ON TAMELY RAMIFIED INFINITE GALOIS EXTENSIONS

by

Farshid Hajir, Michael Larsen, Christian Maire, Ravi Ramakrishna

Abstract. — For a number field K, we consider K^{ta} the maximal tamely ramified algebraic extension of K, and its Galois group $G_K^{\mathrm{ta}} = \mathrm{Gal}(K^{\mathrm{ta}}/K)$. Choose a prime p such that $\mu_p \not\subset K$. Our guiding aim is to characterize the finitely generated pro-p quotients of G_K^{ta}. We give a unified point of view by introducing the notion of *stably inertially generated* pro-p groups G, for which linear groups are archetypes. This key notion is compatible with local *tame liftings* as used in the Scholz-Reichardt Theorem. We realize every finitely generated pro-p group G which is stably inertially generated as a quotient of G_K^{ta}. Further examples of groups that we realize as quotients of G_K^{ta} include congruence subgroups of special linear groups over $\mathbb{Z}_p[\![T_1, \cdots, T_n]\!]$. Finally, we give classes of groups which cannot be realized as quotients of $G_{\mathbb{Q}}^{\mathrm{ta}}$.

Let K a number field. Consider K^{ta}, the maximal tamely ramified algebraic extension of K. Let $G_K^{\mathrm{ta}} = \mathrm{Gal}(K^{\mathrm{ta}}/K)$. Choose a prime p. The maximal pro-p quotient of G_K^{ta} has an infinite number of generators. We are interested in the following question:

Question. — *What are the finitely generated pro-p quotients of* G_K^{ta}*?*

We make some first observations regarding these possible quotients.

– By a classical theorem of Scholz-Reichardt, for p odd, every finite p-group G is a quotient of $G_{\mathbb{Q}}^{\mathrm{ta}}$. See Serre [**22**, Chapter 2, §2.1] for a treatment which in fact generalizes their result. Shafarevich resolved the case of $p = 2$ by introducing the shrinking process; see also a recent work of Schmid [**21**].

– Recall that a pro-p group is called FAb if its open subgroups have finite abelianization. Finitely generated quotients of G_K^{ta} are FAb by class field theory.

– The previous constraint is related to the tame Fontaine-Mazur conjecture [**5**, Conjecture 5a] which implies that every finitely ramified p-adic analytic quotient of G_K^{ta} must

2000 ***Mathematics Subject Classification.*** — 11F80, 11R37, 11R32 .

Key words and phrases. — Tamely ramified extensions, pro-p groups, p-adic analytic groups.

The second author was partially supported by the National Science Foundation grant DMS-2001349. The third author was partially supported by the EIPHI Graduate School (ANR-17-EURE-0002). The fourth author was partially supported by Simons Collaboration grant #524863. He also thanks FEMTO-ST for its hospitality and wonderful research environment during his visit there in the spring of 2022. The first, third and fourth authors were supported by ICERM for a Research in Pairs visit in January, 2022 and by the Western Academy for Advanced Research (WAFAR) for a visit during the summer of 2023.

be finite. By finitely ramified we mean the set of ramification is finite, though the ramification index at a particular prime could be infinite. The only established case of the tame Fontaine-Mazur conjecture is that of 1-dimensional representations (which amounts to the FAb property of finite generated quotients of G_K^{ta}), and this is a good measure of both the importance and the difficulty of studying the finitely generated quotients of G_K^{ta}. Much of this difficulty lies in the subtleties of the tame Galois cohomology - in the wild analogue (where all primes above p are allowed to ramify), Poitou-Tate duality renders many of the calculations much more straightforward.

– In [**19**] surjective representations $G_{\mathbb{Q}} \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}_p)$ are constructed that are unramified at p provided the mod p reduction is unramified at p. These representations are almost certainly ramified at infinitely many tame primes as the Fontaine-Mazur conjecture predicts, though proving so definitively seems very difficult for even representations.

Choose p such that $\mu_p \not\subset K$, where μ_p denotes the pth roots of unity. We make this hypothesis to guarantee linear disjointness of various field extensions which in turn allows us to apply Chebotarev's theorem and successively resolve obstruction problems. See Proposition 1.4. When $\mu_p \subset K$, these issues are technically much more involved and it is not clear that for a fixed number field K, the statements we prove for large enough p always hold for p such that $\mu_p \subset K$. As μ_2 is in every number field, we require $p > 2$. Under the assumption that K does not contain a primitive pth root of unity, we use embedding techniques to characterize many finitely generated pro-p groups G that can be realized as quotients of G_K^{ta}. These constructions are explained below in Theorem A and its three corollaries C, D, and E. We also give classes of groups that are not quotients of G_K^{ta}; see Theorem E. To obtain these results, we give a unified point of view by introducing the notion of *stably inertially generated* pro-p groups G, for which linear groups are archetypes. This key notion has a certain compatibility with local *tame liftings* as used in the Scholz-Reichardt Theorem [**22**, Chapter 2, §2.1] extended by Neukirch [**16**].

The tame p-adic Lie Galois extensions which we construct have the further property that the set of primes that split completely is infinite. This phenomenon arises in the wild "finitely ramified case" when the p-adic Lie group is nilpotent as observed in [**8**], Proposition 4.1. In that situation the set of primes that split completely is related to the μ-invariant of the relevant p-adic Lie extension. Here we show that if one allows infinitely many ramified primes, then infinitely many primes can split completely for the groups $\mathrm{SL}_m^k(\mathbb{Z}_p)$ below. This result is similar to that of [**13**] where the characteristic polynomials of almost all Frobenius elements are arranged to have pure algebraic roots. It seems very difficult to achieve such results using only Galois cohomology without the infinite ramification hypothesis.

All generation statements in this paper refer to topological generators. We will always denote by G a finitely generated pro-p group. We call an element $y \neq 1$ of G *inertial* if there exists $x \in G$ such that

$$[x, y] = y^{\lambda}$$

for some $0 \neq \lambda \in \mathbb{Z}_p$. We say a pro-$p$ group G is *inertially generated* if it is generated by inertial elements. Indeed, this definition is motivated by the standard relation $[\sigma, \tau] = \tau^{q-1}$ for the Galois group over $\mathbb{Q}_q$ of its maximal pro-p extension when $q \cong 1 \bmod p$.

We say the pro-p group G is *stably inertially generated* if each group $P_n(G)$ of the p-central series $(P_n(G))_n$ of G is inertially generated. See §2.5 for the definitions and examples.

Our main theorem is:

Theorem A. — *Let G be a finitely generated pro-p group that is stably inertially generated. Then there exists a Galois extension L/K in K^{ta}/K such that* $\mathrm{Gal}(L/K) \cong G$. *Moreover L can be taken such that the set of primes of K that split completely in L is infinite.*

Let us say few words regarding our strategy, which is classical. We filter our pro-p group G with subgroups H_n such that

— $G/H_2 \cong (\mathbb{Z}/p)^d$ where d is the minimal number of generators of G and

— $H_n/H_{n+1} \cong \mathbb{Z}/p$ for $n \geqslant 2$.

We then construct $G_K^{\mathrm{ta}} \twoheadrightarrow G/H_2$ as the base case of our induction and inductively build compatible homomorphisms $G_K^{\mathrm{ta}} \twoheadrightarrow G/H_n$. Taking the limit solves the problem. It is easy to arrange that all obstructions are local, but then one needs to remove the local obstructions. At each stage of the induction we must allow ramification at another prime *and* make certain there is no local obstruction to lifting to the next step at this new prime. This requires a Galois cohomological argument and that G is stably inertially generated.

We say G is *torsion-generated* if it is generated by elements of finite order. We say it is *stably torsion-generated* if the subgroups $P_n(G)$ are torsion-generated for all $n \geqslant 1$.

Corollary B. — *Let G be a stably torsion-generated pro-p group. Then G can be realized as a quotient* $\mathrm{Gal}(L/K)$ *of G_K^{ta} and the extension L can be taken such that the set of primes of K that split completely in L is infinite.*

This corollary can be compared to Serre's pro-p version of the Scholz-Reichardt Theorem [**22**, Theorem 2.1.11]. The latter theorem does not require G to be finitely generated, but it assumes that G has finite exponent, so, in particular, its elements are all of finite order. By a famous result of Zelmanov, any finitely generated pro-p group G of finite exponent is itself finite, so the pro-p version of Scholz-Reichardt becomes the classical result in the finitely generated case.

Note that stably torsion-generated groups which have non-torsion elements exist. Consider the free group F_2 on two generators x and y. Let $\{a_i\}_{i=1}^{\infty}$ be an enumeration of the countably many elements of this group. Impose the relations $R = \{a_i^{p^{m_i}}\}$ with $m_i \to \infty$ in such a way that the Golod-Shafarevich power series is negative on $(0,1)$ (see Theorem 7.20 of [**14**]). This implies the pro-p completion H of $F_2/\langle R\rangle$ is infinite. Since the words of F_2 are dense in H, By a theorem of Zelmanov [**24**], H contains a free pro-p group as a subgroup and is therefore not torsion.

Assume $p > 2$. For a complete Noetherian local ring A with maximal ideal $\mathfrak{m}$ such that $A/\mathfrak{m} \cong \mathbb{F}_p$, and $k \geqslant 1$, set

$$\mathrm{SL}_m^k(A) := \ker\left(\mathrm{SL}_m(A) \to \mathrm{SL}_m(A/\mathfrak{m}^k)\right).$$

Then,

$$\mathrm{SL}_m^k(A)/\mathrm{SL}_m^{k+1}(A) \cong (\mathfrak{m}^k/\mathfrak{m}^{k+1}) \otimes_{\mathbb{Z}} M_m^0(\mathbb{Z}),$$

where $M_m^0(\mathbb{Z})$ denotes $m \times m$ integer matrices with trace 0. As A is Noetherian this is a finite dimensional vector space over $\mathbb{F}_p$, so

$$\widehat{\mathrm{SL}}_m^1(A) := \operatorname*{proj\,lim}_k \mathrm{SL}_m^1(A)/\mathrm{SL}_m^k(A)$$

is a pro-p group generated by any set of elements in $\mathrm{SL}_m^1(A)$ lifting an $\mathbb{F}_p$-basis of $\mathrm{SL}_m^1(A)/\mathrm{SL}_m^2(A) \cong (\mathfrak{m}/\mathfrak{m}^2) \otimes_{\mathbb{Z}} M_m^0(\mathbb{Z})$. The natural homomorphism $\mathrm{SL}_m^1(A) \to \widehat{SL}_m^1(A)$ is injective by the Krull intersection theorem and surjective by the completeness of A. Therefore, $\mathrm{SL}_m^k(A)$ is a finitely generated pro-p group for all k.

Corollary C. — *For $k, m, n \geqslant 1$, the groups $\mathrm{SL}_m^k(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!])$ are quotients of G_K^{ta}. In particular each $\mathrm{SL}_m^k(\mathbb{Z}_p)$ is a quotient of G_K^{ta}. Moreover these quotients can be chosen to correspond to a Galois extension L/K in which infinitely many primes split completely.*

This result is (in spirit) an extension of those of [**18**], and [**13**] for $\mathrm{SL}_2(\mathbb{Z}_p)$ and [**19**] for $\mathrm{SL}_2(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!])$.

The notion of stably inertially generated pro-p group is particularly well-adapted for p-adic Lie groups. To each p-adic analytic group G one can attach in a natural way a $\mathbb{Q}_p$-Lie algebra L_G [**15**], [**4**]; we recall this principle in §3.2. We focus on the case that L_G is simple. There are only two possibilities: L_G is pluperfect or toral. We say a Lie algebra L is *toral* if ad_x is semisimple for all $x \in L$, and it is *pluperfect* if it admits no non-trivial toral quotient algebra. See §3.3 for the definitions and further discussion of these concepts. Using Theorem A we prove:

Corollary D. — *Let G be a p-adic analytic group with pluperfect Lie algebra L_G. Then there exist homomorphisms $\rho : G_K^{\mathrm{ta}} \to G$ such that the image of ρ is open in G.*

In the other direction, by class field theory one knows that uniform abelian quotients of G_K^{ta} are trivial. See §3.1 for the definition of a uniform group. In fact uniform abelian groups are a special case of a more general family, uniform toral groups (the pro-p group is uniform and its Lie algebra is toral). Examples of uniform toral FAb groups are those whose Lie algebra is the set of trace zero elements of a skew field. See Section 3.5.

