfrak{q}_2'$ and M_2.
Then, in all case, one has $(i) - (iv)$.

Note that the splitting choices on $\mathfrak{q}_1'$ 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 2.2 is the key result we need to establish the strong n-fold Massey property for Γ_K and Γ_K^{ta}. The proof of Theorem 2.2 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 easy to introduce and maintain. In § 3.1 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 it ourselves.

Theorem 2.2. *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 $\mathfrak{q}_i \in S$ the decomposition group $\overline{D}_{\mathfrak{q}_i}$ in F/K respects a local plan $\rho_{\mathfrak{q}_i} : \Gamma_{\mathfrak{q}_i} \to U$. In other words, $D_{\mathfrak{q}_i} \equiv \rho_{\mathfrak{q}_i}(\Gamma_{\mathfrak{q}_i})$ modulo V.*
- *$Gal(F/K) \simeq U/V$.*

Then there exists a Galois extension L/K in $\overline{K}/K$ 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 1.6 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 $K(\zeta_{p^{m+1}})$, F and $\mathrm{Gov}_{K,S}$.

We first solve the problem when the group extension $1 \to V \to U \to U/V \to 1$ is split.

• Let d be the p-rank of U, and let d_0 be the p-rank of U/V. Set $k = d - d_0$.
Since we are in the split setting, $k > 0$. Hence $V \not\subset U^p[U,U]$: there exists a maximal subgroup U_1 of U such that $V \not\subset U_1$. By maximality $U_1 \lhd U$ and we have

$$U/(V \cap U_1) \hookrightarrow U/V \times U/U_1.$$

On the other hand

$$1 \longrightarrow V/(V \cap U_1) \longrightarrow U/(V \cap U_1) \longrightarrow U/V \longrightarrow 1$$

and $V/(V \cap U_1) \simeq VU_1/U_1 \hookrightarrow U/U_1 \simeq \mathbb{Z}/p$. Since $V \not\subset U_1$, we see

$$|U/(V \cap U_1)| = |U/V||U/U_1|,$$

and then

$$g_1 : U/(V \cap U_1) \xrightarrow{\simeq} U/V \times U/U_1 \simeq U/V \times \mathbb{Z}/p\cdot$$

Set $A_1 := V \cap U_1$ so U/A_1 has p-rank $d_0 + 1$. Set $k' = d - (d_0 + 1)$. If $k' > 0$ then, as before, there exists a maximal subgroup U_2 of U such that $A_1 \not\subset U_2$, and then

$$g_2 : U/(A_1 \cap U_2) \xrightarrow{\simeq} U/A_1 \times U/U_2 \simeq U/A_1 \times \mathbb{Z}/p\cdot$$

We continue the process and set $A = V \cap U_1 \cap \cdots \cap U_k$ so

$$g : U/A \xrightarrow{\simeq} U/V \times U/U_1 \times \cdots \times U/U_k \simeq U/V \times (\mathbb{Z}/p)^k\cdot$$

For $i = 1, \cdots, k$, let $x_i \in U$ such that $U/U_i = \langle x_i U_i \rangle \simeq \mathbb{Z}/p$.

For $i = 1, \cdots, k$, let $\eta_i \in H^1(U/A)$ be defined by $\eta_i(x_j) = \delta_{i,j}$, and η_i is trivial on U/V. 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 2.1.
By Proposition 2.1, there exist $\chi_i \in H^1(\Gamma_K)$ for $i = 1, \cdots, k$ such that

(i) for every $\mathfrak{q} \in S$, $\eta_{i|\rho_\mathfrak{q}(\Gamma_p)} = \chi_{i|\Gamma_\mathfrak{q}}$;

(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, such that $v_p(N(\mathfrak{q}'_i) - 1) = m$.

