13 June 2018

Solving Embedding Problems with Bounded Ramification*

by

Moshe Jarden, Tel Aviv University, jarden@post.tau.ac.il

and

Nantsoina Cynthia Ramiharimanana, AIMS, nantsoina@aims.ac.za

Abstract: Let K/K_0 be a finite Galois extension of global fields. We prove that every finite embedding problem with a solvable kernel H for K/K_0 is solvable if it is locally solvable and satisfies two conditions on $\mathrm{char}(K_0)$ and the roots of unity in K.

Moreover, the solution can be chosen to coincide with finitely many (given in advance) local solutions. Finally, and this is the main point of this work, the number of primes of K_0 that ramify in the solution field is bounded by the number of primes of K_0 that ramify in K plus the number of prime divisors of $|H|$, counted with multiplicity.

MR Classification: 11R23

Table of Contents

* This work is an adjustment to global fields of the PhD thesis [Ram16] about number fields of the second author guided by the first author and Barry Green.

Introduction

A sharpened version of the inverse Galois problem is the so-called **embedding problem**. Given a Galois extension K/K_0 of global fields, a finite group G, and an epimorphism $\alpha\colon G \to \mathrm{Gal}(K/K_0)$, one looks for a Galois extension N of K_0 that contains K such that $\mathrm{Gal}(N/K_0) \cong G$ and the restriction map $\mathrm{res}_{N/K}\colon \mathrm{Gal}(N/K_0) \to \mathrm{Gal}(K/K_0)$ coincides with α. Equivalently, with $K_{0,\mathrm{sep}}$ being the separable algebraic closure of K_0, and $\mathrm{Gal}(K_0) = \mathrm{Gal}(K_{0,\mathrm{sep}}/K_0)$, one looks for a continuous epimorphism $\psi\colon \mathrm{Gal}(K_0) \to G$ such that $\alpha \circ \psi = \mathrm{res}_{K_{0,\mathrm{sep}}/K}$. We refer to ψ as a **proper solution** of the embedding problem (whereas, if ψ is only a homomorphism, as above, we say that ψ is a **weak solution** of the embedding problem). The question about the proper solvability of finite embedding problems over K_0 is of course far from being settled. But, in those cases where an embedding problem as above is solvable, one may ask whether a solution field as above can be found with a **bound on the ramification**, i.e., with a bound on the cardinality of the set $\mathrm{Ram}(N/K_0)$ of the primes of K_0 that are ramified in N.

Previous results. The combinatorial arguments of Shafarevich in [Sha54A] and [Sha54B] (which was corrected in [Sha89]) lead for each finite solvable group G to a Galois extension N of K with Galois group G such that the order of the set $\mathrm{Ram}(N/K)$ of primes of K which are ramified in N has an exponential growth in $|G|$. See also [NSW00, p. 476, Thm. 9.5.1].

The work [GeJ98] uses the method of Scholz [Sch37] and Reichardt [Rei37] in order to realize for each prime number l every finite l-group G over K under the condition $l \neq$

$\mathrm{char}(K)$ and $\zeta_l \notin K$. With $|G| = l^n$, the work [GeJ98] constructs a Galois extension N of K such that $\mathrm{Gal}(N/K) \cong G$ and $|\mathrm{Ram}(N/K)| \leq n + r(K)$, where $r(K)$ depends only on arithmetical invariants of K. If $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$, then $r(K) = 0$, so the result of [GeJ98] reproduces in this case a result of Serre in [Ser92] that $|\mathrm{Ram}(N/K)| \leq n$.

The main result of [GeJ98] is generalized by Markin and Ullom in [MaU11]. The latter work constructs for each number field K and every finite nilpotent group G a Galois extension N of K with Galois group G. Moreover, if $(G_i)_i$ is a lower central series of G and $d(G_i/G_{i+1})$ is the minimal number of generators of G_i/G_{i+1}, then $|\mathrm{Ram}(N/K)| \leq \sum_i d(G_i/G_{i+1}) + r(K)$.

Going back to the case of a finite embedding problem $\alpha\colon G \to \mathrm{Gal}(K/K_0)$ with $\mathrm{Ker}(\alpha)$ solvable for number fields, Neukirch observes in [Neu79] that for each prime divisor $\mathfrak{p}$ of K_0, the completions $\hat{K}_\mathfrak{p}/\hat{K}_{0,\mathfrak{p}}$ at $\mathfrak{p}$ gives rise to a local embedding problem. We denote the group of roots of unity in K by $\mu(K)$. In the spirit of Scholz-Reichardt, [Neu79] proves that if the group $\mathrm{Ker}(\alpha)$ is solvable, $\gcd(|\mathrm{Ker}(\alpha)|, |\mu(K)|) = 1$, and each of the local embedding problems is weakly solvable, then the original embedding problem is properly solvable. We denote the set of primes of the global field K_0 by $\mathbb{P}(K_0)$. For each $\mathfrak{p} \in \mathbb{P}(K_0)$ we identify $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ with a closed subgroup of $\mathrm{Gal}(K_0)$. Then, one may even find a proper solution that coincides on $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ with a given local weak solution $\varphi_\mathfrak{p}$ for finitely many $\mathfrak{p}$'s. However, [Neu79] gives no bound on the ramification of the proper solution. The results of [Neu79] are generalized to the case of global fields in [NSW15, p. 563, Thm. 9.5.5].

The main result. It is exactly the latter gap that our work intends to fill out. To this end we recall that if $n = \prod_{i=1}^m l_i^{r_i}$ is a decomposition of a positive integer n into a product of powers of distinct primes $l_1, \ldots, l_m$, then $\Omega(n) = \sum_{i=1}^m r_i$. If K is a finite extension of K_0, then $\mathrm{Ram}(K/K_0)$ denotes the set of $\mathfrak{p} \in \mathbb{P}(K_0)$ that ramify in K. Our main result is:

Theorem A: *Let K/K_0 be a finite Galois extension of global fields, set* $\Gamma = \mathrm{Gal}(K/K_0)$, *and consider a finite embedding problem*

(1)
$$\begin{tikzcd} & & & \mathrm{Gal}(K_0) \arrow[d, "\rho"] & \\ 1 \arrow[r] & H \arrow[r] & G \arrow[r, "\alpha"] & \Gamma \arrow[r] & 1, \end{tikzcd}$$

with a solvable kernel H. Suppose that

(a1) $\mathrm{char}(K_0) \nmid |H|$, $\gcd(|H|, |\mu(K)|) = 1$, *and*

(a2) *for each $\mathfrak{p} \in \mathbb{P}(K_0)$ there exists a homomorphism $\psi_\mathfrak{p}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to G$ such that $\alpha \circ \psi_\mathfrak{p} = \rho|_{\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})}$ (we call $\psi_\mathfrak{p}$ a* **local solution***).*

Let T be a finite subset of $\mathbb{P}(K_0)$ that contains $\mathrm{Ram}(K/K_0)$ and for each $\mathfrak{p} \in T$ let $\varphi_\mathfrak{p}$ be a local solution.