Theorem E. — *If the p-class field tower of K is finite then the pro-p group G_K^{ta} has no non-trivial uniform toral quotient. In particular, for a fixed K, the latter statement is true for all large enough primes p.*

Uniform toral groups are finitely generated. Given a number field K, one expects by Gras' conjecture [**6**] that the Galois group over K of its maximal pro-p extension unramified outside primes above p is free pro-p for p large enough. The number of generators would be $r_2(K)+1$ where $r_2(K)$ is the number of pairs of complex embeddings of K. The uniform toral FAb groups of Theorem E are quotients of such groups for large enough $r_2(K)$, so they provide (conjectural) examples of wildly ramified Galois groups that cannot arise as quotients of G_K^{ta}. The Fontaine-Mazur conjecture for tame extensions predicts Theorem E holds without the class field tower hypothesis.

In order to refine Corollary D consider the following context.

Let T be a (possibly infinite) set of primes of K, $K^{\mathrm{ta},T}/K$ be the maximal T-split extension of K in K^{ta}, and $G_K^{\mathrm{ta},T} = \mathrm{Gal}(K^{\mathrm{ta},T}/K)$.

Assuming the condition that $\mu_p \not\subset K$, all the previous results can be extended to $G_K^{\mathrm{ta},T}$ without difficulty.

Set

$$\alpha_T := \sum_{\mathfrak{q}\in T} \frac{\log N(\mathfrak{q})}{N(\mathfrak{q})-1} \text{ and } \alpha_T^{\mathrm{GRH}} := \sum_{\mathfrak{q}\in T} \frac{\log N(\mathfrak{q})}{\sqrt{N(\mathfrak{q})}-1},$$

where $N(\mathfrak{q}) := \#\mathscr{O}_K/\mathfrak{q}$.

For $v|\infty$ set

$$\alpha_\mathfrak{q} = \begin{cases} \frac{1}{2}(\gamma + \log 4\pi) & v \text{ is real} \\ \gamma + \log 2\pi & v \text{ is complex} \end{cases} \text{ and } \alpha_\mathfrak{q}^{\mathrm{GRH}} = \begin{cases} \frac{1}{2}(\frac{\pi}{2} + \gamma + \log 8\pi) & v \text{ is real} \\ \gamma + \log 8\pi & v \text{ is complex} \end{cases}$$

where γ is Euler's constant. Theorem F below, unlike Theorem E, requires no condition on the p-class field tower of K.

Theorem F. — *Let d_K to be the absolute discriminant of K.*
1) Take T such that $\alpha_T + \sum_{v|\infty} \alpha_\mathfrak{q} > \log\sqrt{|d_K|}$. Then $G_K^{\mathrm{ta},T}$ has no non-trivial uniform toral quotient.
2) Assume the GRH and T such that $\alpha_T^{\mathrm{GRH}} + \sum_{v|\infty} \alpha_\mathfrak{q}^{\mathrm{GRH}} > \log\sqrt{|d_K|}$. Then $G_K^{\mathrm{ta},T}$ has no non-trivial uniform toral quotient.

In § 1 we establish the Galois cohomological machinery we need, Proposition 1.4 being the important technical result. In § 2 we perform the inductive lifting process, making key use of Definition 2.6 to prove Theorem A. In § 3 we establish results on p-adic Lie algebras and classes of pro-p groups that allow us to obtain the rest of our results.

Notations. Throughout this article $p > 2$ is an odd prime number and G is a finitely generated pro-p group.

- Set $G^{ab} := G/\overline{[G,G]}$, $G^{p,el} := G^{ab}/(G^{ab})^p$, and $d(G) := \dim G^{p,el}$.
- Let $(P_n(G))$ be the p-central series of G: $P_1(G) = G$ and for $n \geqslant 1$, $P_{n+1}(G) = \overline{P_n(G)^p[G, P_n(G)]}$. The sequence $(P_n(G))$ forms a basis of open normal subgroups of G.
- All cohomology groups have coefficients in $\mathbb{Z}/p$ with trivial action so we write $H^i(G)$ for $H^i(G, \mathbb{Z}/p)$.
- K is a number field with $\mu_p \not\subset K$ and K^{ta} is the maximal tamely ramified extension of K and $G_K^{\mathrm{ta}} = \mathrm{Gal}(K^{\mathrm{ta}}/K)$.
- For a prime $\mathfrak{q}$ of K we denote the cardinality of $\mathscr{O}_K/\mathfrak{q}$ by $N(\mathfrak{q})$.
- For a finite set of primes S of residue characteristic different from p, set K_S to be the maximal pro-p extension of K unramified outside S and $G_S = \mathrm{Gal}(K_S/K)$.
- $K_\mathfrak{q}$ is the completion of K at the prime $\mathfrak{q}$, $G_\mathfrak{q} := \mathrm{Gal}(\overline{K}_\mathfrak{q}/K_\mathfrak{q})$ and $U_\mathfrak{q}$ is the group of units of $K_\mathfrak{q}$. We let $\sigma_\mathfrak{q}$ and τ_q be, respectively, a Frobenius element and a generator of inertia in the Galois group of the maximal pro-p extension of $K_\mathfrak{q}$.
- J is the idele group of K. The subgroup $U = \prod_\mathfrak{q} U_\mathfrak{q} \subset J$ are those ideles that are locally units everywhere and $U_S \subset U$ are those ideles in U that are 1 at every $\mathfrak{q} \in S$.
- $V_S := \{x \in K^\times | x \in K_\mathfrak{q}^{\times p},\ \forall \mathfrak{q} \in S; x \in U_\mathfrak{q} K_\mathfrak{q}^{\times p}\ \forall \mathfrak{q}\}$ and $Б_S = (V_S/K^{\times p})^\wedge$ is called the Selmer group.
- For $S \supseteq T$, set $V_T^S = \{x \in K^\times \mid\ x \in K_\mathfrak{q}^{\times p}\ \forall\ \mathfrak{q} \in T \text{ and } x \in U_\mathfrak{q} K_\mathfrak{q}^{\times p}\ \forall\ \mathfrak{q} \notin S\}$ and $Б_T^S = (V_T^S/K^{\times p})^\wedge$.

1. The local-global principle

1.1. The Shafarevich and Selmer groups. — Let Z be a finite set of tame primes and recall G_Z is the Galois group of the maximal extension of K unramified outside primes above Z. We will analyze our obstructions in group cohomology via the exact restriction sequence

$$0 \to Ш_Z^2 \to H^2(G_Z) \xrightarrow{\mathrm{Res}_Z} \prod_{\mathfrak{q}\in Z} H^2(G_{\mathfrak{q}}) \tag{1}$$

where $Ш_Z^2$ is defined as the kernel of the restriction map Res_Z. The groups V_Z and $Б_Z$ from the Notations are crucial to the study of G_Z. We record two important results (parts (i) and (iv)) and several basic facts about these groups.

Lemma 1.1. — *Let K be a number field. Then*
(i) $Ш_S^2 \hookrightarrow Б_S$.
(ii) $S_1 \subset S_2 \implies V_{S_2} \subseteq V_{S_1}$.
(iii) Let U_K be the units of the number field K and $Cl_K[p]$ be the p-torsion of the class group of K. There is an exact sequence

$$1 \to U_K/U_K^p \to V_\varnothing/K^{\times p} \to Cl_K[p] \to 1.$$

As $\mu_p \not\subset K$ we have $\dim Б_{K,\varnothing} = r_1(K) + r_2(K) - 1 + \dim Cl_K[p]$.
(iv) There is a finite set Z_0 of $\dim Б_{K,\varnothing}$ *tame primes such that* $Б_{Z_0} = 0$ *so* $Ш_S^2 = 0$ *for any* $S \supseteq Z_0$.
(v) For $S \supseteq T$, $V_T^{S\cup T} \subseteq V_\varnothing^S$.
(vi) $V_T = U_T J^p \cap K^\times$ *so* $V_T/K^{\times p} = (U_T J^p \cap K^\times)/K^{\times p} \cong (U_T J^p \cap J^p K^\times)/J^p$.
(vii) $V_T^S = (U_T J^p \prod_{\mathfrak{q}\in S\setminus T} K_{\mathfrak{q}}^\times) \cap K^\times$ *so* $V_T^S/K^{\times p} = (U_T J^p \prod_{\mathfrak{q}\in S\setminus T} K_{\mathfrak{q}}^\times \cap J^p K^\times)/J^p$.

Proof. — (i) See [**14**, Chapter 11, Theorem 11.3].
(ii) This is immediate from the definition.
(iii) One can alternatively define $V_\varnothing = \{\alpha \in K^\times | (\alpha) = I^p\}$. Let I be an ideal representing a class of C of $CL_K[p]$ so $I^p = (\alpha)$. The map $\alpha \mapsto C$ is surjective and one easily sees the kernel is U_K/U_K^p.
(iv) This is consequence of the finiteness of $Б_{K,\varnothing}$: see for example Theorem 1.12 of [**10**].
(v), (vi) and (vii) These are immediate from the definitions. □

Remark 1.2. — It is worth remarking the injection (i) above is an isomorphism if S contains all primes above p. The failure of this map to be surjective in the tame setting can be thought of as the reason tame Galois cohomology is difficult.

1.2. Global cohomology classes with given local conditions. —

1.2.1. — Proposition 1.3 below is Proposition 10.7.9 of [**17**]. The proof in [**17**] invokes previous results from that text using Poitou-Tate duality. We give a proof more in the spirit of §11.3 of [**14**], using only class field theory.

Proposition 1.3. — *Let $S \supseteq T$ be finite sets of primes. There is an exact sequence*

$$0 \to H^1(G_S^T, \mathbb{Z}/p) \to H^1(G_S, \mathbb{Z}/p) \to \prod_{\mathfrak{q}\in T} H^1(G_{\mathfrak{q}}, \mathbb{Z}/p) \to Б_{S\setminus T}^S \to Б_S \to 0$$

where G_S is the Galois group of the maximal extension of K unramified outside S and G_S^T is the Galois group of the maximal extension of K unramified outside S split completely at T.

Proof. — Recall $U_X \subset J$ are those ideles that are 1 at $\mathfrak{q} \in X$ and units at $\mathfrak{q} \notin X$. Consider the sequence

$$0 \to \frac{U_S J^p \cap J^p K^\times}{J^p} \xrightarrow{\psi_1} \frac{(U_{S\backslash T} J^p \prod_{\mathfrak{q}\in T} K_{\mathfrak{q}}^\times) \cap J^p K^\times}{J^p} \xrightarrow{\psi_2} \prod_{\mathfrak{q}\in T} \frac{K_{\mathfrak{q}}^\times}{K_{\mathfrak{q}}^{\times p}}$$
$$\xrightarrow{\psi_3} \frac{J}{U_S J^p K^\times} \xrightarrow{\psi_4} \frac{J}{(U_S J^p \prod_{\mathfrak{q}\in T} K_{\mathfrak{q}}^\times) K^\times} \to 0$$

where ψ_1 is the natural inclusion, ψ_2 is the projection to the T-coordinates, ψ_3 is extension from T-coordinates to the ideles by including the component 1 at all $\mathfrak{q} \notin T$ and taking the quotient by $U_S J^p K^\times$, and ψ_4 is the natural projection. We will prove this sequence is exact and dualizing will give the result.

Exactness at the first, fourth and fifth terms is clear. We now show the sequence is a complex. That $\psi_2 \circ \psi_1$ is trivial follows from the fact that, since $S \supseteq T$, it is trivial on $U_S J^p$. We show $\psi_3 \circ \psi_2$ is trivial. Let $u_{S\backslash T} j_1^p t \in (U_{S\backslash T} J^p \prod_{\mathfrak{q}\in T} K_{\mathfrak{q}}^\times) \cap J^p K^\times$ so we can write $u_{S\backslash T} j_1^p t = j_2^p \gamma$ where $\gamma \in K^\times$ and thus $u_{S\backslash T} j^p t = \gamma \in K^\times$ where $j = j_1/j_2$. Up to pth powers of ideles, we see γ is a unit outside of S, a pth power at $S\backslash T$ and

$$\psi_3(\psi_2(u_{S\backslash T} j_1^p t)) = \psi_3(\psi_2(u_{S\backslash T} j^p t)) = \psi_3(\psi_2(\gamma))$$

which has component γ at $\mathfrak{q} \in T$ and 1 elsewhere. Let $\tilde{u}_S$ be the idele with component 1 at $\mathfrak{q} \in S$ and γ elsewhere. As γ is, up to pth powers, a unit outside of S we see $\tilde{u}_S \in U_S J^p$ and $\gamma^{-1} \tilde{u}_S \psi_3(\psi_2(\gamma))$ has component γ^{-1} at $\mathfrak{q} \in S\backslash T$ and 1 elsewhere. As γ^{-1} is a pth power at $S\backslash T$, we have, in $J/(U_S J^p) K^\times$,

$$\psi_3(\psi_2(u_{S\backslash T} j_1^p t)) = \psi_3(\psi_2(\gamma)) = \gamma^{-1} \tilde{u}_S \psi_3(\psi_2(\gamma)) \in J^p$$

so $\psi_3 \circ \psi_2$ is trivial and the sequence is a complex.

