THE SYLOW SUBGROUPS OF THE ABSOLUTE GALOIS GROUP $\mathrm{Gal}(\mathbb{Q})$

LIOR BARY-SOROKER, MOSHE JARDEN, AND DANNY NEFTIN

Abstract. We describe the ℓ-Sylow subgroups of $\mathrm{Gal}(\mathbb{Q})$ for an odd prime ℓ, by observing and studying their decomposition as $F \rtimes \mathbb{Z}_\ell$, where F is a free pro-ℓ group, and $\mathbb{Z}_\ell$ are the ℓ-adic integers. We determine the finite $\mathbb{Z}_\ell$-quotients of F and more generally show that every split embedding problem of $\mathbb{Z}_\ell$-groups for F is solvable. Furthermore, we analyze the $\mathbb{Z}_\ell$-action on generators of F.

1. Introduction

The absolute Galois group $\mathrm{Gal}(\mathbb{Q}) = \mathrm{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q})$, where $\tilde{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$, is a central object in Galois theory and number theory. As a Galois group, $\mathrm{Gal}(\mathbb{Q})$ is profinite, and hence admits a Sylow theory [22, Chapter 2.3]. We denote an ℓ-Sylow subgroup of $\mathrm{Gal}(\mathbb{Q})$ by $\mathrm{Gal}(\mathbb{Q}^{(\ell)})$, where $\mathbb{Q}^{(\ell)}$ is the fixed field of the Sylow subgroup. Similarly for any field K, $\mathrm{Gal}(K^{(\ell)})$ is an ℓ-Sylow subgroup of $\mathrm{Gal}(K)$.

For local fields K, the Sylow subgroups $\mathrm{Gal}(K^{(\ell)})$ have been studied and are completely understood: if $K = \mathbb{Q}_p$, either $\mathrm{Gal}(K^{(\ell)})$ is generated by two elements σ, τ such that σ normalizes τ, as follows from Iwasawa [16, Theorem 7.5.2], or a group on countably many generators subject only to one known relation if $p = \ell$. The latter was proved by Labute [11], cf. [12], solving a question of Serre, based on the work of Shafarevich, Serre, and Demushkin [23, §5.6].

For a global field K and $\ell = \mathrm{char}\, K$, $\mathrm{Gal}(K^{(\ell)})$ is a free pro-ℓ group on countably many generators by Artin-Schreier theory [23, §2.2 Corollary 1]. However, when $\ell \neq \mathrm{char}\, K$ the structure of $\mathrm{Gal}(K^{(\ell)})$ is much more subtle: $\mathrm{Gal}(K^{(\ell)})$ is far from being free, and neither $\mathrm{Gal}(K^{(\ell)})$ nor its maximal quotients with restricted ramification are finitely generated, cf. Remark 5.12. In particular, with the exception of the determination of its finitely generated subgroups in [2], the structure of $\mathrm{Gal}(K^{(\ell)})$ for a global field K and $\ell \neq \mathrm{char}\, K$ has so far been unapproachable.

We describe $\mathrm{Gal}(K^{(\ell)})$ for a global field K and $\ell \neq \mathrm{char}(K)$ by observing and studying the following decomposition.

Denote by μ_{ℓ^∞} the group of ℓ-power roots of unity.

Theorem 1.1. *Let K be a global field and $\ell \neq \mathrm{char}(K)$ an odd prime*[1]*. Put $Z = \mathrm{Gal}(K^{(\ell)}(\mu_{\ell^\infty})/K^{(\ell)})$ and $F = \mathrm{Gal}(K^{(\ell)}(\mu_{\ell^\infty}))$. Then $Z \cong \mathbb{Z}_\ell$, F is a free*

[1]Similar results hold for $\ell = 2$, see §3.

pro-ℓ group on infinitely many generators, and

$$\mathrm{Gal}(K^{(\ell)}) = F \rtimes Z. \tag{1}$$

We call the decomposition (1) the **cyclotomic decomposition**. To describe the action of Z on F, we first determine the finite quotients of F as a Z-group by more generally studying embedding problems for F which respect the Z-action. We then apply the resulting tools to make the first step towards determining the Z-action on F by analyzing the action on generators of F up to elements in $F^\ell[F,F]$, the first level in the lower ℓ-central series of F.

As in profinite group theory, in which embedding problems are used to determine profinite groups, we study the Z-group F via Z-embedding problems. A **finite Z-embedding problem** for F is a pair of Z-epimorphisms $(\alpha\colon F \to \Gamma, \beta\colon G \to \Gamma)$, where G, Γ are finite Z-groups. A **proper solution** of (α, β) is a lifting of β to a Z-epimorphism $\gamma\colon F \to G$, cf. §2.1.

Analogously to the classical setting, solvability of Z-embedding problems is reduced to solvability of Frattini Z-embedding problems and of split Z-embedding problems. Here (α, β) is **split** if β has a section as a Z-homomorphism.

Theorem 1.2. *Every finite split Z-embedding problem for F is properly solvable. In particular, every finite ℓ-group G equipped with a Z-action is a quotient of F as a Z-group.*

We note that in general Frattini Z-embedding problems for F are not solvable. Nevertheless one can reduce such problems to a classical setting over global fields, see Proposition 4.3.

The proof of Theorem 1.2 is based on the observation of Colliot-Thélène that fields with pro-ℓ absolute Galois group are ample [10, Theorem 5.8.3], Pop's theorem on solvability of split embedding problems for function fields over an ample field [10, Theorem 5.9.2], and Hilbert's irreducibility theorem.

To study the Z-action on generators of F, we describe the structure of the Frattini quotient $\overline{F} = F/F^\ell[F,F]$ as a Z-module, and determine its finite direct Z-summands. Since Z acts on the group ring $\mathbb{F}_\ell[Z/\ell^n Z]$, it also acts on $\mathbb{F}_\ell[[Z]] = \varprojlim \mathbb{F}_\ell[Z/\ell^n Z]$. A Z-module M is said to be a direct Z-summand of $\overline{F}$ of multiplicity ω, if $\overline{F} \cong M^\omega \times M'$, where M^ω is the product of countably many copies of M, and M' has no Z-summands isomorphic to M.

Theorem 1.3. *The finite direct Z-summands of $\overline{F}$ are $\mathbb{F}_\ell[Z/\ell^n Z]$, $n \in \mathbb{N}$, each appearing with multiplicity ω. If furthermore K is a number field, then $\mathbb{F}_\ell[[Z]]$ is direct Z-summand of multiplicity ω in $\overline{F}$.*

In analogy to the works of Demushkin, Serre and Labute, where the relations are determined up to elements in a low level of a filtration and then lifted to the entire group, Theorem 1.3 gives relations in a presentation of $\mathrm{Gal}(K^{(\ell)})$ up to elements in the first level $F^\ell[F,F]$ of the lower ℓ-central series of F. Namely,

letting σ be a generator of Z, each summand $\mathbb{F}_\ell[Z/\ell^k Z]$ gives a subset of generators $x_1, \ldots, x_{\ell^k}$ of F subject only to the relations $\sigma x_i \sigma^{-1} = x_i x_{i+1}$ for $i = 1, \ldots, \ell^k - 1$ and $\sigma x_{\ell^k} \sigma^{-1} = x_{\ell^k} y$, for some $y \in F^\ell[F, F]$. Similar relations are obtained for each $\mathbb{F}_\ell[[Z]]$ summand, see Corollary 5.10.

A main difficulty in studying $\overline{F}$ is that $\overline{F}$ not finitely generated as a Z-module. To overcome this difficulty we utilize the theory of Ulm invariants, cf. §5.1. This new approach is parallel to that of Minac, Schulz, and Swallow [14] and [15], but also allows dealing with modules over an infinite group such as Z. The proof then reduces to determining the solvability of Z-embedding problems for elementary abelian Z-groups. To determine the solvability of such problems, we establish a local global principle using the Poitou-Tate duality theorem, and combine it with results from Iwasawa theory. This suffices in order to find the finite Ulm invariants of $\overline{F}$, and hence determine the finite Z-summands of $\overline{F}$.

We also deduce that the infinite Ulm invariants are the Ulm invariants of an interesting but still mysterious Iwasawa module, cf. §5.7. In particular, we deduce using Iwasawa theory that $\overline{F}$ has nontrivial infinite Ulm invariants. It follows that the direct product of all of the Z-summands in Theorem 1.3 is not all of $\overline{F}$, and hence not all generators of $\overline{F}$ arise from Theorem 1.3. Obtaining a full account of the action on the remaining generators is equivalent to determining the above Iwasawa module. We are therefore hopeful that future studies will shed light on the remaining generators and also on the shape of relations up to higher levels of the lower ℓ-central series of F.

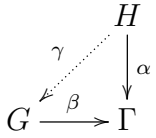
Acknowledgments. We thank Ido Efrat, Dan Haran, Jeffrey Lagarias, Jan Minac, James Milne, Kartik Prasanna, Jack Sonn, and Michael Zieve for helpful discussions, remarks and encouragement. The first author was supported by a Grant from the GIF, the German-Israeli Foundation for Scientific Research and Development. The third author was supported by a short term Minerva grant. This material is based upon work supported by the National Science Foundation under Award No. DMS-1303990.

2. Embedding problems

2.1. **Z-embedding problems.** Let Z be a profinite group. A profinite Z-group is a profinite group H together with a continuous Z-action. A Z-homomorphism $\phi\colon H_1 \to H_2$ is a continuous homomorphism that commutes with the Z-action. We say that a subgroup H_1 of a profinite Z-group H_2 is a Z-subgroup, if the inclusion map $H_1 \to H_2$ is a Z-homomorphism, that is, if H_1 is a closed subgroup that is closed under the action of Z. A Z-embedding problem for a Z-group H, denoted

by (α, β), is a diagram

(2)



in which G, Γ are profinite Z-groups and α, β are Z-epimorphisms. If $Z = 1$, we recover the usual notion of embedding problems for profinite groups. A **solution** of the Z-embedding problem is a homomorphism $\gamma\colon H \to G$ that commutes the above diagram. A solution is called **proper** if it is surjective. A Z-embedding problem is called **split** if β has a section which is Z-morphism. We define the **Z-Frattini** subgroup $\Phi_Z(G)$ of a Z-profinite group G to be the intersection of all maximal Z-subgroup. We call a Z-embedding problem, as above, **Frattini** if $\ker\beta \leq \Phi_Z(G)$. If G is finite (and hence so is Γ) we say that the Z-embedding problem is **finite**. In this work we will be interested in $Z = \mathbb{Z}_\ell$ or $Z = 1$.

Lemma 2.1. *If U is an open subgroup of a profinite Z-group H, then $U_Z = \bigcap_{z\in Z} zU$ is open in H.*

Proof. Since the action map $p\colon Z \times H \to H$ is continuous, $p^{-1}(U)$ is open. Thus there exist open normal subgroups $Z_0 \leq Z$ and $H_0 \leq H$ such that $p^{-1}(U)$ is a finite union of cosets of $Z_0 \times H_0$, say $p^{-1}(U) = \bigcup_{i=1}^n z_i Z_0 \times h_i H_0$. Thus

$$U_Z = \bigcap_{z\in Z} zU = \bigcap_{z\in Z} \bigcup_{i=1}^n z z_i Z_0 h_i H_0 = \bigcap_{z\in Z} \bigcup_{i=1}^n z_i z^{z_i} Z_0 h_i H_0 = \bigcap_{x\in Z/Z_0} \bigcup_{i=1}^n z_i x h_i H_0.$$

We conclude that U_Z is open as a finite intersection of open sets. □

Most of the basic theory of embedding problems carries over to Z-embedding problems. The proofs are similar to the classical proofs. For the sake of completeness, we prove the properties we shall need.

Lemma 2.2. *If $(\alpha\colon H \to \Gamma, \beta\colon G \to \Gamma)$ is a Frattini Z-embedding problem and if $\gamma\colon H \to G$ is a solution, then γ is proper.*

Proof. Let $U = \gamma(H)$. If $U \neq G$, then there is a maximal Z-subgroup V of G that contains U. So

$$\Gamma = \alpha(H) = \beta(\gamma(H)) = \beta(U) \leq \beta(V).$$

By the third isomorphism theorem this implies that $G = V \ker\beta$. Since (α, β) is Frattini, $\ker\beta \leq \Phi_Z(G) \leq V$. So $G = V\ker\beta \leq V\Phi_Z(G) \leq V \neq G$. This contradiction implies that $U = G$, as needed. □

The next lemma says that the study of solvability of embedding problems may be reduced to the study of Frattini and split embedding problems.