Then, there exists an epimorphism $\psi\colon \mathrm{Gal}(K_0) \to G$ such that $\alpha \circ \psi = \rho$, and there exists a set $R \subseteq \mathbb{P}(K_0) \smallsetminus T$ with $|R| = \Omega(|H|)$ that satisfies the following conditions:

(b1) *For each $\mathfrak{p} \in T$ there exists $a \in H$ such that $\psi(\sigma) = a^{-1}\varphi_\mathfrak{p}(\sigma)a$ for all $\sigma \in \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$.*

(b2) *The fixed field N in $K_{0,\mathrm{sep}}$ of $\mathrm{Ker}(\psi)$ satisfies $\mathrm{Ram}(N/K_0) \subseteq T \cup R$, hence $|\mathrm{Ram}(N/K_0)| \leq |T| + \Omega(|H|)$.*

Special cases. Note that if the short exact sequence in (1) splits, then the condition in Theorem A about the local solvability is automatically satisfied. Thus, in this case, Theorem A holds under the mere conditions that H is solvable, $\mathrm{char}(K_0) \nmid |H|$, and $\gcd(|H|, |\mu(K)|) = 1$.

Also, let S be a finite subset of $\mathbb{P}(K_0)$ and denote the maximal Galois extension of K_0 in which each $\mathfrak{p} \in S$ totally splits by $K_{0,\mathrm{tot},S}$. Suppose that $K \subseteq K_{0,\mathrm{tot},S}$. Then, we may assume that $S \subseteq T$ and take $\varphi_\mathfrak{p}$ for each $\mathfrak{p} \in S$ as the trivial homomorphism. We find that the solution field N of (1) is contained in $K_{0,\mathrm{tot},S}$.

Finally, we note that if we take $K = K_0$, $T = \emptyset$, and $|G| = l^n$, where l is a prime number such that $l \neq \mathrm{char}(K)$ and $\zeta_l \notin K$, in Theorem A, then we get a Galois extension N of K with Galois group G such that $|\mathrm{Ram}(N/K)| \leq n$. This improves the estimate $|\mathrm{Ram}(N/K)| \leq n + r(K)$ of the main result of [GeJ98] mentioned above.

Remark. In a forthcoming paper, we plan to remove the condition $\mathrm{char}(K_0) \nmid |H|$ from (a1) of Theorem A, keeping $\gcd(|H|, |\mu(K)|) = 1$ as the only condition on the solvable group H in the theorem.

Simple $\mathrm{Gal}(K_0)$-module. An induction on the order of H reduces Theorem A to the following result:

Proposition B: *Let K/K_0 be a finite Galois extension of global fields and l a prime number. Set $\Gamma = \mathrm{Gal}(K/K_0)$ and $\rho = \mathrm{res}_{K_{0,\mathrm{sep}}/K}$. Then, consider the diagram*

(2)
$$\begin{tikzcd}
 & & G \arrow[d, "\gamma"] & \mathrm{Gal}(K_0) \arrow[d, "\rho"] & \\
\mathbf{1} \arrow[r] & A \arrow[r] & \bar{G} \arrow[r, "\bar{\alpha}"] & \Gamma \arrow[r] & \mathbf{1},
\end{tikzcd}$$

with a short exact sequence, where $A \cong C_l^r$ is a simple $\mathrm{Gal}(K_0)$-module (through ρ and $\bar{\alpha}$; in particular $\mathrm{Gal}(K)$ acts trivially on A) and $\gamma\colon G \to \bar{G}$ is an epimorphism of finite groups with a non-trivial solvable kernel. Let n be a multiple of $l \cdot |\mathrm{Ker}(\gamma)|$. Suppose that

(c1) $\mathrm{char}(K_0) \nmid n$, $\gcd(n, |\mu(K)|) = 1$, *and*

(c2) *for each $\mathfrak{p} \in \mathbb{P}(K_0)$ there exists a homomorphism $\psi_{\mathfrak{p}}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to \bar{G}$ such that $\bar{\alpha} \circ \psi_{\mathfrak{p}} = \rho|_{\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})}$.*

Let T be a finite subset of $\mathbb{P}(K_0)$ that contains $\mathrm{Ram}(K/K_0)$ and for each $\mathfrak{p} \in T$ let $\bar{\varphi}_{\mathfrak{p}}$ be a local solution. Then, there exists an epimorphism $\bar{\psi}\colon \mathrm{Gal}(K_0) \to \bar{G}$ such that $\bar{\alpha} \circ \bar{\psi} = \rho$ and there exists a subset $\bar{R}$ of $\mathbb{P}(K_0) \smallsetminus T$ with $|\bar{R}| = \Omega(|A|) = r$ that satisfies the following conditions:

(d1) *For each $\mathfrak{p} \in T$ there exists $a \in A$ such that $\bar{\psi}(\sigma) = a^{-1}\bar{\varphi}_{\mathfrak{p}}(\sigma)a$ for all $\sigma \in \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$.*

(d2) *The fixed field $\bar{K}$ in $K_{0,\mathrm{sep}}$ of $\mathrm{Ker}(\bar{\psi})$ satisfies $\mathrm{Ram}(\bar{K}/K_0) \subseteq T \cup \bar{R}$.*

(d3) $\gcd(n, |\mu(\bar{K})|) = 1$.

(d4) *For each $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus T$ there exists a homomorphism $\psi'_{\mathfrak{p}}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to G$ such that $\gamma \circ \psi'_{\mathfrak{p}} = \bar{\psi}|_{\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})}$.*

The proof of Proposition B follows [Neu79] except for the control on the ramification for which we prove and apply an improved version (Lemma 2.3) of [GeJ98, Lemma 7.1].

A COMPARISON OF ESTIMATES. We would like to stress that the vanishing of the constant $r(K)$ that appears both in [GeJ98] and [MaU11] is an essential ingredient of our result and its proof. Indeed, take for simplicity $T = \emptyset$. Assume in the context of Diagram (2) that we could only find an epimorphism $\bar{\psi}$: $\mathrm{Gal}(K_0) \to \bar{G}$ such that $\bar{\alpha} \circ \bar{\psi} = \rho$ and the fixed field $\bar{K}$ of $\mathrm{Ker}(\bar{\psi})$ in $K_{0,\mathrm{sep}}$ satisfies $|\mathrm{Ram}(\bar{K}/K_0)| \leq |\mathrm{Ram}(K/K_0)| + \Omega(|\mathrm{Ker}(\bar{\alpha})|) + r(K)$. Then, in the induction step, we would be able to find an epimorphism ψ: $\mathrm{Gal}(K_0) \to G$ such that $\gamma \circ \psi = \bar{\psi}$ and the fixed field N of $\mathrm{Ker}(\psi)$ would satisfy

(3) $|\mathrm{Ram}(N/K_0)| \leq |\mathrm{Ram}(K/K_0)| + \Omega(|\mathrm{Ker}(\bar{\alpha} \circ \gamma)|) + r(K) + r(\bar{K})$.