(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 $K_2 := FM_1 \cdots M_k$. By (iii) and $(iv) - (v)$, one gets

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

Condition (i) above implies the two isomorphisms g and h respect 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 to $D_\mathfrak{q}(K_2/K)$ in $U/A \simeq Gal(K_2/K)$. Moreover, for the other ramified primes $\mathfrak{q}'_i$, one has $v_p(N(\mathfrak{q}'_i) - 1) = m$, 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 $S_2 := S \cup \{\mathfrak{q}'_1, \cdots, \mathfrak{q}'_k\}$. Moreover, 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 for the $\mathfrak{q}'_i$ (see Example 1.9).

As A is contained in the Frattini subgroup of U, the proof of the split case is done. Note that all the $\mathfrak{q}'_i$ are

We now proceed by induction when $1 \to V \to U \to U/V \to 1$ does not split.
• Let $H_2 \subset U^p[U,U]$ be normal in U and consider a sequence $H_n \subset H_2$, $n \geqslant 2$, of normal subgroups of U, such that $H_n/H_{n+1} \simeq \mathbb{Z}/p$ and $H_n = U$ for $n \gg 0$: this is always possible since U is a p-group.
Set $\Gamma = \Gamma_K$ or Γ_K^{ta}. Consider the embedding problem $(\mathscr{E}_n)$:

$$\begin{array}{ccccccc} & & & & & & \Gamma \\ & & & & & ?\rho_{n+1} \swarrow & \downarrow \rho_n \\ 1 & \longrightarrow & H_n/H_{n+1} & \longrightarrow & U/H_{n+1} & \xrightarrow[g_n]{} & U/H_n \end{array}$$

where g_n is the natural projection.

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 $Ш^2_{N_2} = 1$.

At each level U/H_n we want to:

(*i*) solve the *nonsplit* embedding problem $(\mathscr{E}_n)$;

(*ii*) adjust the solution by an element of H^1 (adding ramification at a new prime) 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.

– By construction and that $Ш_{N_2} = 0$, there is no obstruction to lift the decomposition group $D_\mathfrak{q}$ of $\mathfrak{q}$ in U/H_2 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 1.10.)
One can apply §1.3: there exists a $\mathbb{Z}/p$-extension of K_3/K_2, unramified outside N_2, Galois over K, solving the lifting problem $(\mathscr{E}_2)$ to U/H_3. That is (i) of the strategy.

– The problem now is that the decomposition group $D_\mathfrak{q}$ at $\mathfrak{q} \in N_2$ in K_3/K may be off the local plan and therefore it may not be liftable to U/H_4. If we are on all local plans in N_2, we proceed as we did previously to lift to U/H_4.
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 $(\mathscr{E}_\mathfrak{q})$, 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.
The quotient H_2/H_3 is generated by the image of an element $y \in U$ of order p^{m_0} with $m_0 \leqslant m$. We now use Proposition 1.7 to find a tame place $\mathfrak{q}_2$ such that for $R_2 = \{\mathfrak{q}_2\}$

$$(f_\mathfrak{q})_{\mathfrak{q} \in N_2} \in Im(\psi_{R_2}), \;\; v_p(N(\mathfrak{q}_2) - 1) = m,$$

and $\mathfrak{q}_2$ 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 $\mathfrak{q}_2$ splits completely in K_2/K, we are on the S-R local plan for $\mathfrak{q}_2$. Set $N_3 = N_2 \cup \{\mathfrak{q}_2\}$. We are on the local plan at all $\mathfrak{q} \in N_3$ and can proceed by induction.
As in the split case, all new primes of ramification are tame, so if $F \subset K^{ta}$, then $K_2 \subset K^{ta}$. □

3. Applications

3.1. **The main result.** In this section we prove:

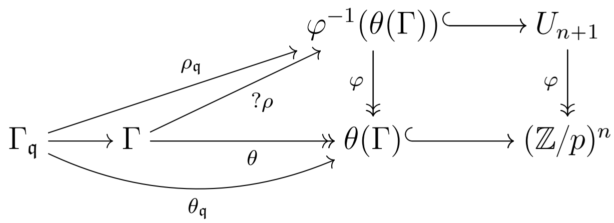
Theorem 3.1. *Let K be a number field and let p be a prime number such that $\zeta_p \notin K$. Let $n \geqslant 3$. Then the profinite groups Γ_K^{ta} and Γ_K satisfiy the strong n-fold Massey property (relative to p).*