Lemma 2.3. *Consider a Z-embedding problem $\mathcal{E} = (\alpha\colon H \to \Gamma, \beta\colon G \to \Gamma)$ for a Z-profinite group H. Then there exists an open Z-subgroup U of G such that $\beta(U) = \Gamma$ and the following properties are satisfied:*

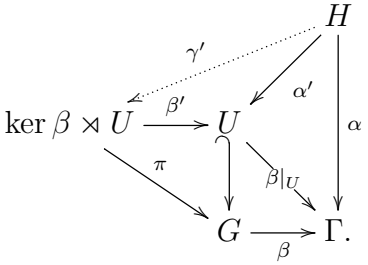
(a) *The Z-embedding problem $\mathcal{E}_U = (\alpha\colon H \to \Gamma, \beta|_U\colon U \to \Gamma)$ is Frattini.*
(b) *A solution $\alpha'\colon H \to U$ of $\mathcal{E}_U$ induces a split Z-embedding problem $\mathcal{E}' = (\alpha'\colon H \to U, \beta'\colon \ker\beta \rtimes U \to U)$, where U acts on $\ker\beta$ by conjugation in G.*
(c) *A proper solution $\gamma'\colon H \to \ker\beta \rtimes U$ of $\mathcal{E}'$ induce a proper solution $\gamma\colon H \to G$ of $\mathcal{E}$ by: $\gamma'(h) = (\sigma, u)$ implies $\gamma(h) = \sigma u$.*

Proof. A limit argument reduces the proof to finite Z-embedding problems.

Let U be minimal among the open Z-subgroups of G that map onto Γ. In particular $\beta(U) = \Gamma$. Since no proper Z-subgroup of U maps onto Γ, we have that $\ker(\beta|_U)$ is contained in each of the maximal Z-subgroup of U, hence $\ker(\beta|_U) \leq \Phi_Z(U)$. This proves (a).

If α' is a solution of $\mathcal{E}_U$, then it is proper by Lemma 2.2. To prove (b), it suffices to observe that $\ker\beta \rtimes U$ is a profinite Z-group with respect to the action $z(\sigma, u) = (z\sigma, zu)$ and that the projection map $\beta'\colon \ker\beta \rtimes U \to U$ is a Z-map.

Let $\pi\colon \ker\beta \rtimes U \to G$ defined by $\pi(\sigma, u) = \sigma u$. It is a Z-epimorphism that commutes in the diagram of Z-maps



Thus if γ' is a proper solution of $\mathcal{E}'$, then γ is a proper solution of $\mathcal{E}$, as needed for (c). □

Lemma 2.4. *Let H_1 be a Z-subgroup of a profinite Z-group H and let $\alpha_1\colon H_1 \to \Gamma$ be a Z-epimorphism on a finite Z-group Γ. Then there exists an open Z-subgroup H_2 of H that contains H_1 and an extension $\alpha_2\colon H_2 \to \Gamma$ of α_1.*

In particular any finite Z-embedding problem for H_1 is the restriction of a corresponding Z-embedding problem for an open subgroup of H that contains H_1.

Proof. The subgroup $U_1 = \ker\alpha_1$ is a normal open Z-subgroup of H_1. Then there exists an open normal subgroup U_2 of H such that $U_2 \cap H_1 \leq U_1$. By Lemma 2.1 we may replace U_2 by $\bigcap_{z\in Z} zU_2$ to assume that U_2 is a Z-subgroup.

Let $H_2 = U_2H_1$. Then H_2 is an open Z-subgroup of H that contains H_1. Let $\alpha_2\colon H_2 \to \Gamma$ be defined by $\alpha_2(u\sigma) = \alpha_1(\sigma)$ for all $u \in U_2$ and $\sigma \in H_1$. Then α_2 is well defined because it is trivial on $U_2 \cap H_1 \leq U_1$ and it is a Z-map because

its kernel U_2 is an open normal Z-subgroup. By definition $\alpha_2|_{H_1} = \alpha_1$, hence the assertion. □

We shall need the following two basic lemmas concerning Sylow subgroups of profinite groups:

Lemma 2.5. *Let ℓ be a prime number, Λ an ℓ-Sylow subgroup of G, and $\alpha\colon G \to H$ an epimorphism of profinite groups. Assume that H is pro-ℓ. Then $\alpha(\Lambda) = H$.*

Proof. The notation $[A : B]$ denotes the index of a subgroup B of a profinite group as a supernatural number, cf. [4, §22.8]. By the isomorphism theorems for profinite groups one has

$$[H : \alpha(\Lambda)] = [G : \Lambda \ker \alpha].$$

Since H is pro-ℓ the left hand side is a (supernatural) power of ℓ. Since Λ is an ℓ-Sylow subgroup, the right hand side, which divides $[G : \Lambda]$, is prime to ℓ. Hence $[H : \alpha(\Lambda)] = 1$, as needed. □

Lemma 2.6. *Let ℓ be a prime number and H a normal subgroup of a profinite group G. Assume $[G : H]$ is prime to ℓ. Then H contains all ℓ-Sylow subgroups of G.*

Proof. Let Λ be an ℓ-Sylow subgroup of H. Then $[G : \Lambda] = [G : H][H : \Lambda]$ is prime to ℓ and so Λ is an ℓ-Sylow subgroup of G. Since H is normal, also $\Lambda^\sigma \le H$ for all $\sigma \in G$. By the Sylow theorem every ℓ-Sylow subgroup of G is of the form Λ^σ, hence the assertion. □

Next we deal with restriction of embedding problems from Sylow subgroups.

Lemma 2.7. *Let ℓ be a prime number, H a profinite group, Λ an ℓ-Sylow subgroup, and $\mathcal{E}_\ell = (\alpha\colon \Lambda \to \Gamma, \beta\colon G \to \Gamma)$ a finite embedding problem with G an ℓ-group. Let $\mathcal{U}$ be the family of pairs (U, α_U) where U is an open subgroups of H containing Λ and $\alpha_U\colon U \to G$ extends α.*

(a) *If there exists $(U, \alpha_U) \in \mathcal{U}$ such that $\mathcal{E}_U = (\alpha_U\colon U \to \Gamma, \beta\colon G \to \Gamma)$ has a solution $\gamma_U\colon U \to G$, then $\gamma = (\gamma_U)|_\Lambda$ is a solution of $\mathcal{E}$. Moreover if γ_U is proper, then γ is proper.*

(b) *If $\ker \alpha$ is abelian and if $\mathcal{E}$ is solvable, then $\mathcal{E}_U$ is solvable.*

Proof. The first assertion of (a), that γ is a solution of $\mathcal{E}$, is trivial. The second assertion of (a) follows from Lemma 2.5.

Now we assume that $A = \ker \alpha$ is abelian and that $\mathcal{E}$ is solvable. Denote by b the class in $H^2(\Gamma, A)$ that corresponds to the extension

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\beta} \Gamma \longrightarrow 1$$

and write $\alpha^*\colon H^2(\Gamma, A) \to H^2(\Lambda, A)$ for the inflation map. Then by Hoechsmann's theorem [16, Proposition 9.4.2], $\alpha^*(b) = 0$.

Let $(U, \alpha_U) \in \mathcal{U}$ and let $i\colon \Lambda \to U$ be the inclusion map. Then $0 = \alpha^*(b) = (\alpha_U \circ i)^*(b) = i^* \circ \alpha_U^*(b)$. Since $|A|$ is a power of ℓ and since $[U : \Lambda] \mid [H : \Lambda]$, hence prime to ℓ, it follows that i^* is injective. So $\alpha_U^*(b) = 0$ and consequently $\mathcal{E}_U$ is solvable by [16, Proposition 9.4.2]. □

We get a field theoretic application of the latter result.

Proposition 2.8. *Let ℓ be a prime, let K be a Hilbertian field, let $K^{(\ell)}$ be a separable extension of K such that $\mathrm{Gal}(K^{(\ell)})$ is an ℓ-Sylow subgroup of $\mathrm{Gal}(K)$, and let $\mathcal{E} = (\alpha\colon \mathrm{Gal}(K^{(\ell)}) \to \Gamma, \beta\colon G \to \Gamma)$ be a finite embedding problem. Assume that G is an ℓ-group, $\ker\alpha$ is abelian, and $\mathcal{E}$ is solvable. Then $\mathcal{E}$ is properly solvable.*

Proof. By Lemma 2.7 there exists an open subgroup U of $\mathrm{Gal}(K)$ that contains $\mathrm{Gal}(K^{(\ell)})$ and an extension $\alpha_U\colon U \to \Gamma$ of α such that the embedding problem $\mathcal{E}_U = (\alpha_U, \beta)$ is solvable. By Galois correspondence $U = \mathrm{Gal}(L)$ for a finite subextension L of $K^{(\ell)}/K$. In particular L is Hilbertian [4, Corollary 12.2.3]. Ikeda's theorem [5] implies that $\mathcal{E}_U$ is properly solvable, hence by Lemma 2.7, $\mathcal{E}$ is properly solvable. □

We shall also need the following technical lemma:

Lemma 2.9. *Let G be a profinite group, let N and P be closed subgroups, and put $F = N \cap P$. Assume that $N \lhd G$, $G = NP$, and $P = F \rtimes Z$, for some $Z \leq P$. Then $G = N \rtimes Z$.*

Proof. Since $N \cap Z = N \cap P \cap Z = F \cap Z = 1$ and $NZ = NFZ = NP = G$, we get the assertion. □

3. The cyclotomic decomposition

Let K be a global field, ℓ a prime number, and $K^{(\ell)}$ the fixed field of an ℓ-Sylow subgroup of $\mathrm{Gal}(K)$.

Let K be a global field and $\tilde{K}$ an algebraic closure of K. For a prime $\mathfrak{p}$ of $K^{(\ell)}$ denote the completion of $K^{(\ell)}$ at $\mathfrak{p}$ by $K_{\mathfrak{p}}^{(\ell)}$. Choosing an embedding of $\tilde{K}$ into an algebraic closure $\tilde{K}_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$, the restriction map induces an embedding of $\mathrm{Gal}(K_{\mathfrak{p}}) = \mathrm{Gal}(\tilde{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$ into $\mathrm{Gal}(K^{(\ell)})$. We identify $\mathrm{Gal}(K_{\mathfrak{p}})$ with its image in $\mathrm{Gal}(K^{(\ell)})$. Thus an embedding problem $(\phi\colon \mathrm{Gal}(K^{(\ell)}) \to \Gamma, \pi\colon G \to \Gamma)$ for $K^{(\ell)}$ induces a *local* embedding problem at $\mathfrak{p}$, namely

$$(\phi_{\mathfrak{p}}\colon \mathrm{Gal}(K_{\mathfrak{p}}^{(\ell)}) \to \Gamma_{\mathfrak{p}}, \pi_{\mathfrak{p}}\colon G_{\mathfrak{p}} \to \Gamma_{\mathfrak{p}}),$$

where $\phi_{\mathfrak{p}} = \phi|_{\mathrm{Gal}(K^{(\ell)}{}_{\mathfrak{p}})}$, $\Gamma_{\mathfrak{p}}$ is the image and $\phi_{\mathfrak{p}}$, $G_{\mathfrak{p}} = \pi^{-1}(\Gamma_{\mathfrak{p}})$, and $\pi_{\mathfrak{p}} = \pi|_{G_{\mathfrak{p}}}$. We shall abuse notation and denote the local embedding problem by $(\phi_{\mathfrak{p}}, \pi)$.

Although local embedding problems in the Sylow setting may be unsolvable, they are solvable after restriction to *any* proper extension:

Proposition 3.1. *Let K be a local field, $\ell \neq \mathrm{char}(K)$ a prime number such that either ℓ is odd or $\sqrt{-1} \in K$. Let $(\phi\colon \mathrm{Gal}(K) \to \Gamma, \pi\colon G \to \Gamma)$ be an embedding problem for K such that G is an ℓ-group and $\ker\pi = C_\ell$. Then for every proper extension $L/K^{(\ell)}$, the restriction of (ϕ,π) to L is solvable.*

Proof. We may replace L by a subfield of it to assume $L/K^{(\ell)}$ is a finite proper extension. By Lemma 2.4 there exists a finite extension K_0/K and an embedding problem $(\phi_0\colon \mathrm{Gal}(K_0) \to \Gamma, \pi)$ such that (ϕ,π) is the restriction of (ϕ_0,π). We may replace K_0 by $K_0(\mu_\ell)$ to assume that $\mu_\ell \subseteq K_0$. Let L_0/K_0 be a finite extension such that $L_0K^{(\ell)} = L$. Then $[L : K^{(\ell)}] \,|\, [L_0 : K_0]$ so $\ell \,|\, [L_0 : K_0]$.