For exactness at the second term, consider $x \in \ker(\psi_2)$. We immediately see x is a pth power at all primes of T and since $x \in U_{S\backslash T} J^p \prod_{\mathfrak{q}\in T} K_{\mathfrak{q}}^\times$ it is a pth power at all primes of $S\backslash T$, so x is a pth power at all primes of S, and away from S, up to pth powers, it is a unit. Thus $x \in U_S J^p$. By hypothesis $x \in J^p K^\times$ so $x \in \operatorname{im}(\psi_1)$.

We now check exactness at the third term. Let $x \in \ker(\psi_3)$. Then $\psi_3(x) = u_S j^p \gamma$ where $u_S \in U_S$, j is an idele and $\gamma \in K^\times$. As ψ_3 is 'extension from T to the ideles by 1', we see that for $\mathfrak{q} \in S\backslash T$, the $\mathfrak{q}$-component of $u_S j^p \gamma$ is 1. As u_S has component 1 at $\mathfrak{q} \in S$ and is a unit outside of S, we see $j^p \gamma$ has $\mathfrak{q}$-component 1 at $\mathfrak{q} \in S\backslash T$ and is a unit outside of S. This implies

$$j^p \gamma \in (U_{S\backslash T} \prod_{\mathfrak{q}\in T} K_{\mathfrak{q}}^\times) \cap J^p K^\times \subseteq (U_{S\backslash T} J^p \prod_{\mathfrak{q}\in T} K_{\mathfrak{q}}^\times) \cap J^p K^\times$$

and $\psi_2(j^p \gamma)$ has the same T-components as x so $x \in \operatorname{im}(\psi_2)$ as desired. The sequence at the beginning of the proof is exact.

Recall that for a group G, we write $G^{p,el}$ for its maximal abelian quotient that is a vector space over $\mathbb{F}_p$. Using Lemma 1.1 (*vi*) with T replaced by S gives the first term of (2) below. The second term comes from Lemma 1.1 (*vii*) with S playing the same role and T there replaced by $S\backslash T$ here. The fourth and fifth terms come from the global Artin map.

$$0 \to \frac{V_S}{K^{\times p}} \to \frac{V_{S\backslash T}^S}{K^{\times p}} \to \prod_{\mathfrak{q}\in T} \frac{K_{\mathfrak{q}}^\times}{K_{\mathfrak{q}}^{\times p}} \to G_S^{p,el} \to (G_S^T)^{p,el} \to 0. \tag{2}$$

Dualizing and using the local Artin map for the third term completes the proof. □

1.2.2. — We will use Proposition 1.3 to control the image of $\text{Res}_{N,R} : H^1(G_{N\cup R}) \to \prod_{\mathfrak{q}\in N} H^1(G_\mathfrak{q})$ when $R = \{\tilde{\mathfrak{q}}\}$. The hypothesis $\mu_p \not\subset K$ is crucial for linear disjointness of various field extensions of K.

Proposition 1.4. — *Let N be a fixed finite set of tame primes with $K \subseteq L \subseteq K_N$ and let $(f_\mathfrak{q}) \in \prod\limits_{\mathfrak{q}\in N} H^1(G_\mathfrak{q}, \mathbb{Z}/p)$. Assume $(f_\mathfrak{q})$ is not in the image of the restriction map $H^1(G_N) \to \prod_{\mathfrak{q}\in N} H^1(G_\mathfrak{q})$. Then there exist infinitely many finite primes $\tilde{\mathfrak{q}}$ such that $(f_\mathfrak{q}) \in Im(\text{Res}_{N,\{\tilde{\mathfrak{q}}\}})$. Moreover, the primes $\tilde{\mathfrak{q}}$ can be chosen such that*

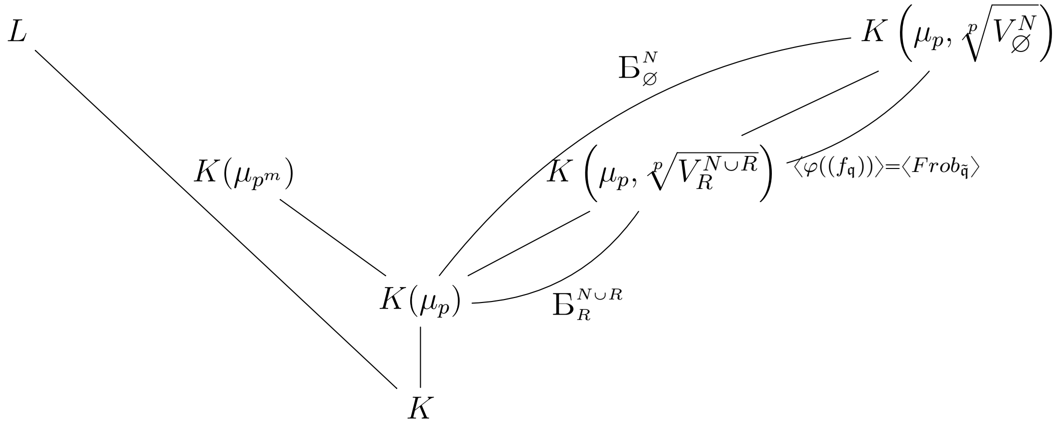
(i) $\tilde{\mathfrak{q}}$ splits completely in L/K,

(ii) the p-adic valuation of $N(\tilde{\mathfrak{q}}) - 1$ is larger than some given integer m.

Proof. — Recall first the following commutative diagram obtained from applying Proposition 1.3 with $(S,T) = (N,N)$ and $(S,T) = (N \cup R, N)$. The first two vertical maps are inflation maps and thus injective. The third map is the identity. The fourth and fifth maps are duals of natural inclusions of Lemma 1.1 (v) and (ii).

$$\begin{tikzcd}
0 \arrow[r] & H^1(G_N^N) \arrow[r, "\text{Inf}"] \arrow[d] & H^1(G_N) \arrow[r, "\text{Res}_N"] \arrow[d] & \prod_{\mathfrak{q}\in N} H^1(G_\mathfrak{q}) \arrow[r, "\varphi"] \arrow[d] & Б_\varnothing^N \arrow[r] \arrow[d] & Б_N \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H^1(G_{N\cup R}^N) \arrow[r, "\text{Inf}"] & H^1(G_{N\cup R}) \arrow[r, "\text{Res}_{N,R}"] & \prod_{\mathfrak{q}\in N} H^1(G_\mathfrak{q}) \arrow[r, "\varphi_R"] & Б_R^{N\cup R} \arrow[r] & Б_{N\cup R} \arrow[r] & 0
\end{tikzcd}$$

By Lemma 1.1, $V_R^{N\cup R} \subset V_\varnothing^N$ and we have the field diagram below with three of the Galois groups indicated.


L
$K\left(\mu_p, \sqrt[p]{V_\varnothing^N}\right)$
$Б_\varnothing^N$
$K(\mu_{p^m})$
$K\left(\mu_p, \sqrt[p]{V_R^{N\cup R}}\right)$
$\langle\varphi((f_\mathfrak{q}))\rangle = \langle Frob_{\tilde{\mathfrak{q}}}\rangle$
$K(\mu_p)$
$Б_R^{N\cup R}$
K

We are supposing $(f_\mathfrak{q}) \in \prod_{\mathfrak{q}\in N} H^1(G_\mathfrak{q})$ is not in the image of Res_N. Then $\varphi((f_\mathfrak{q})) \neq 0$ and $(f_\mathfrak{q})$ is in the image of $\text{Res}_{N,R} \iff \varphi_R((f_\mathfrak{q})) = 0$, namely $(f_\mathfrak{q}) \mapsto 0$ under the fourth vertical map.

For $\alpha \in V_\varnothing^N$ and $\tilde{\mathfrak{q}} \notin N$ and of characteristic different from p, we have $\alpha \in U_{\tilde{\mathfrak{q}}} K_{\tilde{\mathfrak{q}}}^{\times p}$ so $K\left(\mu_p, \sqrt[p]{V_\varnothing^N}\right)/K(\mu_p)$ is unramified at such a $\tilde{\mathfrak{q}}$. Using Chebotarev's Theorem, choose a prime $\tilde{\mathfrak{q}}$ whose Frobenius in $Б_\varnothing^N = Gal\left(K\left(\mu_p, \sqrt[p]{V_\varnothing^N}\right)/K(\mu_p)\right)$ spans the same non-trivial line as $\varphi((f_\mathfrak{q})) \in Б_\varnothing^N$. It is not hard to show to show all primes of $K(\mu_p)$ above

$\tilde{\mathfrak{q}}$ have Frobenius elements in $Gal\left(K\left(\mu_p, \sqrt[p]{V_{\varnothing}^N}\right)/K(\mu_p)\right)$ that are nonzero scalar multiples of one another, so the choice is irrelevant. Taking $R = \{\tilde{\mathfrak{q}}\}$, we see $\alpha \in V_R^{N\cup R}$ is locally a pth power at $\tilde{\mathfrak{q}}$ so $K\left(\mu_p, \sqrt[p]{V_R^{N\cup R}}\right)/K(\mu_p)$ is the maximal sub-extension of $K\left(\mu_p, \sqrt[p]{V_{\varnothing}^N}\right)/K(\mu_p)$ in which $\tilde{\mathfrak{q}}$ splits completely so $\varphi_R((f_{\mathfrak{q}})) = 0$ as desired.

Since $\mu_p \not\subset K$ and $V_{\varnothing}^N \subset K$, $Gal\left(K\left(\mu_p, \sqrt[p]{V_{\varnothing}^N}\right)/K(\mu_p)\right)$ is in the (necessarily nontrivial) ω-component under the action of $\mathrm{Gal}(K(\mu_p)/K))$, where ω is the cyclotomic character. As $\mathrm{Gal}(L(\mu_{p^m})/K(\mu_p))$ is in the trivial eigenspace, $L(\mu_{p^m})$ and $K\left(\mu_p, \sqrt[p]{V_{\varnothing}^N}\right)$ are linearly disjoint over $K(\mu_p)$ and we can choose $\tilde{\mathfrak{q}}$ to satisfy (i) and (ii). □

Remark 1.5. — Proposition 1.4 is reminiscent of Proposition 3.4 of [**19**], though that result invokes Poitou-Tate duality.

2. Realization of quotients of G_K^{ta}

Let G be a finitely generated pro-p group. Let $d := d(G) := \dim H^1(G)$ denote the generator rank of G, that is, the minimum size of a generating set of G.

We will realize groups G as quotients of G_K^{ta} by induction. To do this we need a sequence of normal open subgroups $(H_n)_{n\geqslant 2}$ of G such that:

(i) $H_2 = [G,G]G^p$, and $\bigcap_n H_n = 1$;

(ii) for every $n \geqslant 2$, the quotient H_n/H_{n+1} is isomorphic to $\mathbb{Z}/p$, and is generated by the image of an *inertial element* y_n of H_n. Also see Definition 2.6.

2.1. The first step of the inductive process.

— We will solve the main problem of this paper by induction. Proposition 2.2 below is the base case. Its proof uses the following result of Gras [**7**], Chapter V, Theorem 2.4:

Lemma 2.1. — *Let K be a number field, T a finite set of primes of K, and $\mathfrak{q} \notin T$ a prime ideal of K. There exists a $\mathbb{Z}/p$-extension L/K ramified at exactly $\mathfrak{q}$ (i.e. it is ramified at $\mathfrak{q}$ and at no other prime) and such that a finite set of primes T splits completely in L if and only if $\mathfrak{q}$ splits completely in $K\left(\mu_p, \sqrt[p]{V_{\varnothing}^T}\right)/K$.*

This lemma allows us to prove the base case of the induction that will be the proof of Theorem 2.14 which is also Theorem A.