Let $\chi_1, \cdots, \chi_n \in H^1(\Gamma)$, and set

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

Let $F := K(\theta) \subset \overline{K}$ be the fixed field the kernel of θ, that is intersection of the kernels $Ker(\chi_i)$. Note $K(\theta) \subset K^{ta}$. Set $G_0 = Gal(F/K)$. Then G_0 is isomorphic to $(\mathbb{Z}/p)^r$.
Finally, we remark that our proof does not explicitly use the cup product condition C_n. This property is invoked implicitly when we use that the local Galois groups $\Gamma_\mathfrak{q}$ satisfy the strong n-fold Massey property for $n \geqslant 3$.

Proof. 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 [16, Proposition 4.1] and [15, Theorem 4.3] Demushkin groups satisfy the strong n-fold Massey property for $n \geqslant 3$. The lifts of $\theta_{\mathfrak{q}}$ to homomorphisms $\rho_{\mathfrak{q}} : \Gamma_{\mathfrak{q}} \to U_{n+1}$ whose existence is guaranteed by [16] and [15] necessarily have image in $\varphi^{-1}(\theta(\Gamma)) \subset U_{n+1}$. These are the Massey local plans referred to at the end of §1.5.



We simply apply Theorem 2.2 with $U = \varphi^{-1}(\theta(\Gamma))$ and $U/V = \theta(\Gamma)$ 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. ☐

Remark 3.2. *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 1.8.*

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

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

The proof of Theorem 3.1 above is *not* explicit for the ramified primes of θ. The condition in C_n is also used only in the local results we cite from [16] and [15]. In this section we give another proof that is explicit 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 3.3. *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 characterstic and that $\zeta_p \in K_{\mathfrak{q}}$ one has

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

As $\mu_p \simeq \mathbb{Z}/p$ in $K_{\mathfrak{q}}$, the perfect local pairing becomes $H^1(\Gamma_{\mathfrak{q}}, \mathbb{Z}/p) \times H^1(\Gamma_{\mathfrak{q}}, \mathbb{Z}/p) \to H^2(\Gamma_{\mathfrak{q}}, \mathbb{Z}/p)$. That $\dim H^1(\Gamma_{\mathfrak{q}}) = 2$ gives that $\chi_{i,\mathfrak{q}}$ is its own annihilator under the local pairing. The result follows from the condition $\chi_{i,\mathfrak{q}} \cup \chi_{i+1,\mathfrak{q}} = 0$. ☐

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. If $\chi_{j,\mathfrak{q}} = \chi_{j+1,\mathfrak{q}} = \cdots = \chi_{j+k,\mathfrak{q}} = 0$ we simply take $\rho_{\mathfrak{q}}$ to be the trivial lift to U_{n+1} on this block.

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

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

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. E.g., starting with $\theta = (\chi_1, \chi_2, \chi_3)$ 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 $\gamma \in \{\sigma_{\mathfrak{q}}, \tau_{\mathfrak{q}}\}$:

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

We will show $\rho_{\mathfrak{q}}(\sigma_{\mathfrak{q}})$ and $\rho_{\mathfrak{q}}(\tau_{\mathfrak{q}})$ commute. From the definition of $\Lambda_{\mathfrak{q}}$ below, we have $\Lambda_{\mathfrak{q}}^n = 0$. Since $p > n$, ρ_q gives a representation of $\Gamma_{\mathfrak{q}}^{ab}$, the abelianization of $\Gamma_{\mathfrak{q}}$ which is our local plan. We now show the commutation result. Set