Unfortunately our proof gives no control on $\bar{K}$, so we cannot bound $r(\bar{K})$ in terms of the initial data of the embedding problem. Thus, (3) would only say that $\mathrm{Ram}(N/K_0)$ is a finite set, so the whole point of our result would disappear.

ELIMINATION OF $r(K)$. The rest of the introduction overviews the proof of Proposition B with an emphasize on the bound on the ramification of the solution of embedding problem (2). Among others, it explains how $r(K)$ disappears from the bound on the ramification.

A LOCAL-GLOBAL PRINCIPLE. Since (2) is locally solvable (by (c2)), a local global principle (Lemma 10.6), yields a weak solution ψ_0 to embedding problem (2).

We adjust ψ_0 to the desired proper solution by using two degrees of freedom. First, for each $a \in A$, we may replace ψ_0 by the homomorphism ψ_0': $\mathrm{Gal}(K_0) \to \bar{G}$ defined by $\psi_0(\sigma) = a^{-1}\psi_0(\sigma)a$. We say that ψ_0' is **A-equivalent** to ψ_0 and denote the equivalence class of ψ_0 by $[\psi_0]$. Then, we denote the set of all equivalence classes by $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), \bar{G})$ and define a free transitive action of $H^1(\mathrm{Gal}(K_0), A)$ on $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), \bar{G})$. Similarly, for each prime $\mathfrak{p}$ of K_0 we set $\rho_{\mathfrak{p}} = \rho|_{\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})}$. Then, $\mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), \bar{G})$ is a principal homogeneous space under the action of $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ (Lemma 10.4). The actions involving the global and the local principal homogeneous spaces are our second degree of freedom.

The set $S_{0,l}(K)$. The constant $r(K)$ mentioned above is the cardinality of a finite subset $S_{0,l}(K)$ of $\mathbb{P}(K)$ introduced in Subsection 1.6. Among others, $S_{0,l}(K)$ contains all archimedean primes of K and all primes that lie over l (if K is a number field). Let $\mathfrak{s}_1, \ldots, \mathfrak{s}_k$ be the elements of $S_{0,l}(K)|_{K_0} \smallsetminus T$. Since $\mathrm{Ram}(K/K_0) \subseteq T$, the primes $\mathfrak{s}_1, \ldots, \mathfrak{s}_k$ are unramified in K.

Surjectivity and number of roots of unity. We take care of the surjectivity and the number of roots of unity in the solution field by using the Chebotarev density theorem. Let m be the smallest number of generators of $\mathrm{Gal}(K(\zeta_n)/K)$. We use Lemma 11.2 in order to choose non-archimedean primes $\mathfrak{q}, \mathfrak{p}_1, \ldots, \mathfrak{p}_m$ of K_0 away from $T \cup \{\mathfrak{s}_1, \ldots, \mathfrak{s}_k\}$ that totally split in K and for each $\mathfrak{p} \in \{\mathfrak{s}_1, \ldots, \mathfrak{s}_k\} \cup \{\mathfrak{q}, \mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ an unramified local solution $\varphi_\mathfrak{p}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to \bar{G}$ such that if a weak solution $\bar{\psi}$ of (2) coincides with $\varphi_\mathfrak{p}$ on $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$, then $\bar{\psi}$ is surjective and $\gcd(|H|, |\mu(\bar{N})|) = 1$, where H is the group appearing in (1) and $\bar{N}$ is the solution field associated with $\bar{\psi}$. We set $T^* = T \cup \{\mathfrak{s}_1, \ldots, \mathfrak{s}_k\} \cup \{\mathfrak{q}, \mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$. We have to make sure that, among others, $\{\mathfrak{s}_1, \ldots, \mathfrak{s}_k\}$ remain unramified in the solution field of (2) that we construct.

Elimination of extra ramification. Let $\mathfrak{r}_1, \ldots, \mathfrak{r}_s$ be the primes of K_0 away from T^* where ψ_0 ramifies, and set $T^{**} = T^* \mathbin{\dot\cup} \{\mathfrak{r}_1, \ldots, \mathfrak{r}_s\}$. Then, ψ_0 is unramified at each $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus T^{**}$. By Part C of the proof of Proposition 12.3, there exists an unramified local solution $\varphi_\mathfrak{p}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to \bar{G}$ of (2) for each $\mathfrak{p} \in \{\mathfrak{r}_1, \ldots, \mathfrak{r}_s\}$. Unfortunately, we have no control on s. However, we are able to change ψ_0 in such away that it becomes ramified, in addition to on $\mathrm{Ram}(K/K_0)$, only on r new primes of K_0 away from T^{**}.

In order to do so, we choose for each $\mathfrak{p} \in T^{**}$ an element $y_\mathfrak{p} \in H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ such that $[\varphi_\mathfrak{p}] = [\psi_{0,\mathfrak{p}}]^{y_\mathfrak{p}}$. Then, Proposition 9.3, applied to T^{**} rather than to T, yields an $x \in H^1(\mathrm{Gal}(K_0), A)$ such that $\mathrm{res}_\mathfrak{p}(x) = y_\mathfrak{p}$ for each $\mathfrak{p} \in T^{**}$ and a set $\bar{R} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$ such that x is unramified away from $T \cup \bar{R}$. Then, $\bar{\psi}$ with $[\bar{\psi}] = [\psi_0]^x$ is a solution of (2) that satisfies $[\bar{\psi}_\mathfrak{p}] = [\varphi_\mathfrak{p}]$ for each $\mathfrak{p} \in T$ and $\mathrm{Ram}(\bar{N}/K_0) = T \cup \bar{R}$. Indeed, by its choice, $[\varphi_\mathfrak{p}]$ is unramified if $\mathfrak{p} \in T^{**} \smallsetminus T$, and $[\bar{\psi}_\mathfrak{p}] = [\psi_{0,\mathfrak{p}}]^{\mathrm{res}_\mathfrak{p}(x)}$ is unramified if both $[\psi_{0,\mathfrak{p}}]$ and $\mathrm{res}_\mathfrak{p}(x)$ are unramified (Lemma 10.5).

The construction of x. Let $(y_\mathfrak{p})_{\mathfrak{p}\in T^{**}}$ be the local data given in the preceding paragraph. Lemma 9.2 yields an element $z \in H^1(\mathrm{Gal}(K_0), A)$ such that $\mathrm{res}_\mathfrak{p}(z) = y_\mathfrak{p}$ for each $\mathfrak{p} \in T^{**}$. Moreover, $\mathfrak{p}$ totally splits in $K(\zeta_l)$ if $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus T^{**}$ and $\mathrm{res}_\mathfrak{p}(z)$ is ramified. Then, we consider the set $V = T^{**} \cup \{\mathfrak{p} \in \mathbb{P}(K_0) \mid \mathrm{res}_\mathfrak{p}(z) \text{ is ramified}\}$. We define an element $\eta_\mathfrak{p} \in H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ for each $\mathfrak{p} \in V$ by $\eta_\mathfrak{p} = 1$ if $\mathfrak{p} \in T^{**}$ and $\eta_\mathfrak{p} = \mathrm{res}_\mathfrak{p}(z)^{-1}$ if $\mathfrak{p} \in V \smallsetminus T^{**}$. We prove, in the notation of commutative diagram (1) of Section 5 for $n = 1$, that for each $\mathfrak{p} \in V$ and every $\mathfrak{P}$ in $\mathbb{P}(K)$ over $\mathfrak{p}$ there exists an element $\tilde{\eta}_\mathfrak{P} \in H^1(\mathrm{Gal}(\hat{K}_\mathfrak{P}), A)$ such that $\eta_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{cor}_\mathfrak{P}(\tilde{\eta}_\mathfrak{P})$.