Proposition 2.2. — *Let K be a number field. There exists an elementary abelian p-extension L/K with $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/p)^d$ ramified at $\{\mathfrak{q}_1, \ldots \mathfrak{q}_d\}$ such that $D_{\mathfrak{q}_i} \cong \mathbb{Z}/p$, where $D_{\mathfrak{q}_i}$ is the decomposition group of $\mathfrak{q}_i$ in L/K. One can also choose the $\mathfrak{q}_i$ such that the p-adic valuation of $N(\mathfrak{q}_i) - 1$ is larger than some given integer n_i, for each i.*

Proof. — We want an extension L/K with $\mathrm{Gal}(L/K) \cong G \cong (\mathbb{Z}/p)^d$ where the primes $\mathfrak{q}_i$ that ramify have no residue field extension. This argument is a variant of the split case of the Theorem of Scholz-Reichardt and uses the governing extension $K\left(\mu_p, \sqrt[p]{V_{\varnothing}^T}\right)/K$ of Lemma 2.1. For any $n_1 \geqslant 1$, we first use Chebotarev's theorem to choose $\mathfrak{q}_1$ of K that splits completely in $K\left(\mu_{p^{n_1}}, \sqrt[p]{V_{\varnothing}}\right)/K$.

By Lemma 2.1, we see there is a $\mathbb{Z}/p$-extension L_1/K ramified at exactly $\mathfrak{q}_1$.

Now set $T = \{\mathfrak{q}_1\}$. Assume $n_2 \geqslant 1$ is given and apply Lemma 2.1 with the additional requirements that $\mathfrak{q}_2$ splits completely in L_1/K and $K(\mu_{p^{n_2}})/K$. Then there is a $\mathbb{Z}/p$-extension L_2/K ramified at exactly $\mathfrak{q}_2$ in which $\mathfrak{q}_1$ splits. As $\mathfrak{q}_2$ splits in L_1/K, we see both $\mathfrak{q}_1$ and $\mathfrak{q}_2$ have decomposition group $\mathbb{Z}/p$ in $\mathrm{Gal}(L_1L_2/K) \cong (\mathbb{Z}/p)^2$.

Now set $T = \{\mathfrak{q}_1, \mathfrak{q}_2\}$ and use Lemma 2.1 to find a $\mathfrak{q}_3$ that also splits completely in L_1L_2/K and $K(\mu_{p^{n_3}})/K$. Continuing in this fashion, set $L = L_1L_2 \cdots L_d$ to obtain the result. □

2.2. The embedding problem. — Let G be a finitely generated pro-p group filtered by a sequence of normal subgroups $G^p[G,G] = H_2 \supset H_3 \supset \cdots$ of G such that for $n \geqslant 2$, $H_n/H_{n+1} \cong \mathbb{Z}/p$.

Consider the central extension

$$1 \to H_n/H_{n+1} \to G/H_{n+1} \overset{g_n}{\to} G/H_n \to 1,$$

where g_n is the natural map and $H_n/H_{n+1} \cong \mathbb{Z}/p$ so the p-group G/H_n acts trivially on H_n/H_{n+1}. Since $H_2 = G^p[G,G]$, the Frattini subgroup of G, we have for $n \geqslant 2$,

$$d(G) = d(G/H_n) = d(G/H_{n+1}),$$

where d denotes the minimal number of generators. This implies the group extension is not split.

Let Γ be a pro-p group, and for some $n \geqslant 2$, let $f_n : \Gamma \twoheadrightarrow G/H_n$ be a surjective homomorphism and consider the embedding problem:

$$\begin{tikzcd}
 & & & \Gamma \arrow[dl, dotted, "?\rho_{n+1}"'] \arrow[d, two heads, "\rho_n"] & \\
1 \arrow[r] & H_n/H_{n+1} \arrow[r] & G/H_{n+1} \arrow[r, two heads, "g_n"'] & G/H_n & (\mathscr{E}_n)
\end{tikzcd}$$

As $G/H_{n+1} \to G/H_n$ is not split, the homomorphism ρ_{n+1} is surjective if it exists.

The embedding problem is controlled by $H^2(\Gamma) := H^2(\Gamma, \mathbb{Z}/p)$. Let ε_n be the element in $H^2(G/H_n)$ corresponding to the group extension:

$$1 \longrightarrow H_n/H_{n+1} = \mathbb{Z}/p \longrightarrow G/H_{n+1} \longrightarrow G/H_n \longrightarrow 1. \tag{3}$$

As $d = d(G/H_n) = d(G/H_{n+1})$ we see $\varepsilon_n \neq 0$, that is the exact sequence (3) does not split.

Let us recall:

Theorem 2.3. — *Let* $\mathrm{Inf} : H^2(G/H_n) \to H^2(\Gamma)$ *be the inflation map. The embedding problem* $(\mathscr{E}_n)$ *has a solution if and only if* $\mathrm{Inf}(\varepsilon_n) = 0$. *Moreover, since* $n \geqslant 2$, *any solution is always proper, that is* ρ_{n+1} *is surjective. The set of solutions (modulo equivalence) of* $(\mathscr{E}_n)$ *is a principal homogeneous space over* $H^1(\Gamma)$.

Proof. — Proposition 3.5.9 and 3.5.11 of [**17**]. □

2.3. The strategy. — Given $n \geqslant 2$, let K_n/K be a Galois extension in K^{ta} such that $\mathrm{Gal}(K_n/K) \cong G/H_n$. Set $\Gamma_n = \mathrm{Gal}(K_n/K)$.

Let S_n be the finite set of tame primes ramified in L_n/K. Recall K_{S_n} is the maximal extension of K unramified outside S_n and $G_{S_n} = \mathrm{Gal}(K_{S_n}/K)$. Observe that $L_n \subset K_{S_n}$. We assume S_n contains Z_0 as in Lemma 1.1, *(iv)* so $\text{Ш}^2_{S_n} = 0$.

By Theorem 2.3 applied to $\Gamma := G_{S_n}$, we note that if there is no local obstruction at any $\mathfrak{q} \in S_n$ to lifting G/H_n to G/H_{n+1}, then the embedding problem $(\mathscr{E}_n)$ has a solution in K_{S_n}/K.

The question is then: *How do we create a situation for which there is no local obstruction for every quotient of G?*

Our strategy is as follows: By Proposition 2.2 there is a map $G_{S_2} \twoheadrightarrow G/P_2(G)$ ramified at $\{\mathfrak{q}_1, \dots, \mathfrak{q}_d\}$. As $S_2 = \{\mathfrak{q}_1, \dots, \mathfrak{q}_d\} \cup Z_0$, we see $\text{Ш}^2_{S_2} = 0$ by Lemma 1.1 (iv). We will later show for each $\mathfrak{q} \in S_2$ there are lifts of $G_{\mathfrak{q}} \to G_{S_2} \twoheadrightarrow G/P_2(G)$ to $G_{\mathfrak{q}} \to G$ so Theorem 2.3 and (1) give a solution to $(\mathscr{E}_2)$. We then use the H^1 group (and the principal homogenous space property, see Theorem 2.3) to obtain a new solution for $(\mathscr{E}_2)$ with no obstructions for $(\mathscr{E}_3)$ at $\mathfrak{q} \in S_2$. This requires introducing ramification at a new prime $\tilde{\mathfrak{q}}$ in such a manner that $G_{\tilde{\mathfrak{q}}} \to G/H_2$ can be lifted to $G_{\tilde{\mathfrak{q}}} \to G$. Thus there is no local obstruction to $(\mathscr{E}_3)$ at $\tilde{\mathfrak{q}}$ as well so a solution exists and we can repeat the process. For this, we use Proposition 1.4 with the fields K_n here playing the role of L there.

2.4. Lifting local homomorphisms. — We retain the notations of the previous sections. In particular, we suppose given a sub-extension K_n/K of K_{S_n}/K, with Galois group $\Gamma_n \cong G/H_n$.

Recall we have the exact sequence

$$0 \to \text{Ш}^2_{S_n} \to H^2(G_{S_n}) \to \oplus_{\mathfrak{q} \in S_n} H^2(G_{\mathfrak{q}})$$

where $S_n \supseteq Z_0$ of Lemma 1.1 (iv) so $\text{Ш}^2_{S_n} = 0$. Thus the embedding problem $(\mathscr{E}_n)$ has a solution exactly when it has a local solution for every $\mathfrak{q} \in S_n$. The question is then reduced to the lifting problem of *ramified quotients in G* of tame local groups.

Recall that all tame primes we consider satisfy $N(\mathfrak{q}) \equiv 1 \bmod p$. For these $\mathfrak{q}$ the pro-p completion of $G_{\mathfrak{q}}$ is $\mathbb{Z}_p \rtimes \mathbb{Z}_p$. In this pro-$p$ completion, let $\tau_{\mathfrak{q}} \in G_{\mathfrak{q}}$ be a generator of the inertia, and $\sigma_{\mathfrak{q}}$ be the Frobenius. They satisfy the unique relation $[\sigma_{\mathfrak{q}}, \tau_{\mathfrak{q}}] = \tau_{\mathfrak{q}}^{N(\mathfrak{q})-1}$. See [**14**, §10.1].

For each $\mathfrak{q}$ in our set of primes which may be ramified, we will give a *local plan*, that is a homomorphism $\rho_{\mathfrak{q}} : G_{\mathfrak{q}} \to G$ lifting $\rho_{\mathfrak{q},n} : G_{\mathfrak{q}} \to G/H_n$.

$$\begin{tikzcd}
& G_{\mathfrak{q}} \arrow[ld, dotted, "?\rho_{\mathfrak{q}}"'] \arrow[d, "\rho_{\mathfrak{q},n}"] \\
G \arrow[r, two heads] & G/H_n
\end{tikzcd}$$

For $\mathfrak{q} \in Z_0$ we choose the local plan to be any unramified map from $G_{\mathfrak{q}} \to G$ lifting the image of $\sigma_{\mathfrak{q}} \in G/H_n$ to an element of G. The existence follows immediately from the fact that there are no obstructions to lifting problems with $G = \mathbb{Z}_p$, namely the p-cohomological dimension is one. We explain some specific ramified local plans in § 2.4.1 and 2.4.2 and give a general overview in § 2.5.2.

2.4.1. Torsion pro-p groups. — This is the idea of the proof of the Scholz-Reichardt theorem. Suppose that G contains an element y of order p^m. Take a prime $\mathfrak{q}$ with $p^m \mid N(\mathfrak{q}) - 1$. Suppose a representation $\rho_{\mathfrak{q},n} : G_{\mathfrak{q}} \longrightarrow G/H_n$ defined by $\rho_{\mathfrak{q},n}(\sigma_{\mathfrak{q}}) = \bar{1}$ and $\rho_{\mathfrak{q},n}(\tau_{\mathfrak{q}}) = \bar{y}$ is given. Since $y^{N(\mathfrak{q})-1} = 1$, the map $\rho_{\mathfrak{q}} : G_{\mathfrak{q}} \to G$ given by $\rho_{\mathfrak{q}}(\sigma_{\mathfrak{q}}) = 1$ and $\rho_{\mathfrak{q}}(\tau_{\mathfrak{q}}) = y$ is a local plan; in particular, $\rho_{\mathfrak{q}}$ is a lift of $\rho_{\mathfrak{q},n}$ from G/H_n to G. This is why we need to specify $v_p(N(\mathfrak{q}) - 1)$ in advance.

2.4.2. Torsion-free pro-p groups. — When the pro-p group G is torsion-free, the situation is relatively rigid.

Lemma 2.4. — *Let G_0 be a torsion-free p-adic analytic group of dimension d, and let $\varphi : G_0 \twoheadrightarrow D$ be a continuous morphism of G_0 to an analytic group D having the same dimension. Then φ is an isomorphism.*

Proof. — As φ is surjective, $\ker(\varphi)$ is analytic of dimension zero and hence finite. As G_0 is torsion-free, $\ker(\varphi) = 1$. □

Proposition 2.5. — *Let D be the decomposition group at $\mathfrak{q} \nmid p$ in some torsion-free Galois group G. If $\rho_{\mathfrak{q}} : G_{\mathfrak{q}} \to D$ is such that $\rho_{\mathfrak{q}}(\tau_{\mathfrak{q}})$ is infinite then $\rho_{\mathfrak{q}}$ is an isomorphism.*

Proof. — The image of $\tau_{\mathfrak{q}}$ being infinite forces the image of $\sigma_{\mathfrak{q}}$ to be infinite as well. As the decomposition group is p-adic analytic, the result follows from Lemma 2.4. □

Proposition 2.5 shows that if there is tame ramification in a torsion-free pro-p group G, then G must "contain $G_{\mathfrak{q}}$".

2.5. Stably inertially generated pro-p groups. — Let G be a finitely generated pro-p group. Let $(P_n(G))$ denote the p-central series of G, meaning that $P_1(G) := G$, and $P_{n+1}(G) := P_n(G)^p[G, P_n(G)]$.

2.5.1. Some Definitions. —

Definition 2.6. — Suppose H is a pro-p group, $1 \neq y \in H$. We call y inertial if there exists $x \in H$ such that $[x, y] = y^{ap^k}$ with $a \in \mathbb{Z}_p^\times$ and $k \geqslant 1$.