Since $\ker\pi$ is of order ℓ and since Γ is an ℓ-group, the action of $\mathrm{Gal}(K_0)$ on $\ker\pi$ via the action of Γ is trivial. As $\mu_\ell \subseteq K_0$, μ_ℓ is also a trivial $\mathrm{Gal}(K_0)$-module and hence $\ker\pi \cong \mu_\ell$ as $\mathrm{Gal}(K_0)$-modules. Thus, π defines a class $\alpha_\pi \in \mathrm{H}^2(\Gamma,\mu_\ell)$. By Hoechsmann's theorem [16, Proposition 9.4.2], (ϕ_0,π) is solvable if and only if the image of α_π under the inflation map

$$\phi_0^* : \mathrm{H}^2(\Gamma,\mu_\ell) \to \mathrm{H}^2(\mathrm{Gal}(K_0),\mu_\ell)$$

is trivial.

It is well known that the group $\mathrm{H}^2(\mathrm{Gal}(K_0),\mu_\ell)$ identifies with the ℓ-torsion of the Brauer group $\mathrm{Br}(K_0)[\ell]$ which is isomorphic via the natural invariant map inv_{K_0} to $\frac{1}{\ell}\mathbb{Z}/\mathbb{Z}$, [20]. Moreover, we get the following commutative diagram:

$$\begin{array}{ccccc} \mathrm{H}^2(\Gamma,\mu_\ell) & \xrightarrow{\phi_0^*} & \mathrm{Br}(K_0)[\ell] & \xrightarrow{\mathrm{inv}_{K_0}} & (\frac{1}{\ell}\mathbb{Z})/\mathbb{Z} \\ & \searrow^{\phi_1^*} & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \cdot[L_0:K_0]} \\ & & \mathrm{Br}(L_0)[\ell] & \xrightarrow{\mathrm{inv}_{L_0}} & (\frac{1}{\ell}\mathbb{Z})/\mathbb{Z} \end{array} \tag{3}$$

where ϕ_1 is the restriction of ϕ_0 to $\mathrm{Gal}(L_0)$ and the vertical maps are restriction and multiplication by $[L_0 : K_0]$, respectively. Since $\ell \,|\, [L_0 : K_0]$, the vertical maps are the zero maps. In particular, $\phi_1^*(\alpha_\pi) = \mathrm{res} \circ \phi_0^*(\varepsilon) = 0$. Thus, (ϕ_1,π) is solvable and hence its restriction (ϕ,π) to L is solvable. □

For every positive integer k let μ_{ℓ^k} be the group of ℓ^k-th roots of unity and $\mu_{\ell^\infty} = \bigcup_{k=1} \mu_{\ell^k}$ be the group of all ℓ-power roots of unity.

Proposition 3.2. *Let K be a global field, $\ell \neq \mathrm{char}(K)$ a prime number such that either ℓ is odd or $\sqrt{-1} \in K$. Let $(\phi\colon \mathrm{Gal}(K^{(\ell)}) \to \Gamma, \pi\colon G \to \Gamma)$ be an embedding problem for $K^{(\ell)}$ such that G is an ℓ-group. Then the restriction (ϕ_ℓ,π) of (ϕ,π) to $K^{(\ell)}(\mu_{\ell^\infty})$ is properly solvable.*

Proof. Since $\mu_\ell \subseteq K^{(\ell)}$, we may replace K by $K(\mu_\ell)$ to assume without loss of generality that $\mu_\ell \subseteq K$. If π is an isomorphism, then (ϕ_ℓ,π) is clearly properly solvable, hence we assume that $\ker\pi$ is nontrivial.

We proceed by induction on the order of $|G|$. Since G is an ℓ-group, $\ker\pi$ contains a subgroup of order ℓ which is normal in G. Thus π decomposes as

$\pi_C \circ \pi'$ where $\pi' \colon G \to G/C$ is the natural projection and $\pi_C \colon G/C \to \Gamma$. Let $L := K^{(\ell)}(\mu_{\ell^\infty})$. Since $|G/C| < |G|$, the induction assumption gives a proper solution $\psi' \colon \mathrm{Gal}(L) \to G/C$ of (ϕ, π_C). It therefore suffices to show that (ψ', π') has a proper solution ψ, since then $\pi \circ \psi = \pi_C \circ \pi' \circ \psi = \pi_C \circ \psi' = \phi$ and so ψ properly solves (ϕ, π).

Let $\alpha_{\pi'} \in \mathrm{H}^2(G/C, C)$ be the element corresponding to the group extension π', and consider its image in the following commutative diagram:

$$\begin{array}{ccc} \mathrm{H}^2(G/C, C) & & \\ {\scriptstyle (\psi')^*}\downarrow & \searrow^{\prod (\psi'_{\mathfrak{q}})^*} & \\ \mathrm{H}^2(\mathrm{Gal}(L), C) & \xrightarrow{\mathrm{res}} & \prod_{\mathfrak{q}} \mathrm{H}^2(\mathrm{Gal}(L_{\mathfrak{q}}), C), \end{array} \tag{4}$$

where $(\psi')^*, (\psi'_{\mathfrak{q}})^*$ are inflation maps, and the products are taken over all primes $\mathfrak{q}$ of L. By the Albert-Brauer-Hasse-Noether theorem the restriction map

$$\mathrm{H}^2(\mathrm{Gal}(K'), \mu_\ell) \to \prod_{\mathfrak{p}} \mathrm{H}^2(\mathrm{Gal}(K'_{\mathfrak{p}}), \mu_\ell),$$

is injective for every global field K', where $\mathfrak{p}$ runs over all primes of K'. Taking an inductive limit which runs over all global fields $K' \subseteq L$, and noting that $C \cong \mu_\ell$ as trivial $\mathrm{Gal}(L)$-modules, we deduce that the restriction map in (4) is injective. Thus, as we $(\psi')^*(\alpha_{\pi'}) = 0$ if $(\psi'_{\mathfrak{q}})^*(\alpha_{\pi'}) = 0$. Thus, by Hoechsmann's theorem [16, Proposition 9.4.2], (ψ', π') is solvable if $(\psi'_{\mathfrak{q}}, \pi')$ is solvable for every prime $\mathfrak{q}$ of L.

By Lemma 2.4 there exists a finite subextension $K^{(\ell)}(\mu_{\ell^r})$, $r > 0$, of $K^{(\ell)}(\mu_{\ell^\infty})/K$ and an extension $\psi'' \colon \mathrm{Gal}(K^{(\ell)}(\mu_{\ell^r})) \to G/C$ of ψ' such that (ψ', π') is the restriction of the finite embedding problem (ψ'', π').

Let $\mathfrak{p}$ be a prime of $K^{(\ell)}(\mu_{\ell^r})$. Since the degree of the extension $K^{(\ell)}_{\mathfrak{p}}(\mu_{\ell^r})/K_{\mathfrak{p}}(\mu_{\ell^r})$ is prime to ℓ, $K^{(\ell)}_{\mathfrak{p}}(\mu_{\ell^r})$ contains only finitely many ℓ-power roots of unity and hence $K^{(\ell)}_{\mathfrak{p}}(\mu_{\ell^\infty})/K^{(\ell)}_{\mathfrak{p}}(\mu_{\ell^r})$ is a proper extension. Proposition 3.1 implies that the restriction of (ψ', π') to $L_{\mathfrak{q}}$ is solvable for any prime $\mathfrak{q}$ dividing $\mathfrak{p}$. Thus, (ψ', π') is solvable as its local embedding problems are solvable. As $K(\mu_{\ell^\infty})$ is an abelian extension of a global field, it is Hilbertian by Kuyuk's theorem [4, Theorem 16.11.3], and hence Proposition 2.8 implies that (ψ', π') is properly solvable.

□

Theorem 1.1 is a special case of the following theorem:

Theorem 3.3. *Let K be a global field and $\ell \neq \mathrm{char}(K)$ a prime. If $\ell = 2$ and K is a number field, assume further that $K \cap \mathbb{Q}(\mu_{\ell^\infty})$ is (totally) imaginary. Then $\mathrm{Gal}(K^{(\ell)}) \cong F \rtimes Z$, where $Z = \mathrm{Gal}(K^{(\ell)}(\mu_{\ell^\infty})/K^{(\ell)}) \cong \mathbb{Z}_\ell$ and $F = \mathrm{Gal}(K^{(\ell)}(\mu_{\ell^\infty}))$ is a free pro-p group on countably many generators.*

Proof. Let (ϕ, π) be a finite embedding problem over $K^{(\ell)}(\mu_{\ell^\infty})$. By Lemma 2.4, there is a finite embedding problem (ϕ_0, π) over $K^{(\ell)}(\mu_r)$, for some $r \geq 0$, whose

restriction to $K^{(\ell)}$ is (ϕ, π). Therefore by Proposition 3.2, (ϕ, π) is properly solvable. Thus, its absolute Galois group F is a free pro-ℓ group on countably many generators [21]. Thus the restriction map gives rise to a short exact sequence

$$1 \longrightarrow F \longrightarrow \mathrm{Gal}(K^{(\ell)}) \xrightarrow{\alpha} Z \longrightarrow 1. \tag{5}$$

Set $Z = \mathrm{Gal}(K^{(\ell)}(\mu_{\ell^\infty})/K^{(\ell)})$. Since $\mu_\ell \subseteq K^{(\ell)}$, and since $K \cap \mathbb{Q}(\mu_{\ell^\infty})$ is (totally) imaginary if $\ell = 2$ and K is a number field, we have $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/K \cap \mathbb{Q}(\mu_{\ell^\infty})) \cong \mathbb{Z}_\ell$. Thus, $Z \cong \mathbb{Z}_\ell$ as a nontrivial subgroup. Since $\mathbb{Z}_\ell$ is projective in the category of pro-ℓ groups, (5) splits and its splitting gives an isomorphism $\mathrm{Gal}(K^{(\ell)}) \cong F \rtimes Z$. □

For $\ell = 2$, if K has a real prime, then the sequence

$$1 \longrightarrow \mathrm{Gal}(K(\mu_{\ell^\infty})) \longrightarrow \mathrm{Gal}(K^{(\ell)}) \xrightarrow{\alpha} \mathrm{Gal}(K(\mu_{\ell^\infty})/K) \longrightarrow 1$$

does not split.

Otherwise, there is an embedding of $\mathrm{Gal}(K(\mu_{\ell^\infty})/K) \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ into $\mathrm{Gal}(K)$. But this is impossible since the normalizer of an involution τ in an absolute Galois group is exactly $\langle \tau \rangle$, cf. [1, Proposition 19.4.3(b)].

Corollary 3.4. *Let K be a number field equipped with a real prime. Then*

$$\mathrm{Gal}(K^{(2)}) \cong (F \rtimes \mathbb{Z}_2) \rtimes \mathbb{Z}/2,$$

where F is a free pro-2 group on countably many generators.

Proof. By Theorem 1.1, we have $\mathrm{Gal}(K^{(2)}(\sqrt{-1})) \cong F \rtimes \mathbb{Z}_2$. Since K has a real place, there is an embedding of $\overline{K}$ into $\mathbb{C}$ such that the complex conjugation τ fixes K. Thus, the restriction of τ to $\overline{K}$ is an involution which restricts to the nontrivial automorphism of $K^{(2)}(\sqrt{-1})/K^{(2)}$. This gives a splitting of the extension

$$1 \longrightarrow F \rtimes \mathbb{Z}_2 \longrightarrow \mathrm{Gal}(K^{(2)}) \longrightarrow \mathrm{Gal}(K^{(2)}(\sqrt{-1})/K^{(2)}) \longrightarrow 1,$$

proving the desired result. □

If K is totally imaginary but $K \cap \mathbb{Q}(\mu_{2^\infty})$ is totally real, by Artin's theorem $\mathrm{Gal}(K^{(2)})$ has no involutions and hence even the sequence

$$1 \to F \rtimes \mathbb{Z}_2 \to \mathrm{Gal}(K^{(2)}) \to \mathrm{Gal}(K^{(2)}(\sqrt{-1})/K^{(2)}) \to 1,$$

does not split.

4. The action via Z-embedding problems

In this section we study the action in the cyclotomic decomposition via Z-embedding problems. We consider the following more general setup. Let K be a Hilbertian field and $\ell \neq \mathrm{char}\, K$ a prime number. If $\ell = 2$ and $\mathrm{char}\, K = 0$, assume that $\sqrt{-1} \in K$. As before set $L = K^{(\ell)}(\mu_{\ell^\infty})$, $Z = \mathrm{Gal}(L/K^{(\ell)})$, and $F = \mathrm{Gal}(L)$. Theorem 1.2 is then a special case of:

Theorem 4.1. *Every finite split Z-embedding problem for F is properly solvable.*

To prove the theorem we first deal with split embedding problems for $\mathrm{Gal}(K^{(\ell)})$:

Proposition 4.2. *Let $(\phi\colon \mathrm{Gal}(K^{(\ell)}) \to \Gamma, \pi\colon G \to \Gamma)$ be a finite split embedding problem for $\mathrm{Gal}(K^{(\ell)})$ with G an ℓ-group. Then (ϕ, π) is properly solvable.*

Proof. Let N be the fixed field of $\ker\phi$, and so $N/K^{(\ell)}$ is Galois and the map ϕ decomposes as $\phi = \phi' \circ r$, where $r\colon \mathrm{Gal}(K^{(\ell)}) \to \mathrm{Gal}(N/K^{(\ell)})$ is the restriction map and $\phi'\colon \mathrm{Gal}(N/K^{(\ell)}) \to \Gamma$ is an isomorphism. We may replace Γ by $\mathrm{Gal}(N/K^{(\ell)})$ and the maps π, ϕ by $(\phi')^{-1}\circ\pi$ and r, respectively, to assume that $\Gamma = \mathrm{Gal}(N/K^{(\ell)})$ and ϕ is the restriction map.