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

so

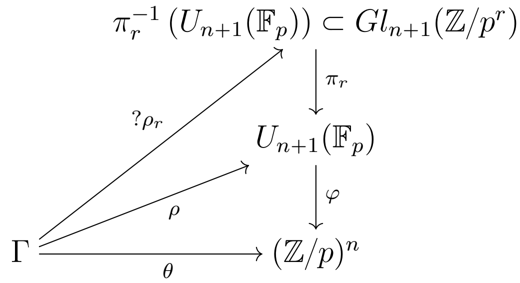
$$\begin{array}{rcl} \rho_{\mathfrak{q}}(\sigma_{\mathfrak{q}})\rho_{\mathfrak{q}}(\tau_q) & = & (I + \chi_{1,\mathfrak{q}}(\sigma_q)\Lambda_{\mathfrak{q}})\,(I + \chi_{1,\mathfrak{q}}(\tau_q)\Lambda_{\mathfrak{q}}) \\ & = & I + (\chi_{1,\mathfrak{q}}(\sigma_{\mathfrak{q}}) + \chi_{1,\mathfrak{q}}(\tau_{\mathfrak{q}}))\Lambda_{\mathfrak{q}} + \chi_{1,\mathfrak{q}}(\sigma_q)\chi_{1,\mathfrak{q}}(\tau_{\mathfrak{q}})\Lambda_{\mathfrak{q}}^2 \\ & = & I + (\chi_{1,\mathfrak{q}}(\tau_{\mathfrak{q}}) + \chi_{1,\mathfrak{q}}(\sigma_{\mathfrak{q}}))\Lambda_{\mathfrak{q}} + \chi_{1,\mathfrak{q}}(\tau_q)\chi_{1,\mathfrak{q}}(\sigma_{\mathfrak{q}})\Lambda_{\mathfrak{q}}^2 \\ & = & \rho_{\mathfrak{q}}(\tau_{\mathfrak{q}})\rho_{\mathfrak{q}}(\sigma_{\mathfrak{q}}). \end{array}$$

We have proved:

Corollary 3.4. *Let $n \geqslant 3$, $p > n$ and $\zeta_p \notin K$. Then the strong Massey 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.*

3.3. **More liftings.** Set $r \geqslant 1$. 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 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:



Here ρ is a lift given by Theorem 3.1. Since $Ker(\pi_r)$ is a p-group, we have $\rho_r(\Gamma)$ is also a p-group.

Theorem 3.5. *Take $\Gamma = \Gamma_K^{ta}$ or Γ_K, and suppose $\zeta_p \notin K$. For $n \geqslant 3$, let $\theta : \Gamma \to (\mathbb{Z}/p)^n$ satisfy C_n. Let ρ be given by Theorem 3.1, 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 $r \geqslant 1$, 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 [16, Proposition 4.1] and [15, 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 3.1 we realize a global lift $\rho : \Gamma \to U_{n+1}(\mathbb{F}_p)$ of θ whose restrictions to $\Gamma_\mathfrak{q}$ 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, 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 given by:

- Böckle [1, Theorem 1.3] for the tame primes ($\mathfrak{q} \nmid p$),
- Emerton and Gee [4, Theorem 6.4.4] for the wild primes ($\mathfrak{q}|p$).

In [1] and [4], 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 2.2 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] shows that there exist local lifts $\rho_{r,\mathfrak{q}}$ of $\rho_\mathfrak{q}$ in $Gl_{n+1}(\mathbb{Z}/p^r)$, that can be taken with image in $U_{n+1}(\mathbb{Z}/p^r)$, in the tame and wild setting. 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 2.2 with U, U/V, and the above local plans $\rho_{r,\mathfrak{q}}$. □

Remark 3.6. *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 3.7. *Observe that in the nondegenerate case, the group $\rho_r(\Gamma)$ contains $U_{n+1}(\mathbb{Z}/p^r)$.*

To conclude let us show why the condition "$\zeta_{p^r} \in K_\mathfrak{q}$" given in [2] is in a certain sense necessary.