Remark 2.7. — 1) A torsion element $y \neq 1$ is inertial. Indeed, take $x = 1$, $a = 1$ and p^k to be the order of y.
2) For an element y as above, we can replace x by a suitable power x^{p^t}. This allows us to assume $x \in H_{n+1} \subset H_2$ for any n. This change shifts k to $k + t$.

Definition 2.8. — A pro-p group H is called inertially generated if it can be generated by inertial elements $y_1, \cdots, y_d$. A finitely generated pro-p group G is called stably inertially generated, if the $P_n(G)$ are inertially generated.

Stably inertially generated pro-p groups G are FAb. Indeed, for every n, the abelianization $P_n^{ab}(G)$ of $P_n(G)$ is generated by (the classes of) inertial elements, which are torsion in $P_n^{ab}(G)$. Now it is easy to see that the finiteness of the $P_n^{ab}(G)$ implies the finiteness of U^{ab} for every open subgroup U of G.

Remark 2.9. — We have $\langle \tau_{\mathfrak{q}} \rangle = I_{\mathfrak{q}} \subset G_{\mathfrak{q}} \subset G_K^{\mathrm{ta}}$. If the class number of K is prime to p, then the $I_{\mathfrak{q}}$ generate G_K^{ta} and $[\sigma_{\mathfrak{q}}, \tau_{\mathfrak{q}}] = \tau_{\mathfrak{q}}^{N(\mathfrak{q})-1}$ so G_K^{ta} is inertially generated. We expect it is not stably inertially generated. Inertially generated pro-p groups that are not stably inertially generated exist.

Example 2.10. — Let $G_0 := \langle t \rangle \ltimes H$ be the semi-direct product of $H = \langle a_1, \cdots, a_{p-1} \rangle \cong \mathbb{Z}_p^{p-1}$ by $\langle t \rangle$ of order p with the action:

$$ta_1t^{-1} = a_2;\ ta_2t^{-1} = a_3;\ \cdots;\ ta_{p-2}t^{-1} = a_{p-1};\ ta_{p-1}t^{-1} = a_{p-1}^{-1}a_{p-2}^{-1} \cdots a_1^{-1}.$$

This is well-defined. Note $G_0/[G_0, G_0] = \langle \overline{t}, \overline{a_1} \rangle \cong \mathbb{Z}/p \times \mathbb{Z}/p$, hence G_0 is generated by t and a_1t. A simple computation shows that $(a_1t)^p = 1$, so we have the relations

$t^p = (a_1 t)^p = 1$ and G_0 is inertially generated, but not FAb (the subgroup H is open) and therefore not stably inertially generated.

Remark 2.11. — Set $\mathfrak{gr}_n := \mathfrak{gr}_n(G) := P_n(G)/P_{n+1}(G)$ and $d_n := \dim \mathfrak{gr}_n(G)$. As G is finitely generated, we have $d_n < \infty$. Recall that the map $x \mapsto x^p$ sends $\mathfrak{gr}_n(G)$ to $\mathfrak{gr}_{n+1}(G)$. By Nakayama's Lemma, it is easy to see that if $\mathfrak{gr}_n$ is generated by the images of inertial elements y_i, then $P_n(G)$ is inertially generated (the conjuguate of a inertial element is still inertial). In particular if $P_n(G)$ is inertially generated, the map $x \mapsto x^p$ produces inertial elements in $P_{n+1}(G)$. As we will see, the power of uniform groups is that this map induces an isomorphism between $\mathfrak{gr}_n$ and $\mathfrak{gr}_{n+1}$ for every $n \geqslant 1$; so a uniform group G is stably inertially generated if and only if G is inertially generated.

Example 2.12. — The pro-p group SL_2^1 is stably inertially generated.

Let $G = \mathrm{SL}_2^1(\mathbb{Z}_p) = \ker(\mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{Z}/p))$. Set

$$x = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}, \; y = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}, \; z = \begin{pmatrix} 1+p & p \\ -p & 1-p \end{pmatrix} \in G.$$

The group G is topologically generated by the elements x, y, z.

Given a prime $\mathfrak{q}$ with $p \mid N(\mathfrak{q}) - 1$, let $\alpha \in \mathbb{Z}_p$ be the square root of $N(\mathfrak{q})$ that is 1 mod p. Set

$$s = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}, \; t = \begin{pmatrix} \frac{\alpha+\alpha^{-1}}{2} & \frac{-\alpha+\alpha^{-1}}{2} \\ -\frac{\alpha+\alpha^{-1}}{2} & \frac{\alpha+\alpha^{-1}}{2} \end{pmatrix} \in G.$$

It is a routine computation to check the relations

$$[s, x] = x^{N(\mathfrak{q})-1}, \; [s^{-1}, y] = y^{N(\mathfrak{q})-1}, \text{ and } [t, z] = z^{N(\mathfrak{q})-1}.$$

These are identical to the relation of a tame local group $G_{\mathfrak{q}}$, namely $[\sigma_{\mathfrak{q}}, \tau_{\mathfrak{q}}] = \tau_{\mathfrak{q}}^{N(\mathfrak{q})-1}$, where $\sigma_{\mathfrak{q}}$ is a lift of the Frobenius and $\tau_{\mathfrak{q}}$ a generator of the ramification. Thus we will be able to create local plans for $G = \mathrm{SL}_2^1(\mathbb{Z}_p)$. One also observes that for every n, the subgroups $P_n(G)$ are topologically generated by the elements $x^{p^n}, y^{p^n}, z^{p^n}$, which also are compatible with tame local relations.

If G is stably inertially generated then there exists a sequence of subgroups H_n as in the beginning of Section 2.

Lemma 2.13. — *If G is stably inertially generated then there exists a sequence of normal open subgroups $(H_n)_{n \geqslant 2}$ of G such that:*

(*i*) *$H_1 = G$, $H_2 = [G, G]G^p$, and $\bigcap_n H_n = 1$;*

(*ii*) *the quotient $H_1/H_2 \cong (\mathbb{Z}/p)^d$ can be generated by the image of inertial elements $y_1, \cdots, y_d$ of G for which there exists some $x_i \in H_2$ with $[x_i, y_i] = y_i^{a_i p^{k_i}}$ where $a_i \in \mathbb{Z}_p^\times$ and $k_i \geqslant 1$;*

(*iii*) *for every $n \geqslant 2$, the quotient H_n/H_{n+1} is isomorphic to $\mathbb{Z}/p$, and is generated by the image of inertial element $y \in H_n$ for which there exists some $x \in H_{n+1}$ with $[x, y] = y^{ap^k}$ where $a \in \mathbb{Z}_p^\times$ and $k \geqslant 1$.*

Proof. — (*i*) follows as G is a finitely generated pro-p group and (*ii*) and (*iii*) follow from the definition of stably inertially generated and Remark 2.7. □

2.5.2. The local plan. — Let $y \in H_n \backslash H_{n+1}$ be a inertial element. By Remark 2.7 we can take x in H_{n+1} such that $[x, y] = y^{ap^k}$ for some $a \in \mathbb{Z}_p^\times$, and $k \geqslant 1$. Take a prime $\mathfrak{q}$ such that $N(\mathfrak{q}) = 1 + bp^k$ with $b \in \mathbb{Z}_p$ (we are again specifying a lower bound for $v_p(N(\mathfrak{q}) - 1)$ in advance), and consider the reduction map $\rho_{\mathfrak{q},n} : G_v \to D_{\mathfrak{q},n} \subset G/H_n$, where $D_{\mathfrak{q},n}$ is a decomposition group at $\mathfrak{q}$ in G/H_n, that sends $\sigma_\mathfrak{q}$ to $\overline{1}$ and $\tau_\mathfrak{q}$ to $\overline{y}$.

Set $\alpha = \dfrac{\log_p(1 + bp^k)}{\log_p(1 + ap^k)} \in \mathbb{Z}_p$. The homomorphism $\rho_\mathfrak{q} : G_\mathfrak{q} \to G$, sending $\sigma_\mathfrak{q} \mapsto x^\alpha$ and $\tau_\mathfrak{q} \mapsto y$ is easily seen to be a local plan for $G_\mathfrak{q}$ into G. In particular, $\rho_\mathfrak{q}$ lifts $\rho_{\mathfrak{q},n}$. *Thus there is no obstruction to lift $\rho_{\mathfrak{q},n}$ from $D_{\mathfrak{q},n}$ to G/H_{n+1}.*

2.6. The result. — Let G be a stably inertially generated pro-p group. Recall the various primes we have used:

- — Z_0 is a set of primes chosen via Lemma 1.1 (*iv*). This set guarantees that for all $S_n \supset Z_0$, the $Ш^2_{S_n}$ groups we consider are trivial. The local plan for any prime in Z_0 is unramified.
- — The set $\{\mathfrak{q}_1, \dots, \mathfrak{q}_d\}$ of Proposition 2.2 is chosen to give a map $G_{S_2} \twoheadrightarrow G/H_2 \cong (\mathbb{Z}/p)^d$ where each $I_{\mathfrak{q}_i} = D_{\mathfrak{q}_i} \subset G/H_2$ is $\mathbb{Z}/p$ where $I_{\mathfrak{q}_i}$ is the inertia group. From §2.5.2, there is a local plan $G_{\mathfrak{q}_i} \to G$ for each i.
- — The prime $\tilde{\mathfrak{q}}$ of Proposition 1.4 is used once we have solved $(\mathscr{E}_n)$ to provide a global cohomology class that solves all the local plans at primes in S_n. We will choose $\tilde{\mathfrak{q}}$ so that it has a local plan and we can continue the inductive lifting process.

In this section we prove:

***Theorem 2.14* (Theorem A).** — *Let G be a finitely and stably inertially generated pro-p group. Then there exists a Galois extension L/K in K^{ta}/K such that* $\mathrm{Gal}(L/K) \cong$ *G. Moreover the extension L/K can be taken such that the set of primes splitting completely is infinite.*

Proof. — We consider a sequence of normal open subgroup H_n of G as in Lemma 2.13. The proof is by induction. We will explain the complete splitting at the end of the proof. Recall d is the generator rank of G.

• Since G is stably inertially generated, we see $G = \langle y_1, \cdots, y_d \rangle$ where the y_i are inertial and $x_i \in P_2(G)$ satisfy the relation $[x_i, y_i] = y_i^{a_i p^{n_i}}$.

Proposition 2.2 gives the first step. Namely we obtain K_2/K with $\mathrm{Gal}(K_2/K) \cong (\mathbb{Z}/p)^d$, K_2/K is ramified at $\{\mathfrak{q}_1, \dots, \mathfrak{q}_d\}$ and $\mathbb{Z}/p \cong D_{\mathfrak{q}_i} \subset \mathrm{Gal}(K_2/K)$. Set $S_2 = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_d\} \cup Z_0$ so $Ш^2_{S_2} = 0$ by Lemma 1.1 (*iv*).

Let $\rho_2 : G_{S_2} \to G/H_2$ be the homomorphism sending $\tau_{\mathfrak{q}_i}$ to $\overline{y_i}$ and $\sigma_{\mathfrak{q}_i}$ to $\overline{1}$ and recall we have a local plan for each $G_{\mathfrak{q}_i}$, $i = 1, \cdots, d$.

By Theorem 2.3 there exists a $\mathbb{Z}/p$-extension of K_3'/K_2 in K_{S_2}/K, Galois over K, solving the lifting problem $(\mathscr{E}_2)$, that is, we have a map $G_{S_2} \twoheadrightarrow G/H_3$.

• The problem now is that the decomposition group $D_\mathfrak{q}$ at $\mathfrak{q} \in S_2$ in $\mathrm{Gal}(K_3'/K)$ may not be liftable to G/H_4, that is we may be off the local plan. However, the local plan to G/H_3 does exist and by Theorem 2.3 differs from our local solution to $(\mathscr{E}_2)$ by an element of $f_\mathfrak{q} \in H^1(G_\mathfrak{q})$. By Lemma 2.13, the quotient H_2/H_3 is generated by the image of an inertial element $y \in G$ for which there exists some $x \in H_3$ such that $[x, y] = y^{ap^k}$.

We use Proposition 1.4 with $N = S_2$ and $R = \{\tilde{\mathfrak{q}}\}$ with $\tilde{\mathfrak{q}}$ splitting completely in K_2/K, $(f_\mathfrak{q}) \in \mathrm{Im}(\psi_R)$ and $v_p(N(\tilde{\mathfrak{q}}) - 1) = k$.