By [10, Theorem 5.8.3] $K^{(\ell)}$ is ample. Hence by [10, Theorem 5.9.2] there exist a Galois extension $F/K^{(\ell)}(x)$ such that $\mathrm{Gal}(F/K^{(\ell)}(x)) \cong G$, N is the algebraic closure of K in F, and the restriction map $\mathrm{Gal}(F/K^{(\ell)}(x)) \to \Gamma$ coincides with π (after the identification $\mathrm{Gal}(F/K^{(\ell)}(x)) = G$).

Let K_0 be a finite subextension of $K^{(\ell)}(x)/K$ to which the above descends to as follows: there exist N_0/K_0 Galois with Galois group Γ such that $N = N_0K^{(\ell)}$ and $F_0/K_0(x)$ Galois with group G such that $F = F_0K^{(\ell)}$, N_0 is the algebraic closure of K_0 in F_0, $G = \mathrm{Gal}(F_0/K_0(x))$ and the restriction map $\mathrm{Gal}(F_0/K(x)) \to \mathrm{Gal}(N_0/K_0)$ coincides with π.

Note that K_0 is Hilbertian as a finite extension of K [4, Proposition 16.11.1]. Hence there exists $a \in K_0$ such that the prime $(x-a)$ of $K_0(x)$ is inert in F_0. Let M be the residue field of F_0 at $x = a$. Then M/K_0 is Galois with Galois group G, $N_0 \subseteq M$, and the restriction map $\mathrm{Gal}(M/K_0) \to \mathrm{Gal}(N_0/K_0)$ coincides with π. In other words, if $\phi_0\colon \mathrm{Gal}(K_0) \to \mathrm{Gal}(M/K_0) = G$ and $\psi\colon \mathrm{Gal}(K_0) \to \mathrm{Gal}(M/K_0)$ are the restriction maps, then ψ is a proper solution of (ϕ_0, π). Then $\psi|_{\mathrm{Gal}(K^{(\ell)})}$ is a solution of (ϕ, π) which is proper by Lemma 2.5. □

Proof of Theorem 4.1. Let $(\phi\colon F \to G, \pi\colon G \to \Gamma)$ be a finite split Z-embedding problem with G an ℓ-group. Since $\mathrm{Gal}(K^{(\ell)}) = F \rtimes Z$, we may extend (ϕ, π) to a split embedding problem

$$(\phi'\colon F \rtimes Z \to \Gamma \rtimes Z, \pi'\colon G \rtimes Z \to \Gamma \rtimes Z)$$

for $\mathrm{Gal}(K^{(\ell)})$, where $\phi'(x, z) = (\phi(x), \phi(z))$ and $\pi'(g, z) = (\pi(g), z)$, for every $x \in F$, $z \in Z$, and $g \in G$.

Since Z acts on the finite group G continuously, the kernel of the action is an open subgroup of Z, say $\ell^r Z$, $r \geq 0$. Composing with the natural projection $Z \to Z/\ell^r Z$ we obtain a finite embedding problem

$$(\phi''\colon F \rtimes Z \to \Gamma \rtimes (Z/\ell^r Z), \pi''\colon G \rtimes (Z/\ell^r Z) \to \Gamma \rtimes (Z/\ell^r Z))$$

for $K^{(\ell)}$ and we have the commutative diagram of profinite groups

(6)
$$\begin{array}{ccc} & & F \rtimes Z \\ & & \downarrow{\scriptstyle \phi'} \quad \searrow{\scriptstyle \phi''} \\ G \rtimes Z & \xrightarrow{\pi'} & \Gamma \rtimes Z \\ \downarrow & & \downarrow \\ G \rtimes (Z/\ell^r Z) & \xrightarrow{\pi''} & \Gamma \rtimes (Z/\ell^r Z). \end{array}$$

By Proposition 4.2 the embedding problem (ϕ'', π'') has a proper solution, say $\psi''\colon F \rtimes Z \to G \rtimes (Z/\ell^r Z)$. We note that $G \rtimes Z$ is the fiber product of $\Gamma \rtimes Z$ and $G \rtimes (Z/\ell^r Z)$ over $\Gamma \rtimes (Z/\ell^r Z)$. So $\psi' = \psi'' \times \phi'$ is a solution of (ϕ', π'). Clearly ψ' is surjective, hence it is a proper solution. Restricting ψ' to F yields a solution $\psi\colon F \to G$ of the Z-embedding problem (ϕ, π). □

As oppose to split embedding problems, Frattini Z-embedding problems need not be solvable. We now descend these problems to cyclotomic extensions of number fields.

For a number field $K(\mu_\ell) \subseteq K' \subseteq K^{(\ell)}$, Lemma 2.9 shows that the splitting $\mathrm{Gal}(K^{(\ell)}) = \mathrm{Gal}(L) \rtimes Z$ induces a splitting $\mathrm{Gal}(K') = \mathrm{Gal}(K'(\mu_{\ell^\infty})) \rtimes Z$ such that the restriction map $\mathrm{Gal}(L) \to \mathrm{Gal}(K'(\mu_{\ell^\infty}))$ is a Z-homomorphism.

Proposition 4.3. *Let $(\phi : \mathrm{Gal}(L) \to \Gamma, \pi)$ be a Z-embedding problem. Then there is a number field $K(\mu_\ell) \subseteq K' \subseteq K^{(\ell)}$ and a Z-embedding problem*

$$(\phi' : \mathrm{Gal}(K'(\mu_{\ell^\infty})) \to \Gamma, \pi)$$

whose restriction to L is (ϕ, π). Furthermore, for every such K' and ϕ', (ϕ, π) is solvable if and only if (ϕ', π) is solvable. In particular, if π is Z-Frattini, (ϕ, π) is properly solvable if and only if (ϕ', π) is properly solvable.

Proof. Let $N := \mathrm{Gal}(K(\mu_{\ell^\infty}))$ be a Z-group via the induced splitting $\mathrm{Gal}(K(\mu_\ell)) = N \rtimes Z$. By Lemma 2.4, ϕ extends to $\phi' : U \to \Gamma$ for some open Z-subgroup $U \leq N$. Let K' be the fixed field of $U \rtimes Z$. Since $UZ = U\mathrm{Gal}(L)Z \supseteq \mathrm{Gal}(K^{(\ell)})$, we have $K' \subseteq K^{(\ell)}$. Since $U \rtimes Z$ is open in $\mathrm{Gal}(K(\mu_\ell))$, K' is a number field. Since $U \leq N$, μ_{ℓ^∞} is fixed by U and $K'(\mu_{\ell^\infty})$ is the fixed field of U. Thus, ϕ' is the desired Z-homomorphism. The equivalence for solvability follows by Proposition 2.2. The equivalence for proper solvability follows by Proposition 2.8. □

Explicit examples of non-solvable Z-Frattini embedding problems appear in the following section (Proposition 5.7).

5. Action on $F/F^\ell[F, F]$

Let $\mathrm{Gal}(K^{(\ell)}) = F \rtimes Z$ be the cyclotomic decomposition for a global field K and a prime $\ell \neq \mathrm{char}\, K$. If K is a number field and $\ell = 2$ we assume $\sqrt{-1} \in K$.

Recall that $Z = \mathrm{Gal}(L/K^{(\ell)}) \cong \mathbb{Z}_\ell$ and $F = \mathrm{Gal}(L)$ is a free pro-ℓ group, where $L = K^{(\ell)}(\mu_{\ell^\infty})$. Letting $\overline{F} = F/F^\ell[F,F]$, Theorem 1.3 follows from:

Theorem 5.1. *For any positive integer N the Z-group $\overline{F}$ decomposes as $\overline{F} = V_{\leq N} \times V_{>N}$ where:*

$$V_{\leq N} \cong \mathbb{F}_\ell[[Z]]^\omega \times \prod_{n=1}^{N} \mathbb{F}_\ell[Z/\ell^n Z]^\omega$$

and $V_{>N}$ has no Z-summands of dimension $\leq \ell^N$ over $\mathbb{F}_\ell$, nor Z-summands Z-isomorphic to $\mathbb{F}_\ell[[Z]]$. Moreover, $V_{\leq N}$ is a Z-summand of $V_{\leq N+1}$ for all N.

To prove Theorem 5.1, we first utilize based on [7, §11,12] the theory of Ulm invariants for countably generated ℓ-torsion profinite Z-modules.

5.1. **Z-modules.** Let M be a countably generated profinite ℓ-torsion Z-module or equivalently a profinite module over $\mathbb{F}_\ell[[Z]]$. The ring $\mathbb{F}_\ell[[Z]]$ is a discrete valuation ring with the augmentation ideal I as a maximal ideal. Hence $I^n M, n \in \mathbb{N}$, is a fundamental system of open neighborhoods of $0 \in M$.

As M is profinite its (Pontryagin) dual $\hat{M} := \mathrm{Hom}(M, \mathbb{F}_\ell)$ is a discrete $\mathbb{F}_\ell[[Z]]$-module with action $(\tau f)(m) = f(\tau^{-1} m)$ for all $m \in M, \tau \in Z$, and $f \in \hat{M}$. Moreover, $\hat{M}$ is $\mathbb{F}_\ell[[Z]]$-torsion since every homomorphism $f \in \hat{M}$ factors through $M/I^n M$ for some $n \in \mathbb{N}$, and hence $I^n f = 0$.

It follows by [7, §12] that the structure of $\hat{M}$ and hence of M is determined by Ulm invariants and the maximal free $\mathbb{F}_\ell[[Z]]$-quotient of M as follows.

Definition 5.2. For a discrete torsion $\mathbb{F}_\ell[[Z]]$-module N, let N^Z be the Z-submodule of all element of N fixed by Z, or equivalently annihilated by I. Consider the descending sequence

$$N \supseteq IN \supseteq I^2 N \supseteq \cdots \supseteq I^n N \supseteq \cdots$$

whose intersection we denote by $N_\omega := \cap_{n \in \mathbb{N}} I^n N$. The **Ulm invariant** $U_n(N)$ is the cardinality of $(I^n N)^Z/(I^{n+1}N)^Z$ for $n \in \mathbb{N}$. The **infinite Ulm invariants** are the Ulm invariants of N_ω.

The finite Ulm invariants $U_n(\hat{M})$ already determine the finite Z-summands of M, as follows. Since $\mathbb{F}_l[[Z]]$ is a complete discrete valuation ring, there is a unique indecomposable $\mathbb{F}_\ell[[Z]]$-module $V_n = \mathbb{F}_\ell[[Z]]/I^n$ of dimension n over $\mathbb{F}_\ell$. Note that for a generator σ of Z, $(\sigma - 1)^{\ell^k} = \sigma^{\ell^k} - 1$. Thus, $I^{\ell^k} = (\sigma^{\ell^k} - 1)$ and hence:

$$V_{\ell^k} \cong \mathbb{F}_\ell[Z/\ell^k Z], \tag{7}$$

for every $k \in \mathbb{N}$.

Proposition 5.3. *Let M be a profinite Z-module. Then:*

(a) *For $n \in \mathbb{N}$, $U_{n-1}(\hat{M})$ is the multiplicity of V_n as a direct Z-summand of M. Furthermore, for every $N \in \mathbb{N}$, $M = M_{\leq N} \times M_{>N}$, where*

$$M_{\leq N} \cong \mathbb{F}_\ell[[Z]]^k \times \prod_{n \leq N} V_n^{U_{n-1}(\hat{M})},$$

$M_{>N}$ has no free $\mathbb{F}_\ell[[Z]]$-quotients and no direct Z-summands of dimension $\leq N$ over $\mathbb{F}_\ell$. Moreover, $M_{\leq N}$ can be chosen to be a direct Z-summand of $M_{\leq N+1}$ for all $N \in \mathbb{N}$.

(b) *The limit $\varprojlim M_{\leq N}$, with respect to the natural projections $M_{\leq N+1} \to M_{\leq N}$, is isomorphic to M if and only if the infinite Ulm invariants of $\hat{M}$ are trivial.*

Proposition 5.3 follows from the theory of discrete torsion $\mathbb{F}_\ell[[Z]]$-modules and its proof is given in §5.9.