By Proposition 4.2, there exists a homomorphism $h\colon \mathrm{Gal}(K) \to A$, primes $\mathfrak{q}_1, \dots, \mathfrak{q}_r \in \mathbb{P}(K_0) \smallsetminus V$, and primes $\mathfrak{Q}_1, \dots, \mathfrak{Q}_r \in \mathbb{P}(K)$, respectively over $\mathfrak{q}_1, \dots, \mathfrak{q}_r$, such that among others, $\mathrm{res}_\mathfrak{P}(h) = \tilde{\eta}_\mathfrak{P}$ for all $\mathfrak{P} \in V_K$ and h is unramified on $\mathbb{P}(K) \smallsetminus (V_K \cup \{\mathfrak{Q}_1, \dots, \mathfrak{Q}_r\})$.

Let u be the image of h under the map $\mathrm{cor}\colon H^1(\mathrm{Gal}(K), A) \to H^1(\mathrm{Gal}(K_0), A)$. We prove that $x = uz$ has the desired properties mentioned under heading “Elimination of extra ramification”.

On the construction of h. The construction proceeds by induction on r (where we recall that $A = C_l^r$). The main case, where $r = 1$ is carried out in Corollary 3.3. That corollary is a translation of Lemma 2.3 via the reciprocity law of class field theory.

Finally, Lemma 2.3 is a generalization of [GeJ98, Lemma 7.1]. We consider a tower $K_0 \subseteq K \subseteq L$ of finite Galois extensions of global fields such that $\zeta_l \notin K$ and L/K is an abelian l-extension (in particular $l \neq \mathrm{char}(K_0)$). Let $n = ql^m$ with $\mathrm{char}(K_0) \nmid q$ and let S be a finite subset of $\mathbb{P}(K)$ that contains $S_{0,l}(K)$. For each $\mathfrak{P} \in S$ let $h_\mathfrak{P}$ be a homomorphism from $\hat{K}_\mathfrak{P}^\times$ into C_l. Then, there exists a non-archimedean prime $\mathfrak{q} \in \mathbb{P}(K_0) \smallsetminus S|_{K_0}$ and a homomorphism h of the idele class group C_K into C_l such that $\mathfrak{q}$ totally splits in $L(\zeta_n)$ (here we use the Chebotarev density theorem), $h|_{\hat{K}_\mathfrak{P}^\times} = h_\mathfrak{P}$ for each $\mathfrak{P} \in S$, there exists $\mathfrak{Q} \in \mathbb{P}(K)$ over $\mathfrak{q}$ with $h(U_\mathfrak{Q}) = C_l$, and $h(U_\mathfrak{P}) = \mathbf{1}$ for each $\mathfrak{P} \in \mathbb{P}(K) \smallsetminus (S \cup \{\mathfrak{Q}\})$. Here $U_\mathfrak{Q}$ (resp. $U_\mathfrak{P}$) are the groups of units of $\hat{K}_\mathfrak{Q}$ (resp. $\hat{K}_\mathfrak{P}$). Note that the latter condition eventually translates into the desired non-ramification condition in the solution field of most of the primes of K_0.

ACKNOWLEDGEMENTS: Our sincere thanks go to Wulf-Dieter Geyer for his constant interest and valued support during this work. We thank Aharon Razon for a careful reading of earlier drafts of the work. We also acknowledge a communication with Kay Wingberg on the structure of the proof by induction. Finally, we thank the anonymous referee for useful suggestions and advice.

1. Preliminaries

PREL
input, 15

A large part of this work is dominated by class field theory and cohomology theory of global fields. In this section we provide the necessary notions connected to global fields, their localizations and completions, and the corresponding groups of ideles.

1.1 NOTATION. For each field K we choose a separable algebraic closure K_{sep} and let $\mathrm{Gal}(K) = \mathrm{Gal}(K_{\mathrm{sep}}/K)$ be the absolute Galois group of K. NOT input, 25

If K is a global field, we let $\mathbb{P}(K)$ be the set of all primes of K. Then, $\mathbb{P}_{\mathrm{arch}}(K)$ is the set of all archimedean primes of K and $\mathbb{P}_{\mathrm{nonarch}}(K)$ is the set of all non-archimedean primes of K. We also write $\mu(K)$ for the group of roots of unity that belong to K. For each positive integer n with $\mathrm{char}(K) \nmid n$, we fix a root of unity ζ_n in K_{sep} of order n.

We use the letter l as a variable on the set of prime numbers and set C_l to be the (multiplicative) cyclic group of order l. Also, we denote the trivial subgroup of each multiplicative group A by $\mathbf{1}_A$ or by $\mathbf{1}$ if A is known from the context.

Finally, we write $A \mathbin{\dot\cup} B$ and $\dot\bigcup_{i=1}^{n} A_i$ to signify that the unions are disjoint.

1.2 TOPOLOGICAL GROUPS. We consider several types of topological groups: finite groups (equipped with discrete topology), arbitrary discrete groups, profinite groups, locally compact groups, and idele groups of global fields (that are also locally compact). Whenever we speak about homomorphisms between topological groups, we tacitly assume that they are continuous. On the rare occasion that a map $\varphi\colon G \to A$ between topological groups is constructed from previously given (continuous) homomorphisms, and we only know that $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$, then we refer to φ as an "abstract homomorphism". PREa input, 54

1.3 Global Fields and their Localizations and Completions. For the rest of this work we fix a global field K_0 of characteristic p. Thus, K_0 is either a number field and $p = 0$, or K_0 is a function field of one variable over a finite field of a positive characteristic p. PREb input, 73

For each $\mathfrak{p} \in \mathbb{P}(K_0)$ we fix a completion $\hat{K}_{0,\mathfrak{p}}$ of K_0 at $\mathfrak{p}$ that contains K_0 and let $\hat{K}_{0,\mathfrak{p},\mathrm{sep}}$ be a separable algebraic closure of $\hat{K}_{0,\mathfrak{p}}$ that contains $K_{0,\mathrm{sep}}$, thereby extending $\mathfrak{p}$ to $K_{0,\mathrm{sep}}$. Let $K_{0,\mathfrak{p}} = \hat{K}_{0,\mathfrak{p}} \cap K_{0,\mathrm{sep}}$. If $\mathfrak{p}$ is archimedean and real (resp. complex), then $K_{0,\mathfrak{p}}$ is a real (resp. algebraic) closure of K_0 at $\mathfrak{p}$. If $\mathfrak{p}$ is non-archimedean, then $K_{0,\mathfrak{p}}$ is a Henselian closure of K_0 at $\mathfrak{p}$.