Proposition 3.8. *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 $\rho_\mathfrak{q}$ in $U_{n+1}(\mathbb{Z}/p^r)$:*

$$\begin{array}{ccc} & & U_{n+1}(\mathbb{Z}/p^r) \\ & \overset{\rho_{\mathfrak{q},r}}{\nearrow} & \downarrow \pi_r \\ \Gamma_\mathfrak{q} & \xrightarrow[\rho_\mathfrak{q}]{} & U_{n+1} \end{array}$$

If a character θ_i on the near diagonal of U_{n+1} 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*, included in each other, 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. □

3.4. **Finite ramification sets.** 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.

3.4.1. *Free and Demushkin groups.* Let S_p be the set of p-adic primes of K. The pro-p group Γ_{S_p} can be free. But, as observed first by Shafarevich, Γ_{S_p} can be a free noncommutative pro-p group, for instance when p is regular, and $K = \mathbb{Q}(\zeta_p)$: in this case Γ_{S_p} is free on $(p+1)/2$ generators. When Γ_{S_p} is free, it obviously satisfies the strong n-fold Massey property for every $n \geqslant 2$. We state a Conjecture of Gras [7, Conjecture 7.11]:

Conjecture (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.*

There is another context for which Γ_{S_p} satisfies the strong n-fold Massey property for every $n \geqslant 3$: when Γ_{S_p} is Demushkin. This situation has been studied in [22], Section 3.

3.4.2. *Deep relations.* When $S \cap S_p = \varnothing$, the pro-p group Γ_S is FAB: every open subgroup has finite abelianization.
Observe first that Γ_S can be trivial. Indeed, take $K = \mathbb{Q}$, and $S = \varnothing$. It can also be cyclic of order p^m. Indeed, 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 property if and only if $n+1 \leqslant p^m$. 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).
There is the following general result of Vogel [20, Corollary 1.2.9]:

Theorem 3.9. *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 property for $2 \leqslant k \leqslant n$.*

Remark 3.10. *We use the terminology as in [21]. Let G be a pro-p group and $n \geqslant 2$ 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 stricly and uniquely defined and equal to 0, for $2 \leqslant k \leqslant n$.*
iii) *G satisfies the strong k-fold Massey vanishing property for $2 \leqslant k \leqslant n$.*
iv) *G satisfies the k-fold Massey vanishing property for $2 \leqslant k \leqslant n$.*

Proof. The implication from *i)* to *ii)* follows from [21, 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 $1 \leqslant i_1, i_2 \leqslant n$. By [21, Theorem A3], for every $f \in R$ and every $1 \leqslant i_1, i_2 \leqslant n$, $I = (i_1, i_2)$, 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 [21, Lemma 2.19], and hence $R \subseteq F_{(3)}$.
Now because $R \subseteq F_{(3)}$, we see that for all $1 \leqslant i_1, i_2, i_3 \leqslant n$, triple Massey products $\langle \chi_{i_1}, \chi_{i_2}, \chi_{i_3} \rangle$ are well defined, by [21, 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 [21, Theorem A3], for every $f \in R$ and every $1 \leqslant i_1, i_2, i_3 \leqslant n$, $I = (i_1, i_2, i_3)$, 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 $f \in R_{(4)}$ by [21, Lemma 2.19]. Hence $R \subseteq R_{(4)}$. Continuing in this way, we show that $R \subseteq F_{(k+1)}$ for all $2 \leqslant k \leqslant n$. In particular, $R \subseteq F_{(n+1)}$. ☐

To conclude, we give another situation where we can apply Theorem 3.9 . 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 3.11. *Take $n \geqslant 3$. Let K be a number field, not totally real, satisfying Gras's 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 property.*

Proof. We apply the strategy of [8]: 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 3.9. Chebotarev's theorem gives a positive density of such primes for our set T. ☐

References

[1] G. Böckle, *Lifting mod p representations to characteristics* p^2, J. Number Theory **101** (2003), no. 2, 310-337.