The finite Ulm invariants of $\hat{M}$ can be computed using Z-embedding problems as follows. Let $\pi_{n,m} : V_n \to V_m$, $\pi : \mathbb{F}_l[[Z]] \to V_1$ be the natural projections, and $\pi_n := \pi_{n,1}$, for positive integers $n \geq m$. For a profinite ℓ-torsion Z-module M, let $\hat{M}^Z$ be the group of Z-invariant homomorphisms $\mathrm{Hom}_Z(M, V_1)$.

Proposition 5.4. *Let M be a profinite $\mathbb{F}_\ell[[Z]]$-module, and $\phi \in \hat{M}^Z$. Then:*

(a) *For every $n \in \mathbb{N}$, $\phi \in I^n\hat{M}$ if and only if the embedding problem (ϕ, π_{n+1}) is solvable.*

(b) *The map ϕ factors through the maximal free quotient of M if and only if the embedding problem (ϕ, π) is solvable.*

The proof of Proposition 5.4 appears in §5.8. For $\phi \in \hat{M}^Z$, we define **the height** $\mathrm{ht}(\phi)$ to be the maximal n for which (ϕ, π_{n+1}) is solvable if such an n exists, and ∞ otherwise. In particular, Proposition 5.4 gives:

$$U_n(\hat{M}) = \left| \{\phi \in \hat{M}^Z \mid \mathrm{ht}(\phi) \geq n\} / \{\phi \in \hat{M}^Z \mid \mathrm{ht}(\phi) > n\} \right|, \tag{8}$$

and

$$(\hat{M})^Z_\omega = \{\phi \in \hat{M}^Z \mid \mathrm{ht}(\phi) = \infty\} \tag{9}$$

5.2. **A local global principle.** In view of (7) and Proposition 5.3, the proof of Theorem 5.1 reduces to finding the maximal free $\mathbb{F}_\ell[[Z]]$-quotient of $\overline{F}$ and the finite Ulm invariants of $\hat{F}$. To find the latter, we establish a local global principle for Z-embedding problems of the form

$$(\phi : \overline{F} \to V_n, \pi_{m,n} : V_m \to V_n).$$

For a prime $\mathfrak{p}$ of L, let $Z_\mathfrak{p}$ be the local Galois group $\mathrm{Gal}(L_\mathfrak{p}/K_\mathfrak{p}^{(\ell)})$. Since $\mathrm{Gal}(L_\mathfrak{p})$ is a $Z_\mathfrak{p}$-group, the restriction $(\phi_\mathfrak{p} : \mathrm{Gal}(L_\mathfrak{p}) \to V_n, \pi_{m,n})$ of (ϕ, π) to $L_\mathfrak{p}$ is a $Z_\mathfrak{p}$-embedding problem. Furthermore, if $\psi : \mathrm{Gal}(L) \to V_n$ is a solution to $(\phi, \pi_{m,n})$

then the restriction $\psi_{\mathfrak{p}} : \mathrm{Gal}(L_{\mathfrak{p}}) \to V_n$ is a solution to $(\phi_{\mathfrak{p}}, \pi_{m,n})$ for every prime $\mathfrak{p}$ of L. We claim that the converse also holds:

Proposition 5.5. *A Z-embedding problem $(\phi : \mathrm{Gal}(L) \to V_n, \pi_{m,n})$ of Z-groups satisfies the local global principle. That is, $(\phi, \pi_{m,n})$ is solvable if and only if $(\phi_{\mathfrak{p}}, \pi_{m,n})$ is solvable for every prime $\mathfrak{p}$ of L. In particular,* $\mathrm{ht}(\phi) = \min_{\mathfrak{p}} \mathrm{ht}(\phi_{\mathfrak{p}})$ *where $\mathfrak{p}$ runs over all primes of L.*

Proof. It suffices to prove the "if" implication. By Proposition 4.3, there is a global field $K(\mu_\ell) \le K' \le K^{(\ell)}$ such that ϕ extends to a Z-homomorphism $\phi' : \mathrm{Gal}(L') \to V_n$, where $L' := K'(\mu_{\ell^\infty})$. We identify $Z = \mathrm{Gal}(L/K^{(\ell)})$ and $\mathrm{Gal}(L'/K')$ via the restriction map. For every prime $\mathfrak{p}$ of L, this gives an identification of $Z_{\mathfrak{p}}$ with the decomposition group of $\mathfrak{p} \cap L'$ in L'/K'.

Let $A := \ker \pi_{m,n}$. Then A is a $\mathrm{Gal}(K')$-module via the restriction map $\mathrm{Gal}(K') \to Z$. We claim that the map:

$$\rho : H^2(\mathrm{Gal}(K'), A) \to \prod_{\mathfrak{p}} H^2(\mathrm{Gal}(K'_{\mathfrak{p}}), A)$$

is injective, where $\mathfrak{p}$ runs over all primes of K'. Let $\hat{A} = \mathrm{Hom}(A, \mu_\ell)$ be the dual $\mathrm{Gal}(K')$-module and $K'(\hat{A})$ the fixed field of the centralizer $H \le \mathrm{Gal}(K')$ of $\hat{A}$ under this action. Since $\mathrm{Gal}(K')$ acts trivially on μ_ℓ and $\mathrm{Gal}(L')$ acts trivially on A, the map $\mathrm{Gal}(K') \to \mathrm{Aut}(\hat{A})$ splits through Z. Thus, H is an open subgroup of $\mathrm{Gal}(K')$ which contains $\mathrm{Gal}(L')$, and hence $G' := \mathrm{Gal}(K'(\hat{A})/K')$ is a finite cyclic ℓ-group. By the Poitou-Tate duality theorem [17, Satz 4.5] (or [16, Theorem 8.6.8]), ρ is injective if and only if

$$\rho' : H^1(G', \hat{A}) \to \prod_{\mathfrak{p}} H^1(G'_{\mathfrak{p}}, \hat{A})$$

is injective, where $G'_{\mathfrak{p}} = \mathrm{Gal}(K'(\hat{A})_{\mathfrak{P}}/K'_{\mathfrak{p}})$ for any prime $\mathfrak{P}$ of $K'(\hat{A})$ lying over $\mathfrak{p}$, and $\mathfrak{p}$ runs over all primes of K'. Since G' is cyclic, by Chebutarev's density theorem there are infinitely many primes $\mathfrak{p}$ for which $G'_{\mathfrak{p}} = G'$. Thus, ρ' and hence ρ are injective, proving the claim.

Let $\tilde{\phi} : \mathrm{Gal}(K') \to V_n \rtimes Z$ be the map given by the composition of the isomorphism $\mathrm{Gal}(K') \cong \mathrm{Gal}(L') \rtimes Z$ and the map $(\phi, \mathrm{id}) : \mathrm{Gal}(L') \rtimes Z \to V_n \rtimes Z$, and let $\tilde{\pi}_{m,n} : V_m \rtimes Z \to V_n \rtimes Z$ be the map given by $(\pi_{m,n}, \mathrm{id})$. Since the Z-embedding problem $(\phi', \pi_{m,n})$ is solvable if and only if the embedding problem $(\tilde{\phi}, \tilde{\pi}_{m,n})$ is solvable, it suffices to show the latter. Similarly, since $(\phi_{\mathfrak{p}}, \pi_{m,n})$ is solvable, the restriction $(\tilde{\phi}_{\mathfrak{p}}, \tilde{\pi}_{m,n})$ of $(\tilde{\phi}, \tilde{\pi}_{m,n})$ to $\mathrm{Gal}(K'_{\mathfrak{p}}) = \mathrm{Gal}(L'_{\mathfrak{p}}) \rtimes Z_{\mathfrak{p}}$ is solvable. The maps

$\tilde{\phi}, \tilde{\phi}_{\mathfrak{p}}$ give the following commutative diagram:

$$\begin{array}{ccc} H^2(V_n \rtimes Z, A) & \xrightarrow{\rho} & \prod_{\mathfrak{p}} H^2(V_n \rtimes Z_{\mathfrak{p}}, A) \\ \downarrow{\scriptstyle \tilde{\phi}^*} & & \downarrow{\scriptstyle \prod_{\mathfrak{p}} \tilde{\phi}_{\mathfrak{p}}^*} \\ H^2(\mathrm{Gal}(K'), A) & \xrightarrow{\rho} & \prod_{\mathfrak{p}} H^2(\mathrm{Gal}(K'_{\mathfrak{p}}), A), \end{array} \tag{10}$$

where $V_n \rtimes Z$ acts on A via the projection onto Z, ρ is the restriction map, and $\mathfrak{p}$ runs through all primes of L'.

Since the action of $V_n \rtimes Z$ on A via the extension $\tilde{\pi}_{m,n}$ factors through the projection onto Z, it agrees with the above chosen action. Thus, $\tilde{\pi}_{m,n}$ defines a class $\alpha_{m,n} \in H^2(V_n \rtimes Z, A)$. Let $\alpha_{m,n}^{(\mathfrak{p})}$ be the $\mathfrak{p}$-th component of $\rho(\alpha_{m,n})$. Since $(\tilde{\phi}_{\mathfrak{p}}, \tilde{\pi}_{m,n})$ is solvable, $\tilde{\phi}_{\mathfrak{p}}^*(\alpha_{m,n}^{(\mathfrak{p})}) = 0$ for all $\mathfrak{p}$. By (10), $\rho\tilde{\phi}^*(\alpha_{m,n}) = 0$. Since ρ is injective, $\tilde{\phi}^*(\alpha_{m,n}) = 0$ and hence $(\tilde{\phi}, \tilde{\pi}_{m,n})$ is solvable, as required. □

5.3. **The local height.** By the above local global principle, to find the global height $\mathrm{ht}(\phi)$ for $\phi \in \hat{F}^Z$, it suffices to find the local heights $\mathrm{ht}(\phi_{\mathfrak{p}})$ for primes $\mathfrak{p}$ of L. We analyze the latter using [6].

A homomorphism $\phi : \mathrm{Gal}(L) \to G$ is **unramified** (resp. **tamely ramified**) at a prime $\mathfrak{p}$ of L if the fixed field of $\ker(\phi)$ is unramified (resp. tamely ramified) over L at $\mathfrak{p}$.

Proposition 5.6. *Let $\mathfrak{p}$ be a prime of L and $\phi \in \hat{F}^Z$. Then:*

(a) $\mathrm{ht}(\phi_{\mathfrak{p}}) = [Z : Z_{\mathfrak{p}}] - 1$ *or* ∞*;*
(b) *If ϕ is unramified, then* $\mathrm{ht}(\phi_{\mathfrak{p}}) = \infty$*;*
(c) *If ϕ ramifies and is tamely ramified, then* $\mathrm{ht}(\phi_{\mathfrak{p}}) = [Z : Z_{\mathfrak{p}}] - 1$.

Proof. As L contains all ℓ-power roots of unity, if $\mathfrak{p}$ is infinite, $\mathfrak{p}$ is complex, and hence $\phi_{\mathfrak{p}}$ is trivial and $\mathrm{ht}(\phi_{\mathfrak{p}}) = \infty$. Hence, we assume $\mathfrak{p}$ is a finite prime.

By Proposition 4.3, ϕ extends to a Z-homomorphism $\phi' : \mathrm{Gal}(L') \to V_1$ where $L' = K'(\mu_{\ell^\infty})$ and $K'/K(\mu_\ell)$ is a finite extension. Moreover, $\mathrm{ht}(\phi_{\mathfrak{p}}) = \mathrm{ht}(\phi'_{\mathfrak{p}\cap L'})$ for any prime $\mathfrak{p}$ of L. Let $G := \mathrm{Gal}(L'_{\mathfrak{p}})$ and G^{ab} (resp. $\overline{G}$) the maximal abelian (resp. elementary abelian) quotient of G viewed as $Z_{\mathfrak{p}}$-groups.

For a finite subextension $E = (L'_{\mathfrak{p}})^{\ell^n Z_{\mathfrak{p}}}$ of $L'_{\mathfrak{p}}/K'_{\mathfrak{p}}$, let $\overline{E}^\times$ denote the profinite completion of the multiplicative group $E^\times$. By local class field theory, $\overline{E}^\times$ is isomorphic via the reciprocity map to $\mathrm{Gal}(E)^{\mathrm{ab}}$, where the subgroup of units in E is mapped to the inertia subgroup in $\mathrm{Gal}(E)^{\mathrm{ab}}$. In particular, the image of the ℓ-power roots of unity in E under the reciprocity map lies in the inertia group.