In the latter case we denote the residue field of K_0 at $\mathfrak{p}$ by $\bar{K}_{0,\mathfrak{p}}$. By Krasner's lemma, $K_{0,\mathrm{sep}}\hat{K}_{0,\mathfrak{p}} = \hat{K}_{0,\mathfrak{p},\mathrm{sep}}$. The same equality also holds for the archimedean primes. It follows that in each case

$$\mathrm{res}_{\hat{K}_{0,\mathfrak{p},\mathrm{sep}}/K_{0,\mathrm{sep}}}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to \mathrm{Gal}(K_{0,\mathfrak{p}})$$

is an isomorphism. We identify $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ with $\mathrm{Gal}(K_{0,\mathfrak{p}})$ under this isomorphism.

For $\mathfrak{p} \in \mathbb{P}(K_0)$ we write $\mathfrak{p} \nmid l, \infty$ if $\mathfrak{p}$ is non-archimedean and $\mathrm{char}(\bar{K}_{\mathfrak{p}}) \neq l$. In the number field case this means that $\mathfrak{p}$ lies neither over l nor over ∞. In the function field case this simply means that $l \neq \mathrm{char}(K_0)$.

For each $\mathfrak{p} \in \mathbb{P}_{\mathrm{nonarch}}(K_0)$, we denote the maximal unramified extension of $\hat{K}_{0,\mathfrak{p}}$ by $\hat{K}_{0,\mathfrak{p},\mathrm{ur}}$ and let $\hat{I}_{\mathfrak{p}} = \mathrm{Gal}(\hat{K}_{0,\mathfrak{p},\mathrm{ur}})$ be the corresponding inertia group.

Next, we denote the normalized $\mathfrak{p}$-adic discrete valuation of $\hat{K}_{0,\mathfrak{p}}$ by $\mathrm{ord}_{\mathfrak{p}}$ and extend it to $\hat{K}_{0,\mathfrak{p},\mathrm{sep}}$ in the unique possible way. We fix an element $\pi_{\mathfrak{p}}$ of $\hat{K}_{0,\mathfrak{p}}$ with $\mathrm{ord}_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = 1$. Let $O_{\mathfrak{p}} = \{z \in \hat{K}_{0,\mathfrak{p}} \mid \mathrm{ord}_{\mathfrak{p}}(z) \geq 0\}$ be the **ring of integers** of $\hat{K}_{0,\mathfrak{p}}$ and let $U_{\mathfrak{p}} = \{z \in \hat{K}_{0,\mathfrak{p}} \mid \mathrm{ord}_{\mathfrak{p}}(z) = 0\}$ be the **group of units** of $O_{\mathfrak{p}}$. Note that $\hat{K}_{0,\mathfrak{p}}^{\times} = \langle \pi_{\mathfrak{p}} \rangle \times U_{\mathfrak{p}}$, where $\langle \pi_{\mathfrak{p}} \rangle = \{\pi_{\mathfrak{p}}^m \mid m \in \mathbb{Z}\}$ is the discrete subgroup of $\hat{K}_{0,\mathfrak{p}}^{\times}$ generated by $\pi_{\mathfrak{p}}$. As such, $\langle \pi_{\mathfrak{p}} \rangle$ is closed in $\hat{K}_{0,\mathfrak{p}}^{\times}$. By [Ser79, p. 66] $U_{\mathfrak{p}} = \varprojlim U_{\mathfrak{p}}/(1 + \pi_{\mathfrak{p}}^i O_{\mathfrak{p}})$ and by [Ser79, p. 66, Prop. 6] $U_{\mathfrak{p}}/(1 + \pi_{\mathfrak{p}}^i O_{\mathfrak{p}})$ is a finite group, hence $U_{\mathfrak{p}}$ is a profinite group.

If ψ is a homomorphism from $\mathrm{Gal}(K_0)$ into a finite group G, we denote the restriction of ψ to $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ (which is by our identification the restriction of ψ to $\mathrm{Gal}(K_{0,\mathfrak{p}})$) by $\psi_{\mathfrak{p}}$.

1.4 Extensions of Primes. Next we consider a finite Galois extension K of K_0 and a prime $\mathfrak{p} \in \mathbb{P}(K_0)$. Let x be a primitive element of K/K_0 and set $f = \mathrm{irr}(x, K_0)$. The polynomial f decomposes over $\hat{K}_{0,\mathfrak{p}}$ into distinct irreducible factors, $f(X) = \prod_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}}(X)$, where $\mathfrak{P}$ ranges over all primes of K that lie over $\mathfrak{p}$ [Neu99, p. 163, Prop. 8.2]. For each $\mathfrak{P}$ over $\mathfrak{p}$ we choose a root $x_{\mathfrak{P}}$ of $f_{\mathfrak{P}}$ in $\hat{K}_{0,\mathfrak{p},\mathrm{sep}}$ (which actually lies in K), write $\hat{K}_{\mathfrak{P}} = \hat{K}_{0,\mathfrak{p}}(x_{\mathfrak{P}})$, and let $\lambda_{\mathfrak{P}}\colon K \to \hat{K}_{\mathfrak{P}}$ be the K_0-embedding of K into $\hat{K}_{\mathfrak{P}}$ that maps x onto $x_{\mathfrak{P}}$. Then, we extend $\lambda_{\mathfrak{P}}$ to an embedding $\lambda_{\mathfrak{P}}\colon K_{0,\mathrm{sep}} \to \hat{K}_{0,\mathfrak{p},\mathrm{sep}}$ and observe that $K_{\mathfrak{P}} = (\hat{K}_{\mathfrak{P}})^{\lambda_{\mathfrak{P}}^{-1}}$ is a Henselian (resp. real or separable algebraic) closure of K at $\mathfrak{P}$ and $\hat{K}_{\mathfrak{P}}$ is a completion of K at $\mathfrak{P}$. By definition, $K_{0,\mathrm{sep}} \cap \hat{K}_{\mathfrak{P}} = K_{\mathfrak{P}}^{\lambda_{\mathfrak{P}}}$ and $K_{0,\mathrm{sep}}\hat{K}_{\mathfrak{P}} = \hat{K}_{0,\mathfrak{p},\mathrm{sep}}$ (because $K_{0,\mathrm{sep}}\hat{K}_{0,\mathfrak{p}} = \hat{K}_{0,\mathfrak{p},\mathrm{sep}}$). Hence, we may identify $\mathrm{Gal}(\hat{K}_{\mathfrak{P}})$ with $\mathrm{Gal}(K_{\mathfrak{P}}^{\lambda_{\mathfrak{P}}})$. Having done that, we have $\mathrm{Gal}(K_{\mathfrak{P}})^{\lambda_{\mathfrak{P}}} = \mathrm{Gal}(\hat{K}_{\mathfrak{P}})$. PREc input, 152

If in addition, $\mathfrak{P}$ is non-archimedean, we write $K_{\mathfrak{P},\mathrm{ur}}$ (resp. $\hat{K}_{\mathfrak{P},\mathrm{ur}}$) for the maximal unramified extension of $K_{\mathfrak{P}}$ (resp. $\hat{K}_{\mathfrak{P}}$), and set $I_{\mathfrak{P}} = \mathrm{Gal}(K_{\mathfrak{P},\mathrm{ur}})$ (resp. $\hat{I}_{\mathfrak{P},\mathrm{ur}} = \mathrm{Gal}(\hat{K}_{\mathfrak{P},\mathrm{ur}})$) for the corresponding inertia group.