Hence there exists $g \in H^1(G_{S_2 \cup R})$ with $g|_{G_{\mathfrak{q}}} = f_{\mathfrak{q}} \,\forall\, \mathfrak{q} \in S_2$. We may act on our solution to $(\mathscr{E}_2)$ by g to produce another solution for which all local obstructions at $\mathfrak{q} \in S_2$ to lifting to G/H_4 vanish; it is on all local plans at S_2. We denote by K_3 the fixed field of the resulting homomorphism $G_{S_2 \cup R} \to G/H_3$.

As we allowed ramification at $\tilde{\mathfrak{q}}$, we need to form a local plan at $\tilde{\mathfrak{q}}$ compatible with our solution to $(\mathscr{E}_2)$. We have $D_{\tilde{\mathfrak{q}},3} = I_{\tilde{\mathfrak{q}},3} = \langle \overline{y} \rangle \cong H_2/H_3 \cong \mathbb{Z}/p$ where $D_{\tilde{\mathfrak{q}},3} \subset G/H_3$ is the image of $G_{\tilde{\mathfrak{q}}}$. Our local plan is $G_{\tilde{\mathfrak{q}}} \to G$ where $\sigma_{\tilde{\mathfrak{q}}} \mapsto x^\alpha$ for suitable α as in § 2.5.2 and $\tau_{\tilde{\mathfrak{q}}} \mapsto y$. Thus we have local plans for all $\mathfrak{q} \in S_3 := S_2 \cup \{\tilde{\mathfrak{q}}\}$ and we are on all of them with our new solution to $(\mathscr{E}_2)$.

We then continue the process by induction. Set $L = \bigcup_n K_n \subset K^{\mathrm{ta}}$. Then $\mathrm{Gal}(L/K) \cong G$.

• If we want the set of primes splitting completely in L/K to be infinite, we proceed as follows. Let us choose a prime $\mathfrak{r}_2$ that splits completely in K_2/K. Set $T_2 = \{\mathfrak{r}_2\}$. The local plan for $\mathfrak{r}_2$ is the trivial homomorphism $G_{\mathfrak{r}_2} \to G$. As previously there exists a $\mathbb{Z}/p$-extension of K_3'/K_2 in K_{S_2}/K, Galois over K, solving the lifting problem $(\mathscr{E}_2)$. Recall that the problem is that the decomposition group $D_{\mathfrak{q}}$ at $\mathfrak{q} \in S_2$ in K_3'/K may be not be lifted in G/H_4, and that $\mathfrak{r}_2$ may not split completely in K_3'/K (we can assume that $\mathfrak{r}_2$ is unramified in K_3'/K). Choose $f_{\mathfrak{r}_2} \in H^1(G_{\mathfrak{r}_2})$ such that acting on our solution to $(\mathscr{E}_2)$ gives trivial decomposition group at $\mathfrak{r}_2 \in T_2$. We again use Proposition 1.4 with $N = S_2 \cup T_2$ to find a global $g \in H^1(G_{N \cup \{\tilde{\mathfrak{q}}\}})$ with $g|_{G_{\mathfrak{q}}} = f_{\mathfrak{q}}$ for all $\mathfrak{q} \in N$. Acting by this class on our first solution to $(\mathscr{E}_2)$ gives a solution on the local plan at all $\mathfrak{q} \in N$ and split completely at $\mathfrak{r}_2 \in T_2$.

Now take a prime $\mathfrak{r}_3 \notin T_2$ that splits completely in K_3/K. Put $T_3 = T_2 \cup \{\mathfrak{r}_3\}$ and continue the process. For all $n \geqslant 2$ we have

(i) $T_2 \subset T_3 \subset \cdots \subset T_n \subset \cdots$,

(ii) $\#T_n = n - 1$,

(iii) and for every n, k, the primes of T_{n+k} split in K_n/K.

Set $T = \bigcup_n T_n$. Then T is infinite, and each prime of T splits completely in L/K. □

Remark 2.15. — We use at most $\log_p |G/H_n|$ tame primes to realize G/H_n as Galois quotient of G_K^{ta}.

Corollary B follows immediately from Theorem A and Remark 2.7. It remains to prove Corollaries C and D and Theorems E and F. See, respectively, Theorems 3.28 and 3.22, Corollary 3.26 and Theorem 3.27.

3. Linear groups and Lie algebras

The group-theoretic results in this section apply to $p = 2$, though our Galois theoretic applications still require $\mu_p \not\subset K$.

3.1. Definitions. — Let G be a finitely generated pro-p group. Recall that $P_n(G)$ denotes the p-central descending series of G, $\mathfrak{gr}_n(G) = P_n(G)/P_{n+1}(G)$, and $d_n = \dim \mathfrak{gr}_n(G)$.

The pro-p group G is called *uniform* if

— G/G^p is abelian where G^p is the normal closure of the subgroup generated by all pth powers in G,

— and if for every $n \geqslant 1$ the map

$$\mathfrak{gr}_n(G) \xrightarrow{x \mapsto x^p} \mathfrak{gr}_{n+1}(G) \tag{4}$$

induces an isomorphism.

In this case, $\mathfrak{gr}_n(G) \cong (\mathbb{Z}/p)^d$ for an integer d called the dimension of G. In particular, $d_n = d$ for every $n \geqslant 2$.

Example 3.1. — For $k \geqslant 1$, set $\mathrm{SL}_m^k := \ker\big(\mathrm{SL}_m(\mathbb{Z}_p) \to \mathrm{SL}_m(\mathbb{Z}/p^k)\big)$ (modulo 2^{k+1} for $p = 2$). Then $G = \mathrm{SL}_m^1$ is uniform of dimension $m^2 - 1$ and for $k \geqslant 1$, $P_k(G) = \mathrm{SL}_m^k$. See [**4**, Chapter 5, Theorem 5.2].

Remark 3.2. — By (4) it is immediate that an inertially generated uniform group is stably inertially generated.

Definition 3.3. — A pro-p group G is called p-adic analytic if G is a closed subgroup of $\mathrm{GL}_m(\mathbb{Z}_p)$ for some m.

Uniform groups are the primary building blocks of p-adic analytic groups.

Theorem 3.4. — *A finitely generated pro-p group G is p-adic analytic if and only if it contains a uniform group H as an open subgroup.*

Proof. — See [**4**, Interlude A and §4, Corollary 4.1]. □

3.2. A dictionary: Lie algebras and p-adic analytic groups.

— We will consider both finitely generated $\mathbb{Z}_p$-Lie algebras, *i.e.* $L \cong \mathbb{Z}_p^d$ and Lie algebras over p-adic fields.

Definition 3.5. — The $\mathbb{Z}_p$-Lie algebra L is called powerful if $[L\,L] \subset 2pL$.

One has [**4**, Theorem 9.10]:

Theorem 3.6. — *There is an equivalence of categories between powerful $\mathbb{Z}_p$-Lie algebras L and uniform groups G.*

As usual, this is obtained via a log map sending a uniform group G to a unique (up to isomorphism) powerful $\mathbb{Z}_p$-Lie algebra $L(G)$ and an exponential map exp sending a powerful Lie algebra L to a unique (up to isomorphism) powerful group G. We set $L_G := L(G) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Given a uniform group G with $x, y \in L(G)$, set $\alpha = \exp(x)$ and $\beta = \exp(y)$. The Lie bracket is defined in $L(G)$ as follows:

$$[x\,y] := \log\left(\lim_n [\alpha^{p^n}, \beta^{p^n}]^{p^{-2n}}\right)$$

where for $g \in P_{m+1}(G)$, we set $g^{p^{-m}}$ to be the unique $g_0 \in G$ such that $g_0^{p^m} = g$.

When G is only p-adic analytic as opposed to uniform, one chooses a uniform open subgroup G_0 of G, and sets $L_G := L_{G_0}$. Of course, L_G does not depend on the choice of G_0.

A Lie algebra over a field is called *perfect* if $[L\,L] = L$. We recall a well-known result useful in our arithmetic context, e.g. for FAb pro-p groups.

Proposition 3.7. — *Let G be a p-adic analytic group G with Lie algebra L_G. The following assertions are equivalent:*

(*i*) *the pro-p group G is FAb;*

(*ii*) *the Lie algebra L_G over $\mathbb{Q}_p$ is perfect;*

(*iii*) *the abelianization G^{ab} of G is finite.*

Proof. — This is classical. See for example [**9**, Proposition 3.18]. □

Example 3.8. — Semisimple Lie algebras are perfect. In particular the groups SL_n^k are FAb.

3.3. Toral and Pluperfect Lie algebras. — Throughout this section, we will always assume that Lie algebras are finite-dimensional over a field F.

Definition 3.9. — A Lie algebra L is called toral if for every $x \in L$, the adjoint endomorphism $\mathrm{ad}_x : y \mapsto [x\,y]$ is semisimple.

Abelian Lie algebras are toral as the adjoint ad_x is the zero map for every $x \in L$.

Proposition 3.10. — *Let L be a toral Lie algebra. There is no element $x \in L$ such that ad_x has a nonzero eigenvalue $\lambda \in F$. In particular, if for every $x \in L$, the characteristic polynomial of ad_x splits over F, then L is abelian.*

Proof. — If ad_x has a non-zero eigenvalue λ with eigenvector y, then

$$\mathrm{ad}_y^2(x) = -\mathrm{ad}_y(\mathrm{ad}_x(y)) = -\mathrm{ad}_y(\lambda y) = 0.$$

By the toral hypothesis ad_y is semisimple, so $0 = \mathrm{ad}_y(x) = -\mathrm{ad}_x(y) = -\lambda y$, contrary to the assumption that $\lambda \neq 0$.

Suppose now that L is not abelian and choose x *not* in the center of L. As ad_x is semisimple it implies that ad_x has non-trivial eigenvalues $\lambda \in F$ (by hypothesis), which is impossible by the previous observation. □

In particular, if F is algebraically closed, toral is equivalent to abelian.

Lemma 3.11. — *Every non-trivial toral Lie algebra L has a non-trivial toral quotient M which is either simple or abelian.*

Proof. — If V is a finite dimensional vector space, W is a subspace of V, and $T\colon V \to V$ is semisimple and satisfies $T(W) \subset W$, then T induces a semisimple linear transformation on V/W. Applying this to ad_x for $x \in L$, it follows that every quotient of a toral Lie algebra L is again toral. Every non-trivial Lie algebra has a non-trivial quotient which is either simple or abelian. □

Definition 3.12. — A Lie algebra L is called pluperfect if every toral quotient L/I, is trivial.

A pluperfect Lie algebra is perfect: If L is not perfect, then $L/[L, L]$ is a non-trivial abelian Lie algebra, and therefore a toral quotient of L, so L is not pluperfect.

Observe that a simple Lie algebra is either toral or pluperfect but not both. Over an algebraically closed field, it cannot be toral, so it must be pluperfect.

Proposition 3.13. — *A non-trivial Lie algebra L is pluperfect if and only if L is perfect and $L/\mathrm{Rad}(L)$ is a direct sum of pluperfect simple Lie algebras.*

Proof. — Let L be pluperfect. If $[L\,L]$ is a proper ideal of L, then $L/[L\,L]$ is a non-trivial abelian and hence toral quotient of L, so L is perfect. Moreover, $L/\mathrm{Rad}(L)$ is semisimple quotient of L, so it can be written as a (possibly empty) direct sum $L_1 \oplus \cdots \oplus L_m$ of simple Lie algebras. Each L_i is therefore a simple quotient of L, so L_i is not toral and must therefore be pluperfect.

Conversely, suppose L has a non-trivial toral quotient L/I. By Lemma 3.11, we may assume that L/I is either abelian or that it is simple. In the first case, L cannot be perfect. So we assume that L/I is simple. The image of $\mathrm{Rad}(L)$ in L/I is a solvable ideal, so it must be (0), so $I \supset \mathrm{Rad}(L)$, and we may think of L/I as a quotient of $L/\mathrm{Rad}(L) = L_1 \oplus \cdots \oplus L_m$ where each L_i is simple. However, all maximal proper ideals of a semisimple Lie algebra are kernels of projection maps $L \to L_i$, so L/I must be isomorphic to one of the L_i, which means that at least one of the summands of $L/\mathrm{Rad}(L)$ is not pluperfect. □

Over an algebraically closed field, therefore, a Lie algebra is pluperfect if and only if it is perfect.

3.4. Inertially generated Lie algebras. — Throughout this section, we will always assume that Lie algebras L are finite-dimensional over a field F of characteristic 0. We introduce the notion of inertially generated Lie algebras as an analog of inertially generated pro-p groups.