Iwasawa's theorem [6, Theorem 25] gives a $Z_{\mathfrak{p}}$-isomorphism:

$$r : G^{\mathrm{ab}} \to T(\mu) \times \Lambda^d,$$

where $T(\mu)$ is the Tate module $T(\mu) := \varprojlim \mu_n$, $\Lambda := \mathbb{Z}_\ell[[Z_{\mathfrak{p}}]]$, and $d = [K'_{\mathfrak{p}} : \mathbb{Q}_\ell]$ if $\mathfrak{p}$ lies over ℓ and 0 otherwise. Moreover, for each finite subextension $E = (L'_{\mathfrak{p}})^{\ell^n Z_{\mathfrak{p}}}$

in $L'_{\mathfrak{p}}/K'_{\mathfrak{p}}$, the reciprocity map and r induce isomorphisms

$$G^{\mathrm{ab}}/I^{\ell^n}G^{\mathrm{ab}} = \mathrm{Gal}(E)^{\mathrm{ab}} \cong \overline{E}^{\times} \cong T(\mu)/I^{\ell^n}T(\mu) \times \Lambda^d/I^{\ell^n}\Lambda^d,$$

where $T(\mu)/I^{\ell^n}T(\mu)$ is mapped to the group of ℓ-power roots of unity in $\overline{E}^{\times}$ and hence to a subgroup of the inertia group in $\mathrm{Gal}(E)^{\mathrm{ab}}$. In particular, the image of $T(\mu)$ under r^{-1} is a subgroup of the inertia group in G^{ab}.

As $\Lambda/\ell\Lambda \cong \mathbb{F}_\ell[[Z]]$ and $T(\mu)/\ell T(\mu) \cong V_1$ as $Z_{\mathfrak{p}}$-modules, it follows that

$$\overline{G} = G^{\mathrm{ab}}/\ell G^{\mathrm{ab}} \cong V_1 \times \mathbb{F}_\ell[[Z]]^d.$$

Let G_1 be the direct Z-summand of $\overline{G}$ which is isomorphic to V_1, so that G_1 is contained in the inertia subgroup of $\overline{G}$.

We separate into two cases as to whether G_1 is contained in $\ker \phi'_{\mathfrak{p}}$. If $G_1 \leq \ker \phi'_{\mathfrak{p}}$, then $\phi'_{\mathfrak{p}}$ splits through $\mathbb{F}_\ell[[Z]]^d$. As $\mathbb{F}_\ell[[Z]]$ is free as an ℓ-torsion Z-module, this implies that $(\phi'_{\mathfrak{p}}, \pi_n)$ is solvable for all $n \in \mathbb{N}$. Thus, $\mathrm{ht}(\phi_{\mathfrak{p}}) = \mathrm{ht}(\phi'_{\mathfrak{p}}) = \infty$. This is in particular the case if $\phi'_{\mathfrak{p}}$ is unramified, proving (b).

On the other hand if $G_1 \not\leq \ker \phi'_{\mathfrak{p}}$, we claim that $\mathrm{ht}(\phi'_{\mathfrak{p}}) = \ell^t - 1$, where $\ell^t := [Z : Z_{\mathfrak{p}}]$. Let σ be a generator of Z. For $n \leq \ell^t$,

$$(\sigma^{\ell^t} - 1) = I^{\ell^t} \subseteq I^n,$$

and hence the Z-module V_n viewed as $Z_{\mathfrak{p}}$-module is the trivial $Z_{\mathfrak{p}}$-module $(\mathbb{F}_\ell)^n$. In particular, the $Z_{\mathfrak{p}}$-embedding problem $(\phi'_{\mathfrak{p}}, \pi_n)$ is solvable and hence $\mathrm{ht}(\phi'_{\mathfrak{p}}) \geq \ell^t - 1$.

For $n > \ell^t$, assume on the contrary that $(\phi'_{\mathfrak{p}}, \pi_n)$ is solvable and hence that its restriction $(\phi''_{\mathfrak{p}} : G_1 \to V_1, \pi_n)$ to G_1 has a solution $\psi_{\mathfrak{p}}$. As $\psi_{\mathfrak{p}}$ is nontrivial, the image $J := \mathrm{Im}\, \psi_{\mathfrak{p}}$ is $Z_{\mathfrak{p}}$-isomorphic to $J \cong V_1$. Since $J \leq V_n$ is fixed by $Z_{\mathfrak{p}}$, one has $I^{\ell^t} J = (\sigma^{\ell^t} - 1)J = 0$. As $n > \ell^t$, the kernel of multiplication by I^{ℓ^t} is contained in IV_n and hence $J \subseteq IV_n = \ker \pi_n$, contradicting $\mathrm{Im}(\pi_n \psi_{\mathfrak{p}}) = \mathrm{Im}(\phi''_{\mathfrak{p}}) \neq 0$. This proves the claim and Part (a).

If $\phi_{\mathfrak{p}}$ ramifies nontrivially and tamely, $\mathfrak{p}$ does not divide ℓ, and $d = 0$. As $\phi_{\mathfrak{p}}$ is nontrivial, this implies that $G_1 \not\leq \ker \phi'_{\mathfrak{p}}$. In such case, the claim gives Part (c), completing the proof. □

5.4. **Finite Ulm invariants.** We can now combine the local global principle and the analysis of local heights to find the finite Ulm invariants of $\hat{F}$:

Proposition 5.7. *The n-th Ulm invariant of $\hat{F}$ is:*

$$U_n(\hat{F}) = \begin{cases} \omega & \text{if } n = \ell^k - 1 \\ 0 & \text{for any other } n \in \mathbb{N} \end{cases}$$

Proof. By Propositions 5.5 and 5.6, the height of each element of $\hat{F}^Z$ is either infinite or $n = \ell^k - 1$, for some k. Hence, by (8), $U_n(\hat{F}) = 0$ for all other $n \in \mathbb{N}$.

For $n = \ell^k - 1$, $k \in \mathbb{N} \cup \{0\}$, we construct an infinite subgroup $F_n \leq \hat{F}^Z$, the non-trivial elements of which are of height $\ell^k - 1$.

Let ℓ^s be the number of ℓ-power roots of unity in $K(\mu_\ell)$ and hence in $K^{(\ell)}$. We first claim that there is an infinite set P_k of rational primes p such that $p \equiv 1 \bmod \ell^{k+s}$, $p \not\equiv 1 \bmod \ell^{k+s+1}$, and there is a prime $\mathfrak{q}$ of K of degree 1 over p.

Let M be the Galois closure of $K/\mathbb{Q}$ and let $C \le \mathrm{Gal}(M(\mu_{\ell^{k+s+1}})/K(\mu_{\ell^{k+s}}))$ be a cyclic subgroup which does not fix $\mu_{\ell^{k+s+1}}$. By Chebotarev's density theorem there are infinitely many rational primes $\mathfrak{q}'$ of $M(\mu_{\ell^{k+s+1}})$ whose Frobenious lies in C. Since C fixes K, the restricion $\mathfrak{q}$ of such $\mathfrak{q}'$ to K is of degree 1 over $(p) = \mathfrak{q}' \cap \mathbb{Q}$. Since the restriction of C to $\mathbb{Q}(\mu_{\ell^{k+s+1}})$ lies in $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^{k+s+1}})/\mathbb{Q}(\mu_{\ell^{k+s}}))$, we get that $p \equiv 1 \bmod \ell^{k+s}$ and $p \not\equiv 1 \bmod \ell^{k+s}$, proving the claim.

For each $p \in P$, let $\tilde{\phi}_p : \mathrm{Gal}(\mathbb{Q}) \to \mathbb{Z}/\ell\mathbb{Z}$ be a nontrivial homomorphism ramified only over p, and $\phi_p \in \hat{F}^Z$ its restriction to F. Let F_n be the subgroup of $\hat{F}$ generated by $\phi_p : F \to V_1, p \in P$.

We claim that every non-trivial $\phi \in F_n$ is of height $\ell^k - 1$. Since $\tilde{\phi}_p$ is ramified only over p, ϕ is ramified only over primes $\mathfrak{p}$ of $K^{(\ell)}$ lying over primes in P. Since $p \equiv 1 \bmod \ell^{k+s}$, $\mu_{\ell^{k+s}} \subseteq \mathbb{Q}_p \subseteq L_\mathfrak{p}$, and hence $\ell^k \mid [Z : Z_\mathfrak{p}]$, for every prime $\mathfrak{p}$ of $K^{(\ell)}$ dividing $p \in P$. Thus by Proposition 5.6.(b-c), $\mathrm{ht}(\phi_\mathfrak{p}) \ge \ell^k - 1$ for all primes $\mathfrak{p}$ of $K^{(\ell)}$. Moreover, as ϕ is the restriction of an element in $\langle \tilde{\phi}_p | p \in P \rangle$, it is ramified over all primes of $K^{(\ell)}$ dividing some $q \in P$. Letting $\mathfrak{q}_0$ be a degree 1 prime of K over q, we get that ϕ is ramified over a prime $\mathfrak{Q}_0$ of $K^{(\ell)}$ lying over $\mathfrak{q}_0$. Since $\mu_{\ell^{k+s+1}} \not\subseteq \mathbb{Q}_q \cong K_{\mathfrak{q}_0}$, $\mu_{\ell^{k+s+1}} \not\subseteq K^{(\ell)}_{\mathfrak{Q}_0}$ and hence $[Z : Z_{\mathfrak{Q}_0}] = \ell^k$. By Proposition 5.6.(c), $\mathrm{ht}(\phi_{\mathfrak{Q}_0}) = \ell^k - 1$. It therefore follows from Proposition 5.5 that

$$\mathrm{ht}(\phi) = \min_\mathfrak{p} \mathrm{ht}(\phi_\mathfrak{p}) = \mathrm{ht}(\phi_{\mathfrak{Q}_0}) = \ell^k - 1,$$

for every $\phi \in F_n$, proving the claim. By (8), we get $U_{\ell^k - 1}(\hat{F}) = \omega$, for all nonnegative integers k. □

5.5. **The maximal free quotient.** To complete the proof of Theorem 5.1, it remains to find the maximal free $\mathbb{F}_\ell[[Z]]$-quotient of $\overline{F}$.

Proposition 5.8. (a) *If K is a number field, the maximal free $\mathbb{F}_\ell[[Z]]$-quotient of $\overline{F}$ is $\mathbb{F}_\ell[[Z]]^\omega$.*

(b) *If K is a global field of positive characteristic and $\ell \ne \mathrm{char}\, K$, then $\overline{F}$ has no free $\mathbb{F}_\ell[[Z]]$-quotients.*

Proof. First assume that K is a number field. Let $K(\mu_\ell) \subseteq K' \subseteq K^{(\ell)}$ be a number field. By Iwasawa theory [24, Theorem 13.31] there is a Z-homomorphism

$$\mathrm{Gal}(K'(\mu)) \to \Lambda^{r_2(K')}$$

with finite cokernel, where $\Lambda := \mathbb{Z}_\ell[[Z]]$. Let J be its image. Since $J/\ell J$ is an $\mathbb{F}_\ell[[Z]]$-submodule of finite index in $(\Lambda/\ell\Lambda)^{r_2(K')} \cong \mathbb{F}_\ell[[Z]]^{r_2(K')}$ and $\mathbb{F}_\ell[[Z]]$ is a discrete valuation ring, $J/\ell J$ is $\mathbb{F}_\ell[[Z]]$-isomorphic to $\mathbb{F}_\ell[[Z]]^{r_2(K')}$. This shows that

$\mathbb{F}_\ell[[Z]]^{r_2(K')}$ is a Z-quotient of $\mathrm{Gal}(K'(\mu_{\ell^\infty}))$ and hence, by Lemma 2.5, it is also a Z-quotient of $\mathrm{Gal}(L)$. Since $r_2(K')$ is arbitrarily large for prime to-ℓ extensions, this gives Part (a).

Assume $\ell \neq \mathrm{char}\, K > 0$. It suffices to show that every Z-homomorphism $\phi : F \to V_1$ does not split through a free $\mathbb{F}_\ell[[Z]]$-module, or equivalently by Proposition 5.4.(b), that (ϕ, π) is nonsolvable. By Proposition 4.3, ϕ extends to a Z-homomorphism $\phi' : \mathrm{Gal}(L') \to V_1$, where $L' = K'(\mu_{\ell^\infty})$ for some finite subextension K' of $K^{(\ell)}/K(\mu_\ell)$. By [6, §12.4], the maximal abelian Z-quotient $X := \mathrm{Gal}(L')^{ab}$ is a Λ-torsion module for which $X/\ell X$ has no free $\Lambda/\ell\Lambda \cong \mathbb{F}_\ell[[Z]]$-quotients. Thus, (ϕ', π) is nonsolvable. Hence, by Proposition 4.3, (ϕ, π) is nonsolvable, proving (b). □

Proof of Theorem 5.1. In view of Proposition 5.3 and (7), it suffices to find the finite Ulm invariants $U_n(\hat{F})$ and the multiplicity of the maximal free $\mathbb{F}_\ell[[Z]]$-quotient of $\overline{F}$. This is done in Propositions 5.7 and 5.8, completing the proof of Theorem 5.1. □

Similarly to the number field case, for global fields K of positive characteristic we get:

Corollary 5.9. *Let K be a global field of positive characteristic and $\ell \neq \mathrm{char}\, K$. For any positive integer N the Z-group $\overline{F}$ decomposes as $\overline{F} = V_{\leq N} \times V_{>N}$ where:*

$$V_{\leq N} \cong \prod_{n=1}^{N} \mathbb{F}_\ell[Z/\ell^n Z]^\omega$$

and $V_{>N}$ has no Z-summands of dimension $\leq \ell^N$ over $\mathbb{F}_\ell$, nor Z-summands Z-isomorphic to $\mathbb{F}_\ell[[Z]]$.