Note that the primitive element x of K/K_0 mentioned in the preceding paragraph is a root of $f_{\mathfrak{P}}$ for a unique $\mathfrak{P}$ over $\mathfrak{p}$. In this case we choose $x_{\mathfrak{P}}$ to be x and conclude that the embedding $\lambda_{\mathfrak{P}}\colon K \to \hat{K}_{\mathfrak{P}}$ is the inclusion map. In this case $K_{0,\mathfrak{p}} \subseteq K_{\mathfrak{P}}$.

For each homomorphism $h\colon \mathrm{Gal}(K) \to A$ we write $\mathrm{res}_{\mathfrak{P}}(h)\colon \mathrm{Gal}(\hat{K}_{\mathfrak{P}}) \to A$ for the homomorphism defined by $\mathrm{res}_{\mathfrak{P}}(h)(\sigma) = h(\sigma^{\lambda_{\mathfrak{P}}^{-1}})$ for each $\sigma \in \mathrm{Gal}(\hat{K}_{\mathfrak{P}})$.

Given a subset S of $\mathbb{P}(K_0)$, we write S_K for the set of all primes of K that lie over S. Conversely, for each subset T of $\mathbb{P}(K)$, we denote the set of primes of K_0 that lie under T by $T|_{K_0}$.

1.5 Total splitting and unramification. Let K_0, K, and $\mathfrak{p}$ be as in Subsection 1.4. Then, $\mathfrak{p}$ **totally splits** in K if the number of prime divisors $\mathfrak{P}$ of K that lie over $\mathfrak{p}$ is equal to $[K : K_0]$. If $\mathfrak{p} \in \mathbb{P}_{\mathrm{nonarch}}(K)$, then the latter statement is equivalent to the condition that the Frobenius automorphism $\left[\frac{K/K_0}{\mathfrak{P}}\right]$ is the trivial element of $\mathrm{Gal}(K/K_0)$. Alternatively, $K \subseteq \hat{K}_{0,\mathfrak{p}}$. Alternatively, $\hat{K}_{\mathfrak{P}} = \hat{K}_{0,\mathfrak{p}}$, so $\mathrm{Gal}(\hat{K}_{\mathfrak{P}}) = \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ for all (alternatively, for one) $\mathfrak{P}|\mathfrak{p}$. SPLT input, 210

A non-archimedean prime $\mathfrak{p}$ of K_0 is **unramified** in K if and only if for each $\mathfrak{P}|\mathfrak{p}$ the extension $\hat{K}_{\mathfrak{P}}/\hat{K}_{0,\mathfrak{p}}$ is unramified, alternatively $K \subseteq \hat{K}_{0,\mathfrak{p},\mathrm{ur}}$. This is the case if and only if $\hat{I}_{\mathfrak{P}} = \hat{I}_{\mathfrak{p}}$.

Following the convention at [NSW15, p. 523, first paragraph], we say that an archimedean prime $\mathfrak{p}$ of K_0 is **unramified** in K if $\mathfrak{p}$ totally splits in K. This means that $K \subseteq \hat{K}_{0,\mathfrak{p}}$.

We denote the set of all primes of K_0 that ramify in K by $\mathrm{Ram}(K/K_0)$.

1.6 Basic Set of Primes. Let K be a global field and consider $\mathfrak{P} \in \mathbb{P}(K)$. If $\mathfrak{P}$ is PREi input, 241
archimedean, then $\hat{K}_{\mathfrak{P}} = \mathbb{R}$ or $\hat{K}_{\mathfrak{P}} = \mathbb{C}$. In this case we set $U_{\mathfrak{P}}$ to be the set of positive elements of $\hat{K}_{\mathfrak{p}}$ if $\mathfrak{P}$ is real and $\hat{K}_{\mathfrak{P}}^{\times}$ if $\mathfrak{P}$ is complex. In each case we set $\pi_{\mathfrak{P}} = 1$. If $\mathfrak{P}$ is non-archimedean, then we choose a prime element $\pi_{\mathfrak{P}}$ with $\mathrm{ord}_{\mathfrak{P}}(\pi_{\mathfrak{P}}) = 1$, and set $U_{\mathfrak{P}} = \{x \in \hat{K}_{\mathfrak{P}} \mid \mathrm{ord}_{\mathfrak{P}}(x) = 0\}$ to be the **group of units** of $\hat{K}_{\mathfrak{P}}$.

Recall that an **idele** of K is an element $\alpha = (\alpha_{\mathfrak{P}})_{\mathfrak{P}} \in \prod_{\mathfrak{P} \in \mathbb{P}(K)} \hat{K}_{\mathfrak{P}}^{\times}$, where $\alpha_{\mathfrak{P}} \in U_{\mathfrak{P}}$ for all by finitely many $\mathfrak{P}$'s. The ideles of K form a multiplicative group denoted by I_K. The group I_K becomes a topological group under the **restricted topology**. A basis of neighborhoods of 1 in I_K is the collection of sets $\prod_{\mathfrak{P} \in S} V_{\mathfrak{P}} \times \prod_{\mathfrak{P} \notin S} U_{\mathfrak{P}}$, where S ranges over the finite sets of primes of K and the $V_{\mathfrak{P}}$'s run over a basis of neighborhoods of $1 \in \hat{K}_{\mathfrak{P}}^{\times}$. In particular, $U_K = \prod_{\mathfrak{P} \in \mathbb{P}(K)} U_{\mathfrak{P}}$ is an open subgroup of I_K.

Another open subgroup of I_K is obtained for each finite subset S of $\mathbb{P}(K)$. It is the group $I_{K,S} = \prod_{\mathfrak{P} \in S} \hat{K}_{\mathfrak{P}}^{\times} \times \prod_{\mathfrak{P} \notin S} U_{\mathfrak{P}}$ of the **S-ideles** of K.

The multiplicative group $K^{\times}$ is embedded diagonally in I_K. As such $K^{\times}$ is discrete and therefore closed in I_K [Neu99, p. 361, Prop. VI.1.5]. The factor group $C_K = I_K/K^{\times}$ is the **idele class group** of K. It is a Hausdorff locally compact group [Neu99, p. 361].