Definition 3.14. — A nonzero element y of a Lie algebra L is called inertial if it is an eigenvector with nonzero eigenvalue of the adjoint ad_x for some x. A Lie algebra L over a field F is called inertially generated if there exists an F-basis $\{y_1, \cdots, y_d\}$ with each y_i inertial.

An inertial element is strongly ad-nilpotent (see [**11**, §16.1]) and therefore ad-nilpotent (see [**11**, §15.1]).

Proposition 3.15. — *Any inertially generated Lie algebra L is pluperfect.*

Proof. — Any quotient of an inertially generated Lie algebra L is again inertially generated. If I is an ideal of L such that L/I is toral, then by Proposition 3.10, L/I has no inertial elements, so L/I is trivial. Thus, L is pluperfect. □

The converse is true in characteristic 0. To prove this, we begin with a lemma.

Lemma 3.16. — *Let L be a Lie algebra spanned by ad-nilpotent elements. Then the span I of the set of inertial elements in L is an ideal.*

Proof. — If z is any ad-nilpotent element of L, then $\mathrm{ad}_z^{\dim L} = 0$ and the function

$$y \mapsto \exp(\,\mathrm{ad}_z)(x) = \sum_{i=0}^{\dim L - 1} \frac{\mathrm{ad}_z^i(y)}{i!}$$

is a Lie algebra automorphism of L (see [**11**, §2.3]). As being inertial is a characteristic property of a Lie algebra, we see that y inertial implies

$$\exp(m\,\mathrm{ad}_z)(y) = \sum_{i=0}^{\dim L - 1} \frac{m^i \mathrm{ad}_z^i(y)}{i!}$$

is inertial. By the linear independence of the sequences $1, m, m^2, \ldots, m^{\dim L - 1}$ as m ranges from 1 to $\dim L$, it follows that each $\dfrac{\mathrm{ad}_z^i(y)}{i!}$ lies in I. Taking $i = 1$ we see ad_z preserves I. Since the nilpotent elements span L, I is preserved by ad_z for all $z \in L$, so it is an ideal. □

Theorem 3.17. — *A pluperfect Lie algebra L is inertially generated.*

Proof. — We consider first the case that L is a simple Lie algebra. Since it is pluperfect, it is not toral, so there exists $x \in L$ such that ad_x is not semisimple. As L is semisimple and F is of characteristic 0, x admits a Jordan-Chevalley decomposition $x = x_s + x_n$, with ad_{x_n} non-zero and nilpotent.

By the Jacobson-Morozov theorem, there exists an injective homomorphism $i \colon \mathfrak{sl}_2 \to L$ sending $e := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ to x_n. As e is inertial in $\mathfrak{sl}_2$, it follows that $x_n = i(e)$ is inertial in L.

Let G denote the algebraic subgroup of $\mathrm{GL}(L)$ which stabilizes the Lie bracket. The Lie algebra of G consists of derivations of L, and as L is semisimple, it coincides with L. Let G° denote its identity component, which is a simple algebraic group with Lie algebra L. As F is perfect and infinite, $G^\circ(F)$ is Zariski-dense in G° [**20**], so L, which is irreducible as a G°-representation, is likewise irreducible over $G^\circ(F)$. Since it contains at least one inertial element and inertial elements map to inertial elements under conjugation by elements of $G^\circ(F)$, L is inertially generated. It follows immediately that for any semisimple Lie algebra, pluperfect implies inertially generated.

Now let L be an arbitrary pluperfect Lie algebra, and let $M := L/\mathrm{Rad}(L)$. As M is a quotient of L, it is likewise pluperfect and therefore inertially generated. By the Lie-Malcev theorem, there exists an embedding of Lie algebras $j \colon M \to L$ whose composition with the quotient morphism $L \to M$ gives the identity. By the comment after Definition 3.14, $j(M)$ is spanned by strongly ad-nilpotent elements. On the other hand, L is perfect, so by [**3**, §5, Théorème 1], $\mathrm{Rad}(L)$ is nilpotent, so L is spanned by ad-nilpotent elements. By Lemma 3.16, the span I of inertial elements is an ideal of L.

Now, $j(M) \subset I$, so $\mathrm{Rad}(L)$ maps onto L/I, which implies that L/I is nilpotent. If $L/I \neq 0$, it has a non-trivial abelian quotient, contrary to the fact that L is perfect. Therefore, $I = L$, and L is inertially generated. □

Corollary 3.18. — *Let $L \subset \mathfrak{sl}_n(F)$ be simple over F. Suppose that there exists $x \in L$ such that ad_x has a nonzero eigenvalue. Then L is inertially generated. In particular this is the case if ad_x has two different eigenvalues $\lambda_1, \lambda_2 \in F$.*

Proof. — By Proposition 3.10, L is pluperfect and Theorem 3.17 shows it is inertially generated. For the second part, observe that if x_s is the semisimple part of x, then $x_s \in L$ since L is simple. In particular, it is not difficult to see that $\lambda_1 - \lambda_2$ is a nonzero eigenvalue of ad_{x_s} in F. □

Proposition 3.19. — *Let L be a simple Lie algebra and G° the identity component of the algebraic group of automorphisms of L. Then L is pluperfect if and only G° is isotropic, i.e., of positive rank over F.*

Proof. — By [**2**, Corollaire 8.5], G° is isotropic if and only if it has a non-trivial unipotent subgroup defined over F. Any non-zero tangent vector of such a subgroup is ad-nilpotent in L.

Conversely, if G° is pluperfect, it is inertially generated, so L contains a non-zero ad-nilpotent element x, which determines a homomorphism of algebraic groups $t \mapsto \exp(\mathrm{ad}(t\,x))$ from the additive group to G°. Thus, G° contains a unipotent subgroup, so it must be isotropic. □

3.5. Examples over local fields. — Let F be $\mathbb{R}$ or a p-adic field. A simple group $G_{/F}$ is anisotropic if and only its group of F-points is compact [**1**, §6.4]. In the real case, this amounts to L being a compact Lie algebra. In the p-adic case, the only anisotropic, simply connected, absolutely simple algebraic groups are inner forms of A_n [**23**, §3.3.3]. At the Lie algebra level, L consists of the elements of reduced trace zero in a division algebra D whose center is a finite extension of $\mathbb{Q}_p$. We can see this explicitly.

Proposition 3.20. — *Let D be a division algebra over $\mathbb{Q}_p$ so D is a Lie algebra with the bracket $[x\,y] = xy - yx$. Let D_0 be the Lie subalgebra of elements of trace zero. The Lie algebra D_0 is simple and perfect, but not pluperfect.*

Proof. — As $D_0 \otimes \overline{\mathbb{Q}_p} \cong \mathfrak{sl}_n$ which is simple, D_0 is simple. One then has to verify that for every $x \in D_0$, the adjoint ad_x is semisimple. But, since D_0 is simple, if we write $\mathrm{ad}_x = \mathrm{ad}_{x_s} + \mathrm{ad}_{x_n}$, with semisimple and nilpotent parts x_s and x_n, then x_s and x_n are in D_0. Since elements of D_0 have multiplicative inverses, $x_n = 0$, and then $x = x_s$ implying that $\mathrm{ad}_x = \mathrm{ad}_{x_s}$. □

Recall that division algebras over $\mathbb{Q}_p$ are classified by the Brauer group of $\mathbb{Q}_p$, which is isomorphic to $\mathbb{Q}/\mathbb{Z}$. For $p > 2$, let $D = (a, p)$ be the (unique up to isomorphism) nonsplit quaternion algebra over $\mathbb{Q}_p$, where a is not a square mod p. Let D_0 be the pure quaternions corresponding to quaternion elements of zero trace, that is a simple Lie algebra L of dimension 3 which is not pluperfect. Hence the explicitly described Lie algebra is perfect but not pluperfect:

$$\langle x, y, z \mid [x\,y] = pz, [x\,z] = pay, [y\,z] = p^2x\rangle.$$

The uniform group is described in the following example.

Example 3.21. — Recall p is odd. Let $a \in \mathbb{Z}$ such that a is not a square mod p. Set $U = \begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix}$, and consider the two following matrices of $\mathrm{SL}_4(\mathbb{Z}_p)$:

$$A = \begin{pmatrix} U & 0 \\ 0 & -U \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & aI_2 \\ I_2 & 0 \end{pmatrix}.$$

Then $A^2 = pI_4$, $B^2 = aI_4$ and $AB = -BA = \begin{pmatrix} 0 & aU \\ -U & 0 \end{pmatrix}$. Hence, the $\mathbb{Q}_p$-algebra generated by I_4, A, B, AB is isomorphic to the quaternion algebra (a, p).

Set $A_0 = pA$, $B_0 = pB$, $C_0 = pAB$, and put $x = \exp(A_0), y = \exp(B_0), z = \exp(C_0) \in \mathrm{SL}_4(\mathbb{Z}_p)$. Then the sub-group G of $\mathrm{SL}_4(\mathbb{Z}_p)$ generated by x, y and z is uniform of dimension 3 and has toral Lie algebra.

3.6. Applications. —

3.6.1. Uniform groups with pluperfect Lie algebras. — We prove our second main result.

***Theorem 3.22* (Corollary D).** — *Every p-adic analytic group G with pluperfect Lie algebra L_G has a uniform open subgroup G_0 which is quotient of G_K^{ta}.*

Proof. — Let G be a p-adic analytic group of Lie algebra L_G. Theorem 3.17 implies that $L = \sum_{i=1}^{d} \mathbb{Q}_p s_i$ for some inertial elements s_i Take a powerful $\mathbb{Z}_p$-Lie subalgebra of L as follows: multiply the elements s_i by p^k for large k so that $L' := \sum_{i=1}^{d} \mathbb{Z}_p s_i$ is powerful. Set $G_0 = \exp(L')$. The group G_0 is uniform and generated by the exponentials of the inertial elements $x_i := p^k s_i$. In the proof of Theorem 3.17 we saw that each x_i is in a SL_2-triple so there exist $y_i, z_i \in L'$, after multiplying by p^k for large k, such that

$$[z_i\, x_i] = 2p^m x_i;\ [z_i\, y_i] = -2p^m y_i;\ [x_i\, y_i] = p^m z_i$$

for some $m \geqslant 1$. These relations are the same as those satisfied by the matrices

$$A = \begin{pmatrix} 0 & p^m \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ p^m & 0 \end{pmatrix}, \text{ and } C = \begin{pmatrix} p^m & 0 \\ 0 & -p^m \end{pmatrix}$$

in SL_2. Exponentiating the various SL_2-triples in L, we see G contains a uniform open subgroup G_0 that is inertially generated. By Remark 3.2, G_0 is stably inertially generated. Theorem 2.14 gives the result. □

Sometimes the lattice to take in L_G is natural, as is the case for the linear groups SL_m^1.

Example 3.23. — Let $\mathfrak{gl}_m := \mathfrak{gl}_m(\mathbb{Z}_p)$ the $\mathbb{Z}_p$-Lie algebra of matrices with coefficients in $\mathbb{Z}_p$. Denote by $E_{i,j}$ the elementary matrices of$\mathfrak{gl}_m$, where 1 has been replaced by p, and for $i = 1, \cdots, m-1$, set $E_i = E_{i,i} - E_{i+1,i+1} + E_{i,i+1} - E_{i+1,i}$.

Let $\mathfrak{sl}_m \subset \mathfrak{gl}_m$ be the sub-Lie-algebra of $\mathfrak{gl}_m$ generated by the $E_{i,j}$ and E_i (all have trace zero). The $\mathbb{Z}_p$-Lie algebra $\mathfrak{sl}_m$ is powerful. Set $y_{i,j} = \exp(E_{i,j})$, $i \neq j$, and $y_i = \exp(E_i)$. The $y_{i,j}$ and y_i generate $\mathrm{SL}_m^1(\mathbb{Z}_p)$.

It is easy to see that the $y_{i,j}$ and y_i are inertial so SL_m^1 is inertially generated, and then stably inertially generated by Remark 3.2.

One then obtains part of Corollary C. The full result is given in § 3.7.

Theorem 3.24. — *For every $m \geqslant 2$ and $k \geqslant 2$, the pro-p groups $\mathrm{SL}_m^k(\mathbb{Z}_p)$ are quotients of G_K^{ta}.*

Proof. — The $\mathrm{SL}_m^k(\mathbb{Z}_p)$ are uniform, and stably inertially generated by Example 3.23. Apply Theorem 2.14. □

3.6.2. Toral uniform extensions. — As $\mathbb{Z}_p$-extensions of number fields are only wildly ramified, there is no tame ramification in an abelian uniform extension of a number field K. This is also a consequence of the following Proposition.