5.6. **Towards a presentation.** As a Corollary to Theorem 5.1, we get the following description of $\mathrm{Gal}(K^{(\ell)})$ in terms of generators and relations.

Let σ be a generator of Z and let $\sigma(x) = \sigma x \sigma^{-1}$ denote the action of σ on $x \in F$. Recall that $X \subseteq F$ is a basis for F if X converges to 1 and F is the free pro-p group generated by X [22, §3.3].

Corollary 5.10. *Let K be a number field, ℓ an odd prime, and $N \in \mathbb{N}$. Then $\mathrm{Gal}(K^{(\ell)})$ is generated by σ and a basis of F which is a disjoint union of three subsets $X_{>N} \cup X_\infty \cup X_{\leq N}$:*

(a) *$X_{\leq N}$ is a disjoint union of infinitely many copies of each of the sets*

$$\{x_1, \ldots, x_{\ell^n}\}, n \leq N,$$

subject to the relations

$$\sigma(x_i) = x_{i+1} x_i y_i \text{ and } \sigma(x_{\ell^n}) = x_{\ell^n} y \tag{11}$$

for some $y, y_i \in \Phi(F)$, $1 \leq i \leq \ell^n - 1$;

(b) X_∞ *is a disjoint union of infinitely many copies of the set* $\{x_n\}_{n\in\mathbb{N}}$ *which converges to* 1 *as* $n\to\infty$*, and is subject to the relations:*

$$\sigma(x_i)=x_{i+1}x_iy_i \text{ and } \sigma^{-1}(x_1)=(\prod_{i\in\mathbb{N}}x_i^{(-1)^i})y, \tag{12}$$

for some $y_i, y\in\Phi(F)$, $i\in\mathbb{N}$*;*

(c) $\langle X_{>N},\Phi(F)\rangle$ *is* Z*-invariant.*

Moreover, we can assume that any finite subset of the y_i*'s appearing in parts (b) and (c) are trivial.*

Proof. Recall that a basis for $\overline{F}$ as a profinite $\mathbb{F}_\ell$-vector space is a minimal generating set which converges to 1. We first choose a basis $\overline{S}$ for $\overline{F}$ as follows. For each Z-summand Z-isomorphic to $V_{\ell^n}\cong\mathbb{F}_\ell[Z/\ell^nZ]$,$n\le N$, include in $\overline{S}$ the basis $\{\overline{x}_i\}_{i=0}^{\ell^n-1}$ of the summand which corresponds to the basis $(\sigma-1)^i\in I^i$, $i=0,\dots,\ell^n-1$, of $\mathbb{F}_\ell[Z/\ell^nZ]$. For each Z-summand Z-isomorphic to $\mathbb{F}_\ell[[Z]]$, include a basis $\{\overline{x}_i\}_{i\in\mathbb{N}}$ which corresponds to $(\sigma-1)^i$, $i\in\mathbb{N}$. Include in $\overline{S}$ a basis of $V_{>N}$. The set $\overline{S}$ is a basis for $\overline{F}$ as it is the union of bases for each of the direct Z-summands in a direct product.

By [22, Proposition 7.6.9], a basis $\overline{S}$ for $\overline{F}$ can be lifted to basis S of F. Since for each V_{ℓ^n}-summand we have $\overline{x}_{i+1}=(\sigma-1)\overline{x}_i$, $i=0,\dots,\ell^n-2$, and $(\sigma-1)\overline{x}_{\ell^n-1}=0$, the relations in (11) follow. The relations in (12) follow since for each $\mathbb{F}_\ell[[Z]]$-summand we have $\overline{x}_{i+1}=(\sigma-1)\overline{x}_i$, $i\in\mathbb{N}$, and

$$\sigma\overline{x}_1=\sum_{i=0}^{\infty}(1-\sigma)^i\overline{x}_1=\sum_{i=0}^{\infty}(-1)^i\overline{x}_i.$$

Moreover, by [22, Corollary 7.6.10] the basis $\overline{S}$ can be lifted to a basis S of F in which finitely many elements in $\overline{S}$ have prescribed liftings. This allows assuming that finitely many of the y_i's in Parts (b) and (c) equal 1. □

We note that one can choose $X_{>N}\supseteq X_{>N+1}$. In order to obtain a presentation mod $\phi(F)$, it remains to determine the action of σ on elements in $\cap_N X_{>N}$.

5.7. **Infinite Ulm invariants.** To determine the structure of $\overline{F}$ as a Z-module completely, it is necessary to find the infinite Ulm invariants of $\hat{F}$ or equivalently the Ulm invariants of $\hat{F}_\omega$. These are connected to Iwasawa theory as follows.

Assume $\mu_\ell\subseteq K$. Let M be the maximal abelian pro-ℓ extension of $K(\mu_{\ell^\infty})$ unramified outside primes with residue characteristic different from ℓ, M^{un} the maximal extension inside M which is everywhere unramified, and M^{sc} the maximal extension inside M^{un} in which all primes of $K(\mu_{\ell^\infty})$ with residue characteristic ℓ split completely. Iwasawa theory [24, §13] studies the Galois groups $X^{\mathrm{sc}}(K):=\mathrm{Gal}(M^{\mathrm{sc}}/K)$, $X^{\mathrm{un}}(K):=\mathrm{Gal}(M^{\mathrm{un}}/K)$ and $X(K):=\mathrm{Gal}(M/K)$ as modules over $\mathrm{Gal}(K(\mu_{\ell^\infty})/K)\cong Z$. These are finitely generated Z-modules and hence admit a

Z-homomorphism with finite kernel and cokernel into a unique Z-module of the form:

$$\Lambda^r \times \prod_{i\in I}(\Lambda/\ell^i\Lambda)^{r_i} \times \prod_{j=1}^{k}\Lambda/(g_i(x)),$$

where $\Lambda := \mathbb{Z}_\ell[[Z]]$, $I \subseteq \mathbb{N}$ is a finite subset, $r, k, r_i \in \mathbb{N}$ for all $i \in I$, and $g_j(x), j = 1, \dots, k$, are monic irreducible polynomials for which all non-leading coefficients are divisible by ℓ. The Iwasawa **μ-invariant** of a Z-module is the corresponding sum $\sum_{i\in I} r_i$.

Consider the Z-modules $X := X(K^{(\ell)})$ and $X^{\mathrm{un}} := X^{\mathrm{un}}(K^{(\ell)})$. By (9), an element $\phi \in \hat{F}_\omega^Z$ has infinite height. Hence, Propositions 5.5 and 5.6 imply that such ϕ factors through X. Moreover, every ϕ which factors through X^{un} and hence is unramified, has infinite height. Thus, we have[2]:

$$(\hat{X}^{\mathrm{sc}})^Z \subseteq (\hat{X}^{\mathrm{un}})^Z \subseteq \hat{F}_\omega^Z \subseteq \hat{X}^Z.$$

The following proposition shows that $\hat{F}_\omega$ has nontrivial Ulm invariants if $K = \mathbb{Q}$.

Proposition 5.11. *Let $K = \mathbb{Q}$ and ℓ an odd prime. Then the Z-module $\hat{F}$ has nontrivial infinite Ulm invariants.*

Proof. The Z-module $\hat{F}_\omega$ has trivial Ulm invariants it satisfies $I^n\hat{F}_\omega = \hat{F}_\omega$ for all $n \in \mathbb{N}$. A module satisfying the latter is called divisible, and by [7, Theorem 4][3], it is a direct sum of Z-modules $\hat{V}$, where V is the free $\mathbb{F}_\ell[[Z]]$-module $\mathbb{F}_\ell[[Z]]$. By duality, we get that if $\hat{F}_\omega$ has trivial Ulm invariants then its dual $\mathbb{F}_\ell[[Z]]$-module is free. Thus, it suffices to construct a Z-homomorphism $\phi : \mathrm{Gal}(L) \to V_1$ with $\mathrm{ht}(\phi) = \infty$ and such that $(\phi, \pi : V \to V_1)$ is non-solvable.

By [25], there is a real quadratic extension $K_0/\mathbb{Q}$ whose class number is divisble by ℓ. Let L_0/K_0 be the $\mathbb{Z}_\ell$-extension inside $K_0(\mu)$. Since L_0/K_0 is a Z-extension for which $L_0K^{(\ell)} = L$, Lemma 2.9 implies that $\mathrm{Gal}(L_1)$ is a Z-group for which the restriction $\mathrm{Gal}(L_1) \to \mathrm{Gal}(L)$ is a Z-homomorphism.

Let M_0/K_0 be an unramified $\mathbb{Z}/\ell\mathbb{Z}$-extension and $\phi_0' : \mathrm{Gal}(K_0) \to \mathbb{Z}/\ell\mathbb{Z}$ a homomorphism whose kernel fixes M_0. Its restrictions $\phi_0 : \mathrm{Gal}(L_0) \to V_1$ and $\phi : \mathrm{Gal}(L) \to V_1$ are unramified Z-homomorphisms. Hence, by Propositions 5.5 and 5.6, $\mathrm{ht}(\phi) = \infty$.

Assume on the contrary that there is a solution ψ to the Z-embedding problem (ϕ, π). By Proposition 4.3, ψ extends to a solution ψ_0 to the Z-embedding problem (ϕ_0, π). Let $K_1 = K_0(\mu_\ell)$, $L_1 = K_0(\mu_{\ell^\infty})$ and $\Delta := \mathrm{Gal}(K_1/K_0)$. In particular, ϕ_0 splits through a Z-homomorphism $\phi_u : X(K_0)/\ell X(K_0) \to V_1$.

At a prime $\mathfrak{p}$ of L that is prime to ℓ, $\mathrm{Gal}(L_\mathfrak{p})$ is cyclic and in particular has no free $\mathbb{F}_\ell[[Z]]$-quotients. Thus, ψ and hence ψ_0 are unramified at primes that

[2]In fact, one can furthermore show $\hat{X}^{\mathrm{sc}} \subseteq \hat{X}^{\mathrm{un}} \subseteq \hat{F}_\omega \subseteq \hat{X}$. This remains to be added.

[3]see [7, §12] for the corresponding statements for modules.

do not divide ℓ. It follows that ψ_0 factors through $X(K_0)$ and hence through $X(K_0)/\ell X(K_0)$, showing that (ϕ_u, π) is solvable.

By Iwasawa's theorem [16, Corollary 11.3.17], the μ-invariants $\mu(X(K_1))$ and $\mu(X^{sc}(K_1))$ are equal. By Ferrero-Washington [3], $\mu(X^{\mathrm{un}}(K_1)) = 0$. Since $X^{\mathrm{un}}(K_1)$ has no free Λ-quotients [24, Proposition 13.19], $\mu(X^{\mathrm{sc}}) \le \mu(X^{\mathrm{un}}) = 0$ and hence $\mu(X^{\mathrm{sc}}(K_1)) = \mu(X(K_1)) = 0$. Considering $X(K_1)$ as a module over

$$\mathrm{Gal}(K_1(\mu_{\ell^\infty})/K_0) \cong \Delta \times \Lambda,$$

we have $X(K_0) \cong X(K_1)^\Delta$ as Λ-modules, showing that $\mu(X(K_0)) = \mu(X(K_1)^\Delta) = 0$. As K_0 is totally real, [24, Theorem 13.31] implies that $X(K_0)$ has no free Λ-quotients. Since moreover $\mu(X(K_0)) = 0$, $X(K_1)/\ell X(K_1)$ has no free $\mathbb{F}_\ell[[Z]]$-quotients, contradicting the solvability of (ϕ_u, π). □

As a consequence for $K = \mathbb{Q}$, it follows from Proposition 5.3.(b) that $\overline{F}$ is not Z-isomorphic to a product of the Z-modules $\mathbb{F}_\ell[[Z]]$ and $V_n, n \in \mathbb{N}$.