For each $\mathfrak{P} \in \mathbb{P}(K)$, the multiplicative group $\hat{K}_{\mathfrak{P}}^{\times}$ naturally embeds into I_K. The image of an element $x \in \hat{K}_{\mathfrak{P}}^{\times}$ under this embedding is the family $(x_{\mathfrak{P}'})_{\mathfrak{P}' \in \mathbb{P}(K)}$, where $x_{\mathfrak{P}'} = 1$ for $\mathfrak{P}' \neq \mathfrak{P}$ and $x_{\mathfrak{P}} = x$. Note that if y is another element of $\hat{K}_{\mathfrak{P}}^{\times}$, $a \in K^{\times}$, and $a(x_{\mathfrak{P}'})_{\mathfrak{P}' \in \mathbb{P}(K)} = (y_{\mathfrak{P}'})_{\mathfrak{P}' \in \mathbb{P}(K)}$, then $a = 1$, so $x = y$. This gives an embedding of $\hat{K}_{\mathfrak{P}}^{\times}$ into $C_K = I_K/K^{\times}$. Note that the image of $\hat{K}_{\mathfrak{P}}^{\times}$ in I_K is closed, hence so is the image of $\hat{K}_{\mathfrak{P}}^{\times}$ in C_K. We identify $\hat{K}_{\mathfrak{P}}^{\times}$ with its image in C_K.

For a set S of primes of K that contains $\mathbb{P}_{\mathrm{arch}}(K)$, we define the group of S-units of K as $K_S = \{x \in K \mid \mathrm{ord}_{\mathfrak{P}}(x) = 0 \text{ for all } \mathfrak{P} \notin S\}$. Then, $K_S = I_{K,S} \cap K^{\times}$.

By [Neu99, p. 360, Prop. VI.1.4], there exists a finite subset $S_0(K)$ of $\mathbb{P}(K)$ that contains $\mathbb{P}_{\mathrm{arch}}(K)$ such that

$$I_K = I_{K,S}K^\times \text{ and } C_K = I_{K,S}/K_S, \tag{1}$$

for each finite subset S of $\mathbb{P}(K)$ that contains $S_0(K)$. If K is a number field and l is a prime number, we enlarge $S_0(K)$ by adding the prime divisors of l and denote the extended set by $S_{0,l}(K)$. If K is a function field, we set $S_{0,l}(K) = S_0(K)$. In each case, we call $S_{0,l}(K)$ a **basic set** of K.

LEMMA 1.7: *Let K be a global field, $l \neq \mathrm{char}(K)$ a prime number, and $S_{0,l}(K)$ a basic set of K.* PREj input, 330

(a) *Assume that an element a of $K^\times$ is an l-power in $\hat{K}_{\mathfrak{P}}$ for every $\mathfrak{P} \in \mathbb{P}(K)$. Then, a is an l-power in K.*

(b) *Let S be a finite set of prime divisors of K that contains $S_{0,l}(K)$. We use a bar to denote the reduction of elements and subgroups of $I_{K,S}$ modulo $I_{K,S}^l$. Then, $\overline{I_{K,S}}/\overline{K_S}$ is a quotient of C_K.*

Proof of (a): Statement (a) is a special case of [ArT52, p. 96, Thm. 1]. See also [NSW15, p. 530, Thm. 9.1.11(ii)]. We offer here an alternative direct proof that uses the Chebotarev density theorem.

Assume toward contradiction that a is not an l-power in K. Then, $X^l - a$ is irreducible in K [Lan93, p. 297, Thm. 1]. We denote the splitting field of $X^l - a$ over K by N and choose a root x of $X^l - a$.

Observe that $H = \mathrm{Gal}(N/K(x))$ is a proper subgroup of $G = \mathrm{Gal}(N/K)$. Hence, $G \smallsetminus \bigcup_{\sigma \in G} H^\sigma$ is a proper subset of G [FrJ08, p. 238, Lemma 13.3.2]. We choose $\tau \in G \smallsetminus \bigcup_{\sigma \in G} H^\sigma$. Then, we use the Chebotarev density theorem to choose a non-archimedean prime divisor $\mathfrak{P}$ of K which is unramified in N such that $\left[\frac{N/K}{\mathfrak{P}}\right]$ is conjugate in G to τ. Hence, $X^l - a$ has no root in $\hat{K}_{\mathfrak{P}}$. This contradicts our assumption.

Proof of (b): By (a), $K_S \cap I_{K,S}^l = K_S^l$. Hence, $\overline{K_S} = K_S/K_S^l \cong K_S I_{K,S}^l / I_{K,S}^l$. Therefore,

$$\overline{I_{K,S}}/\overline{K_S} \cong (I_{K,S}/I_{K,S}^l)/(K_S I_{K,S}^l/I_{K,S}^l) \cong I_{K,S}/K_S I_{K,S}^l$$

is, by (1), a quotient of $C_K = I_{K,S}/K_S$. ∎

2. Homomorphism from C_K to C_l

HOM input, 11

Let K/K_0 be a finite Galois extension of global fields. For a finite subset S of $\mathbb{P}(K)$ that contains $\mathbb{P}_{\mathrm{arch}}(K)$ we say that elements $a_1,\ldots,a_s \in K_S$ are **multiplicatively independent** modulo K_S^l if for all $k_1,\ldots,k_s \in \mathbb{Z}$ and $b \in K_S$ the equality $a_1^{k_1}\cdots a_s^{k_s} = b^l$ implies that $l|k_i$ for $i = 1,\ldots,s$. Here and in the rest of this section, l denotes a prime number with $l \neq \mathrm{char}(K)$.

The first step toward the proof of our main result is a construction of a homomorphism $h\colon C_K \to C_l$ that satisfies several local conditions. This construction generalizes an earlier construction given in [GeJ98, p. 33, Lemma 7.1].

Lemma 2.1 ([GeJ98, p. 27, Lemma 5.2]): *Let S be a finite subset of $\mathbb{P}(K)$ that contains $\mathbb{P}_{\mathrm{arch}}(K)$, let m be a positive integer, and let L be a finite l-**extension** of K (i.e. $[L:K]$ is a power of l). Suppose that $\zeta_l \notin K$. If $a_1,\ldots,a_s \in K_S$ are multiplicatively independent modulo K_S^l, then the fields $L(\zeta_{l^m},\sqrt[l]{a_1}),\ldots,L(\zeta_{l^m},\sqrt[l]{a_s})$ are linearly disjoint and of degree l over $L(\zeta_{l^m})$.* HOMa input, 31

Lemma 2.2: *Let S be a finite set of primes of K that contains $\mathbb{P}_{\mathrm{arch}}(K)$. Let $a_1,\ldots,a_s \in K_S$ be multiplicatively independent elements modulo K_S^l. Let L be a finite l-extension of K, let m be a positive integer, and let M be a finite abelian extension of K. Suppose that $\zeta_l \notin K$. Then, the fields $LM(\zeta_{l^m},\sqrt[l]{a_1}),\ldots,LM(\zeta_{l^m},\sqrt[l]{a_s})$ are linearly disjoint extensions of $LM(\zeta_{l^m})$ of degree l.* HOMb input, 44

Proof: We write $M = M'M''$, where M' is an abelian l-extension of K and M'' is an abelian extension of K whose degree is not divisible by l. Then, $L' = LM'$ is a finite l-extension of K. Applying Lemma 2.1 to L', we find that $L'(\zeta_{l^m},\sqrt[l]{a_1}),\ldots,L'(\zeta_{l^m},\sqrt[l]{a_s})$ are linearly disjoint extensions of $L'(\zeta_{l^m})$ of degree l. In particular, $N = L'(\zeta_{l^m},\sqrt[l]{a_1},\ldots,\sqrt[l]{a_s})$ is an l-extension of K. Since $l \nmid [M'':K]$, the field M'' is linearly disjoint from N over K. Hence, $LM(\zeta_{l^m},\sqrt[l]{a_1}),\ldots,LM(\zeta_{l^m},\sqrt[l]{a_s})$ are linearly disjoint extensions of $LM(\zeta_{l^m})$ of degree l, as claimed. ∎

Here is the promised generalization of [GeJ98, Lemma 7.1].