[2] A. Conti, C. Demarche, M. Florence, *Lifting Galois representations via Kummer flags*, 2024. http://arxiv.org/pdf/2403.08888.

[3] W. G. Dwyer, *Homology, Massey products and maps between groups*, J. Pure Appl. Algebra **6** (1975), n2, 177-190.

[4] M. Emerton, T. Gee, *Moduli stacks of étale* (φ, Γ)*-modules and the existence of crystalline lifts*, Annals of Math. Studies, 2023.

[5] P. Guillot, J. Mináč, A. Harpaz, *Four-fold Massey products in Galois cohomology*, With an appendix by Olivier Wittenberg, Compos. Math. **154** (2018), no.9, 1921–1959.

[6] G. Gras, Class Field Theory: from theory to practice, corr. 2nd ed., Springer Monographs in Mathematics, Springer (2005), xiii+507 pages.

[7] G. Gras, *Les* Θ*-régulateurs locaux d'un nombre algébrique : Conjectures* p*-adiques*, Canadian Journal of Mathematics **68** (2016), 571-624.

[8] F. Hajir, C. Maire, R. Ramakrishna, *Cutting towers of number fields*, Annales Mathématiques du Québec **45** (2021), 321-345.

[9] F. Hajir, M. Larsen, C. Maire, R. Ramakrishna, *On tamely ramified infinite Galois extensions*, 2024. https://arxiv.org/abs/2401.05927.

[10] Y. Harpaz, O. Wittenberg, *The Massey vanishing conjecture for number fields*, Duke Mathematical Journal **172** (2023), no. 1, 1-41.

[11] J. M. Hopkins, K. G. Wickelgren, *Splitting varieties for triple Massey products*, J. Pure Appl. Algebra **219** (2015), no. 5, 1304-1319.

[12] H. Koch, Galois Theory of p-Extensions, Springer-Verlag. Berlin, 2002.

[13] J.C. Lagarias, A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham (1975), Academic Press, London, 409-464.

[14] A. Merkurjev and F. Scavia, *Degenerate fourfold Massey products over arbitrary field*, J. Eur. Math. Soc. (JEMS), to appear. arXiv:2208.13011.

[15] J. Mináč, N.D. Tân, *Triple Massey product and Galois Theory*, J. Eur. Math. Soc. (JEMS) **19** (2017), no. 1, 255–284.

[16] J. Mináč, N.D. Tân, *Counting Galois* $U_4(\mathbb{F}_p)$*-extensions using Massey products*, J. Number Theory **176** (2017), 76-112.

[17] J. Neukirch, *On solvable number fields*, Invent. Math. 53 (1979), no. 2, 135-164.

[18] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of Number Fields, second edition, corrected second printing, GMW 323, Springer-Verlag Berlin Heidelberg, 2013.

[19] J.-P. Serre, Topics in Galois Theory, Research Notes in Mathematics 2nd Edition, A K Peters, Ltd., Wellesley, MA, 2008.

[20] D. Vogel, *Massey products in the Galois cohomology of number fields*, PhD Heidelberg, 2004.

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

[22] K. Wingberg, *Galois groups of local and global type*, J. Reine Angew. Math. **517** (1999), 223–239.

FEMTO-ST Institute, Université de Franche-Comté, CNRS, 15B avenue des Montboucons, 25000 Besançon, France
Email address: christian.maire@univ-fcomte.fr

Department of Mathematics, Western University, London, Ontario, N6A 5B7, Canada
Email address: minac@uwo.ca

Department of Mathematics, Cornell University, Ithaca, NY 14853-4201 USA
Email address: ravi@math.cornell.edu

Faculty Mathematics and Informatics, Hanoi University of Science and Technology, 1 Dai Co Viet Road, Hanoi, Vietnam
Email address: tan.nguyenduy@hust.edu.vn