Remark 5.12. Since [25] gives infinitely many choices of K_0, there are infinitely many unramified $\mathbb{Z}/\ell\mathbb{Z}$-extensions of $K^{(\ell)}$. Thus, neither $X^{\mathrm{un}}(K^{(\ell)})$, nor any maximal quotient of $\mathrm{Gal}(K^{(\ell)})$ with ramification restricted to a finite set, is finitely generated.

5.8. **The height.** Let σ be a generator of Z and $n \in \mathbb{N}$, so that

$$1, \sigma - 1, \dots, (\sigma - 1)^{n-1},$$

is an $\mathbb{F}_\ell$-basis of $V_n = \mathbb{F}_\ell[[Z]]/I^n$. Let $f_0, \dots, f_{n-1}$ denote its dual basis, so that: $f_i((\sigma-1)^j) = 1$ if $i = j$ and 0 otherwise.

Note that $(\sigma - 1)f_0 = 0$ and $(\sigma - 1)f_{i+1} = f_i$ for all $0 \le i \le n-2$. In particular, $\hat{V}_n$ is a cyclic $\mathbb{F}_\ell[[Z]]$-module of dimension n, and hence Z-isomorphic to V_n.

Proof of Proposition 5.4. Let $\phi^* : \hat{M} \to \hat{V}_n$ and $\pi_n^* : \hat{V}_1 \to \hat{V}_n$ be the dual Z-homomorphisms to ϕ and π_n, respectively. The Z-embedding problem (ϕ, π_n) has a solution $\psi : M \to V_n$ if and only if there is a Z-homomorphism $\psi^* : \hat{V}_n \to \hat{M}$ which makes the following diagram commutative, i.e. satisfies $\pi_n^* \circ \psi^* = \phi^*$.

(13)
$$\begin{array}{ccc} & & \hat{M} \\ & \overset{\psi^*}{\nearrow} & \uparrow{\scriptstyle \phi^*} \\ \hat{V}_n & \xleftarrow{\pi_n^*} & \hat{V}_1. \end{array}$$

For simplicity, identify V_1 with $\mathbb{F}_\ell$ so that $\hat{V}_1$ contains an identity map 1. Note that $\phi^*(1) = \phi$ and $\pi_n^*(1) = f_0$.

Assume that (ϕ, π_n) is solvable. As $(\sigma-1)^{n-1} f_{n-1} = f_0$, we have

$$\phi = \phi^*(1) = \psi^*(\pi_n^*(1)) = \psi^*(f_0) = \psi^*((\sigma-1)^{n-1} f_{n-1}) = (\sigma-1)^{n-1}\psi^*(f_{n-1}) \in I^{n-1}\hat{M}.$$

Conversely, assume $\phi = (\sigma-1)^{n-1}\phi'$. As $(\sigma-1)^n\phi' = 0$, there is a (unique) Z-homomorphism $\psi^* : \hat{V}_n \to \hat{M}$ such that $\psi^*(f_{n-1}) = \phi'$. Such ψ^* satisfies:

$$\psi^*\pi_n^*(1) = \psi^*(f_0) = \psi^*((\sigma-1)^{n-1}f_{n-1}) = (\sigma-1)^{n-1}\phi' = \phi = \phi^*(1),$$

and hence $\psi^*\pi_n^* = \phi^*$, giving Part (a).

To see Part (b), note that if ϕ factors as $\phi_2 \circ \phi_1$ where $\phi_2 : \mathbb{F}_\ell[[Z]]^k \to V_1$, then (ϕ_2, π) is solvable and its solution ψ induces a solution $\phi_2 \circ \psi$ of (ϕ, π). On the other hand if (ϕ, π) has a solution ψ, then ϕ factors through ψ and hence also through the maximal free $\mathbb{F}_\ell[[Z]]$-quotient of M. □

5.9. **Ulm invariants and finite summands.** To prove Proposition 5.3, we first prove the following dual statement:

Lemma 5.13. *Let $N \in \mathbb{N}$ and let P be a discrete torsion $\mathbb{F}_\ell[[Z]]$-module. Then $P = P_{\le N} \oplus P_{>N}$ where*

$$P_{\le N} \cong \bigoplus_{n \le N} V_n^{U_{n-1}(P)},$$

and $P_{>N}$ has no Z-summands of dimension $\le N$. Moreover, $P_{\le N}$ is a Z-summand of $P_{\le N+1}$ for all $N \in \mathbb{N}$.

Proof. We argue by induction on N. Assume the decomposition $P = P_{\le N} \oplus P_{>N}$ is given, and by the induction hypothesis for $P_{>N}$ that $U_n(P_{>N}) = 0$ for all $n \le N-1$. In particular, $P_{>N}^Z$ has no elements of height $\le N-1$.

As Z-acts trivially on $P_{>N}^Z$, we regard it as an $\mathbb{F}_\ell$-vector spaces. Let $U_{>N}$ be the $\mathbb{F}_\ell$-subspace of $P_{>N}^Z$ consisting of elements of height $> N$, and U_N a complement of it. In particular, U_N is a maximal $\mathbb{F}_\ell$-subspace of $P_{>N}^Z$ whose nontrivial elements are of height N. Let $\{u_j\}_{j\in J}$ be an $\mathbb{F}_\ell$-basis of U_N. By definition $U_N(P_{>N}) = |J|$.

For each $j \in J$, u_j is of height N, and hence we may pick an element $p_j \in P_{>N}$ such that $(\sigma-1)^N p_j = u_j$. Let P_{N+1} (resp. $\langle p_j \rangle$) be the Z-module generated by $\{p_j\}_{j\in J}$ (resp. by p_j for $j \in J$). As $\langle p_j \rangle$ is a cyclic Z-module of dimension $N+1$ over $\mathbb{F}_\ell$, $\langle p_j \rangle \cong V_{N+1}$ for $j \in J$. Since $\langle p_j \rangle^Z = \mathbb{F}_\ell u_j, j \in J$, are linearly disjoint, the Z-modules $\langle p_j \rangle, j \in J$, are linearly disjoint, and hence $P_{N+1} \cong \oplus_J V_{N+1}$.

Since all nontrivial elements of U_N^Z are of height N, we have $I^k P \cap P_{N+1} = I^k P_{N+1}$ for all k. Since moreover $I^{N+1}P_{N+1} = 0$, [7, Theorem 7][4] implies that $P_{>N} = P_{N+1} \oplus P_{>N+1}$ for some Z-submodule $P_{>N+1} \le P_{>N}$.

We claim that $\mathrm{ht}_{P_{>N+1}}(m) > N$ for any $m \in P_{>N+1}^Z$. Indeed, if $\mathrm{ht}_{P_{>N+1}}(m) = N$ then for any $u \in U_N$, $\mathrm{ht}_{P_{>N}}(m+u) = \min(\mathrm{ht}_{P_{>N+1}}(m), \mathrm{ht}_{P_{N+1}}(u)) = N$, contradicting the maximality of U_N, and proving the claim. As P_{N+1}^Z has no elements of height $\le N$, $P_{>N+1}$ has no Z-summands isomorphic to V_n, for $n \le N+1$. □

Proof of Proposition 5.3. As M decomposes as the direct product of its maximal free $\mathbb{F}_\ell[[Z]]$-quotient $V := \mathbb{F}_\ell[[Z]]^k$ and a submodule P with no free $\mathbb{F}_\ell[[Z]]$-quotients, its dual $\hat{M}$ decomposes as the direct sum of $\hat{V}$ and $\hat{P}$. Since V is a free

[4] See [7, §12] for the corresponding assertions for modules

$\mathbb{F}_\ell[[Z]]$-module, by Proposition 5.4.(b) $I\hat{V} = \hat{V}$ and hence $\hat{V}_\omega = \hat{V}$. It follows that the Ulm invariants of $\hat{M}$ and of $\hat{P}$ are the same.

By Lemma 5.13, $\hat{P}$ decomposes as $\hat{P}_{\le N} \oplus \hat{P}_{>N}$ where $\hat{P}_{\le N} = \oplus_{n\le N} V_n^{U_{n-1}(\hat{M})}$ and $\hat{P}_{>N}$ has no Z-summands of dimension $\le N$. Letting $P_{>N}$ and $P_{\le N}$ be the duals of $\hat{P}_{>N}$ and $\hat{P}_{\le N}$, respectively, by duality we have $M = V \times P_{\le N} \times P_{\ge N}$, where $P_{\le N} \cong \prod_{n\le N} V_n^{U_{n-1}(\hat{M})}$ and $P_{>N}$ has no free quotients and no direct Z-summands of dimension $\le N$. Note that since $\hat{P}_{\le N}$ can be chosen to be a direct Z-summand of $\hat{P}_{\le N+1}$, $M_{\le N} := V \times P_{\le N}$ is a direct Z-summand of $M_{\le N+1} = V \times P_{\le N+1}$ for all $N \in \mathbb{N}$, as needed for Part (a).

The limit $M_0 := \varprojlim M_{\le N}$ is Z-isomorphic to $V \times \prod_{n\in\mathbb{N}} V_n^{U_{n-1}(\hat{M})}$. Hence, its dual $\hat{M}_0$ is Z-isomorphic to $\hat{V} \oplus \bigoplus_{n\in\mathbb{N}} \hat{V}_n^{U_{n-1}(\hat{M})}$. As V_n is self dual, and $I\hat{V} = \hat{V}$, $\hat{M}_0$ has trivial infinite Ulm invariants. Thus by Ulm's theorem [7, Theorem 11], M is Z-isomorphic to M_0 if and only if M has trivial infinite Ulm invariant, proving Part (b). □

References

[1] I. Efrat, Valuations, orderings, and Milnor K-theory. Mathematical Surveys and Monographs, 124, AMS, Providence, RI (2006).

[2] I. Efrat, Finitely generated pro-p absolute Galois groups over global fields. J. Number Theory 77 (1999), no. 1, 83-96.

[3] B. Ferrero, L.C. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields. Ann. Math. 109 (1979), 377–395.

[4] M. D. Fried, M. Jarden, Field arithmetic. vol. 11, 2nd edn. Revised and enlarged by Moshe Jarden. Ergebnisse der Mathematik (3). Springer, Berlin (2005).

[5] M. G. Ikeda, Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem für galoissche Algebren. Abh. Math. Sem. Univ. Hamburg. 24 (1960), 126–131.

[6] K. Iwasawa, On $\mathbb{Z}_\ell$-extensions of algebraic number fields. Ann. Math. 98 (1973), 246–326.

[7] I. Kaplansky, Infinite abelian groups. University of Michigan Publications in Mathematics, no. 2., Ann Arbor, University of Michigan Press (1954).

[8] J. Koenigsmann, Solvable absolute Galois groups are metabelian. Invent. Math. 144 (2001), 1–22.

[9] H. Koch, Galoissche Theorie der p-Erweiterungen. Springer (1970).

[10] M. Jarden, Algebraic Patching. Springer, Heidelberg (2011).

[11] J. P. Labute, Demushkin groups of rank $\aleph_0$. Bull. Soc. Math. France 94 (1966), 211–244.

[12] J. P. Labute, Classification of Demushkin groups. Canad. J. Math. 19 (1967) 106-132.

[13] A. Ledet, Brauer type embedding problems. Fields Institute Monographs (2005).

[14] J. Mináč, J. Swallow, Galois embedding problems with cyclic quotient of order p. Israel J. Math. 145 (2005), 93-112.

[15] J. Mináč, A. Schultz, J. Swallow, Galois module structure of p-th-power classes of cyclic extensions of degree p^n. Proc. London Math. Soc. 92 (2006), 307-341.

[16] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of number fields. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 323. Springer-Verlag, Berlin (2000).

[17] J. Neukirch, Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper. Invent. Math. 6 (1969), 296–314.
[18] J. Neukirch, On solvable number fields. Invent. Math. 53 (1979), 135–164.
[19] F. Pop, Embedding problems over large fields. Ann. of Math. (2) 144 (1996), 1–34.
[20] I. Reiner, Maximal Orders. London Mathematical Society Monographs. New Series. 28. Oxford University Press (2003).
[21] L. Ribes, Introduction to Profinite groups and Galois cohomology. Queen's Papers in Pure and Appl. Math., Queen's university, Kingstone, Ont, no. 24 (1970).
[22] L. Ribes, P. A. Zalesskii, Profinite groups. vol. 40, 2nd edn. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, Springer-Verlag, Berlin, (2010).
[23] J.-P. Serre, Galois cohomology. Springer-Verlag, Berlin, (2002).
[24] L. Washington, Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York (1997).
[25] Y. Yamamoto, On unramified Galois extensions of quadratic number fields. Osaka J. Math. 7 (1970), 57–76.

School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 69978, Israel
E-mail address: barylior@post.tau.ac.il

School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 69978, Israel
E-mail address: jarden@post.tau.ac.il

Deptartment of Mathematics, 530 Church St., University of Michigan, Ann Arbor 48109, USA.
E-mail address: neftin@umich.edu