Proposition 3.25. — *In a toral uniform extension of a number field K, there is no tame ramification.*

Proof. — Suppose that there is tame ramification at $\mathfrak{q}$ in a non-trivial toral uniform extension. By Proposition 2.5 this would imply a relation of the form $[\alpha, \beta] = \beta^{N(\mathfrak{q})-1}$ in the uniform group which produces the relation $[x\, y] = \log_p(N(\mathfrak{q}))y$ in $L(G)$ where $x = \log(\alpha)$ and $y = \log(\beta)$. Indeed, some elementary p-adic analysis yields

$$[x\, y] = \log_p\left(\lim_n [\alpha^{p^n}, \beta^{p^n}]^{p^{-2n}}\right) = \log_p\left(\lim_n \left(\beta^{p^n(N(\mathfrak{q}))}\right)^{p^{-2n}}\right) = \log_p(N(\mathfrak{q}))y,$$

where $\log_p$ is the usual p-adic logarithm. Since $\log_p(N(\mathfrak{q})) \neq 0$, this contradicts Proposition 3.10. □

***Corollary 3.26* (Theorem E).** — *If the Hilbert p-class field tower of K is finite, then there is no non-trivial toral uniform quotient of G_K^{ta}.*

Proof. — Let G be a non-trivial toral uniform pro-p group. If G is quotient of G_K^{ta}, then since the p-class field tower of K is finite, there is tame ramification in the corresponding extension contradicting Proposition 3.25. □

In particular, the group of Example 3.21 is not quotient of G_K^{ta}.

Recall the Fontaine-Mazur conjecture for tame extensions predicts this result holds without the class field tower hypothesis.

To conclude this section, we finish with an extension of the previous result.

***Theorem 3.27* (Theorem F).** — *Let d_K to be the absolute discriminant of K.*
(1) Take T such that $\alpha_T + \sum_{v|\infty} \alpha_{\mathfrak{q}} > \log\sqrt{|d_K|}$. Then $G_K^{\mathrm{ta},T}$ has no non-trivial uniform toral quotient.
(2) Assume the GRH and T such that $\alpha_T^{\mathrm{GRH}} + \sum_{v|\infty} \alpha_{\mathfrak{q}}^{\mathrm{GRH}} > \log\sqrt{|d_K|}$. Then $G_K^{\mathrm{ta},T}$ has no non-trivial uniform toral quotient.

Proof. — We proceed by contradiction. Suppose $G_K^{\mathrm{ta},T}$ has a non-trivial uniform toral quotient $G = \mathrm{Gal}(L/K)$ with $L \subset K^{\mathrm{ta}}$. Then by Proposition 3.25, L/K is unramified. We use Theorem 1 and Proposition 1 of [**12**]: in an infinite unramified extension L/K one unconditionally has $\alpha_T + \sum_{v|\infty} \alpha_{\mathfrak{q}} \leqslant \log\sqrt{|d_K|}$, and assuming the GRH one has $\alpha_T^{\mathrm{GRH}} + \sum_{v|\infty} \alpha_{\mathfrak{q}}^{\mathrm{GRH}} \leqslant \log\sqrt{|d_K|}$, contradicting our assumption. □

3.7. Lifting to the special linear group over complete local Noetherian rings.

— The result below follows immediately from Theorem 2.14. The prime p is odd.

***Theorem 3.28* (Corollary C).** — *For any complete Noetherian local ring A with residue field $\mathbb{F}_p$, $\mathrm{SL}_m^k(A)$ is a quotient of G_K^{ta} and can correspond to a Galois extension L/K in which infinitely many primes split completely.*

Proof. — We first prove the result for the ring $A = \mathbb{Z}_p[\![T_1, \cdots, T_n]\!]$.

The proof is an extension of Example 2.12, with the technical difficulty that we cannot use the exponential map.

First by Proposition 13.29 of [**4**], the sequence $\left(\mathrm{SL}_m^k(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!])\right)_k$ corresponds to the p-central series of $\mathrm{SL}_m^k(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!])$. Set $\mathfrak{m} = (p, T_1, \cdots, T_n)$ the maximal ideal of $\mathbb{Z}_p[\![T_1, \cdots, T_n]\!])$. Hence, it suffices to prove that for each $k \geqslant 1$,

$$\mathrm{SL}_m^k(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!])/\mathrm{SL}_m^{k+1}(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!]) \cong \mathfrak{m}^k/\mathfrak{m}^{k+1} \otimes_{\mathbb{Z}} M_m^0(\mathbb{Z})$$

is spanned by the images of inertial elements of $\mathrm{SL}_m^k(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!])$.

We consider first the case $m = 2$. If $a_0 + \cdots + a_n = k$, the following relations hold in $\mathrm{SL}_2^k(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!])$:

$$\begin{pmatrix} 1-p^k & 0 \\ 0 & (1-p^k)^{-1} \end{pmatrix} \begin{pmatrix} 1 & p^{a_0}T_1^{a_1}\cdots T_n^{a_n} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} (1-p^k)^{-1} & 0 \\ 0 & (1-p^k) \end{pmatrix} = \begin{pmatrix} 1 & p^{a_0}T_1^{a_1}\cdots T_n^{a_n} \\ 0 & 1 \end{pmatrix}^{(p^k-1)^2},$$

$$\begin{pmatrix} (1-p^k)^{-1} & 0 \\ 0 & 1-p^k \end{pmatrix} \begin{pmatrix} 1 & 0 \\ p^{a_0}T_1^{a_1}\cdots T_n^{a_n} & 1 \end{pmatrix} \begin{pmatrix} 1-p^k & 0 \\ 0 & (1-p^k)^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p^{a_0}T_1^{a_1}\cdots T_n^{a_n} & 1 \end{pmatrix}^{(p^k-1)^2}.$$

Also, if

$$N := \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, \ D := \begin{pmatrix} \frac{(1-p^k)+(1-p^k)^{-1}}{2} & \frac{(1-p^k)-(1-p^k)^{-1}}{2} \\ \frac{(1-p^k)-(1-p^k)^{-1}}{2} & \frac{(1-p^k)+(1-p^k)^{-1}}{2} \end{pmatrix},$$

then N is nilpotent and $DND^{-1} = (p^k-1)^2 N$, so

$$D(I + p^{a_0}T_1^{a_1}\cdots T_n^{a_n}N)D^{-1} = (I + p^{a_0}T_1^{a_1}\cdots T_n^{a_n}N)^{(p^k-1)^2},$$

and $\mathfrak{m}^k/\mathfrak{m}^{k+1} \otimes_{\mathbb{Z}} M_2^0(\mathbb{Z})$ is spanned by inertial elements.

To finish the proof for general m, consider all embeddings of $\mathrm{SL}_2^k(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!])$ in $\mathrm{SL}_m^k(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!])$ which come from choosing an ordered pair of standard basis vectors. Together the images of all the inertial elements in $\mathrm{SL}_2^k(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!])$ which we just constructed will span $\mathfrak{m}^k/\mathfrak{m}^{k+1} \otimes_{\mathbb{Z}} M_m^0(\mathbb{Z})$ because the span of all images of $M_2^0(\mathbb{Z})$ in $M_m^0(\mathbb{Z})$ obtained by choosing pairs of basis elements of $\mathbb{Z}^m$ generates $M_m^0(\mathbb{Z})$.

For the general case, observe first that A is isomorphic to $\mathbb{Z}_p[\![T_1, \cdots, T_n]\!]/I$ for some ideal I. It is then sufficient to prove that the reduction map $\mathrm{SL}_m^k(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!]) \to \mathrm{SL}_m^k(A)$ is surjective. Then take $x \in \mathrm{SL}_m^k(A)$ and lift it to an $m \times m$ matrix c with entries in $\mathbb{Z}_p[\![T_1, \cdots, T_n]\!]$ which is congruent to 1 mod $\mathfrak{m}^k$. Say the determinant is d. Then d is 1 mod $\mathfrak{m}^k \cap I$ and is an unit of $\mathbb{Z}_p[\![T_1, \cdots, T_n]\!]$; in particular d^{-1} is 1 mod $\mathfrak{m}^k \cap I$. Multiply the first row of c by d^{-1} to get c'. Then $c' \in \mathrm{SL}_m^k(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!])$ and c' mod I is exactly x. □

The interest of Theorem 3.28 is that the groups $\mathrm{SL}_m^k(\mathbb{Z}_p[\![T_1, \cdots, T_n]\!])$ provide examples of quotients of G_K^{ta} which are “between” p-adic Lie groups and Golod-Shafarevich groups. There is no known infinite pro-p quotient of G_K^{ta} ramified at finitely many primes that is not virtually Golod-Shafarevich, i.e. contains on open subgroup that is Golod-Shafarevich. See [**4**, Chapter 13] for more details.

References

[1] A. Borel, Linear algebraic groups. *Algebraic Groups and Discontinuous Subgroups* (Proc. Sympos. Pure Math., Boulder, Colo., 1965), pp. 3–19, Amer. Math. Soc., Providence, RI, 1966.

[2] A. Borel and J. Tits, *Groupes réductifs.* Inst. Hautes Études Sci. Publ. Math. No. 27 (1965), 55–150.

[3] N. Bourbaki, *Groupes et algèbres de Lie.* Chapitre I: Algèbres de Lie. Seconde édition. Actualités Scientifiques et Industrielles, No. 1285. Hermann, Paris, 1971.

[4] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*, 2nd ed. Cambridge University Press, (1999), xviii+ 365 pages.

[5] J-M. Fontaine and B. Mazur, *Geometric Galois representations*, In Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995.

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

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

[8] F. Hajir and C. Maire, *Prime decomposition and the Iwasawa mu-invariant*, Mathematical Proceedings of the Cambridge Philosophical Society **166** (2019), 599–617.

[9] F. Hajir and C. Maire, *Analytic Lie extensions of number fields with cyclic fixed points and tame ramification* Journal of the Ramanujan Mathematical Society **37** (2022), 63–85.

[10] F. Hajir, C. Maire, and R. Ramakrishna, *On the Shafarevich group of restricted ramification extensions of number fields in the tame case*, Indiana Univ. Math. J. 70 (2021), no. 6, 2693–2710.

[11] J. E. Humphreys, Introduction to Lie Algebras and Representation Theory, third printing revised, Graduate Texts in Mathematics, Vol. 9, Springer-Verlag, New York Heidelberg Berlin, 1972.

[12] Y. Ihara, *How many primes decompose completely in an infinite unramified Galois extension of a global field?*, J. Math. Soc. Japan **35** (1983), no. 4, 693–709.

[13] C. Khare, M. Larsen, and R. Ramakrishna, *Constructing semisimple* p*-adic Galois representations with prescribed properties*, Amer. J. Math. 127 (2005), no. 4, 709–734.

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

[15] M. Lazard, *Groupes analytiques* p*-adiques*, IHES, Publ. Math. **26** (1965), 389–603.

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

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

[18] R. Ramakrishna, *Infinitely ramified Galois representations*, Ann. of Math. (2) 151 (2000), no. 2, 793–815.

[19] R. Ramakrishna, *Constructing Galois representations with very large image*, Canad. J. Math. 60 (2008), no. 1, 208–221.

[20] M. Rosenlicht, *Some rationality questions on algebraic groups*, Ann. Mat. Pura Appl. (4) 43 (1957), 25–50.

[21] P. Schmid, *Realizing* 2*-groups as Galois groups following Shafarevich and Serre*, Algebra and Number Theory **12** (2018), 2387-2400.

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

[23] J. Tits, Classification of algebraic semisimple groups. *Algebraic Groups and Discontinuous Subgroups* (Proc. Sympos. Pure Math., Boulder, Colo., 1965), pp. 33–62, Amer. Math. Soc., Providence, RI, 1966.

[24] E. Zelmanov, *On groups satisfying the Golod-Shafarevich condition, New horizons in pro-p groups* 223–232. Progr. Math., 184 Birkhäuser Boston, Inc., Boston, MA, 2000.

January 11, 2024

Farshid Hajir, Michael Larsen, Christian Maire, Ravi Ramakrishna, Department of Mathematics & Statistics, University of Massachusetts, Amherst, MA 01003, USA
Department of Mathematics, Indiana University, Bloomington, IN 47405, USA • FEMTO-ST Institute, Université de Franche-Comté, CNRS, 15B avenue des Montboucons, 25000 Besançon, FRANCE • Department of Mathematics, Cornell University, Ithaca, NY 14853-4201 USA
E-mail : hajir@math.umass.edu, mjlarsen@indiana.edu, christian.maire@univ-fcomte.fr, ravi@math.cornell.edu