Lemma 2.3: *Let $K_0 \subseteq K \subseteq L$ be a tower of finite Galois extensions of global fields* HOMc input, 84 *such that L/K is an abelian l-extension and L/K_0 is Galois. Suppose $\zeta_l \notin K$. Let S be a finite set of primes of K that contains the basic set $S_{0,l}(K)$ chosen in Subsection 1.6. Let q and m be positive integers with $\mathrm{char}(K_0) \nmid q$ and set $n = ql^m$. For each $\mathfrak{P} \in S$ let $h_{\mathfrak{P}}\colon \hat{K}_{\mathfrak{P}}^{\times} \to C_l$ be a homomorphism. Then, there exists a non-archimedean prime $\mathfrak{q} \in \mathbb{P}(K_0) \smallsetminus S|_{K_0}$ and there exists a homomorphism $h\colon C_K \to C_l$ such that the following holds:*

(a) *$\mathfrak{q}$ totally splits in $L(\zeta_n)$,*

(b) *$h|_{\hat{K}_{\mathfrak{P}}^{\times}} = h_{\mathfrak{P}}$ for each $\mathfrak{P} \in S$,*

(c) *there exists $\mathfrak{Q} \in \mathbb{P}(K)$ over $\mathfrak{q}$ with $h(U_{\mathfrak{Q}}) = C_l$, and*

(d) *$h(U_{\mathfrak{P}}) = \mathbf{1}$ for each $\mathfrak{P} \in \mathbb{P}(K) \smallsetminus (S \cup \{\mathfrak{Q}\})$.*

Proof: We break up the proof into several parts.

PART A: *Continuity.* We claim that every abstract homomorphism $h\colon C_K \to C_l$ that satisfies (b) and (d) is continuous, hence h is a homomorphism in the sense of Section 1.2.

Indeed, let $S' = S \cup \{\mathfrak{Q}\}$. Then, by Subsection 1.6, $I_{K,S'} = \prod_{\mathfrak{P} \in S'} \hat{K}_{\mathfrak{P}}^{\times} \times \prod_{\mathfrak{P} \notin S'} U_{\mathfrak{P}}$ and $C_K = I_{K,S'}/K_{S'}$. Let $\pi\colon I_{K,S'} \to C_K$ be the quotient map and $h' = h \circ \pi$. Thus, it suffices to prove that the abstract homomorphism $h'\colon I_{K,S'} \to C_l$ is continuous.

By (d), $h'(U_{\mathfrak{P}}) = h(U_{\mathfrak{P}}) = \mathbf{1}$ for each $\mathfrak{P} \in \mathbb{P}(K) \smallsetminus (S \cup \{\mathfrak{Q}\})$. By (b), $h'|_{\hat{K}_{\mathfrak{P}}^{\times}} = h|_{\hat{K}_{\mathfrak{P}}^{\times}}$ is continuous for each $\mathfrak{P} \in S$. Hence, it suffices to prove that $h|_{\hat{K}_{\mathfrak{Q}}^{\times}} = h'|_{\hat{K}_{\mathfrak{Q}}^{\times}}$ is continuous.

Indeed, by Subsection 1.3, $\hat{K}_{\mathfrak{Q}}^{\times} \cong \langle \pi_{\mathfrak{Q}} \rangle \times U_{\mathfrak{Q}}$. Since $\langle \pi_{\mathfrak{Q}} \rangle$ is discrete, $h|_{\langle \pi_{\mathfrak{Q}} \rangle}$ is continuous. Next recall that $U_{\mathfrak{Q}}$ is a profinite group (Subsection 1.3). Since each prime of K that divides l is in $S_{0,l} \subseteq S$ (Subsection 1.6), $\mathrm{char}(\bar{K}_{\mathfrak{Q}}) \neq l$. It follows from Hensel's lemma that $1 + \pi_{\mathfrak{Q}}^l O_{\mathfrak{Q}} \le U_{\mathfrak{Q}}^l$. Hence, by Subsection 1.3, $U_{\mathfrak{Q}}^l$ is open in $U_{\mathfrak{Q}}$. Since $U_{\mathfrak{Q}}^l \le \mathrm{Ker}(h|_{U_{\mathfrak{Q}}})$, the group $\mathrm{Ker}(h|_{U_{\mathfrak{Q}}})$ is open in $U_{\mathfrak{Q}}$. Hence, $h|_{U_{\mathfrak{Q}}}$ is continuous. Therefore, $h|_{\hat{K}_{\mathfrak{Q}}^{\times}}$ is continuous, as desired.

PART B: *Reduction of the lemma to constructing a homomorphism g: $\overline{I_{K,S}}/\overline{K_S} \to C_l$.* By the Dirichlet unit theorem, K_S is finitely generated [CaF67, p. 72], hence $(K_S : K_S^l) = l^s$ for some positive integer s. We choose multiplicatively independent generators $a_1, \dots, a_s$ of K_S modulo K_S^l. For each $\mathfrak{Q} \in \mathbb{P}(K) \smallsetminus S$ we can decompose $I_{K,S}$ as

$$I_{K,S} = \prod_{\mathfrak{P} \in S} \hat{K}_{\mathfrak{P}}^{\times} \times U_{\mathfrak{Q}} \times \prod_{\mathfrak{P} \notin S \cup \{\mathfrak{Q}\}} U_{\mathfrak{P}}.$$

Then, we use a bar to denote the reduction of elements and subgroups of $I_{K,S}$ modulo $I_{K,S}^l$. In particular

$$\overline{I_{K,S}} = \prod_{\mathfrak{P} \in S} \overline{\hat{K}_{\mathfrak{P}}^{\times}} \times \overline{U_{\mathfrak{Q}}} \times \prod_{\mathfrak{P} \notin S \cup \{\mathfrak{Q}\}} \overline{U_{\mathfrak{P}}}, \tag{1}$$

and

$$\overline{K_S} = \langle \bar{a}_1, \dots, \bar{a}_s \rangle. \tag{2}$$

Also, for each $\mathfrak{P} \in S$ the homomorphism $h_{\mathfrak{P}}$: $\hat{K}_{\mathfrak{P}}^{\times} \to C_l$ induces a homomorphism $\bar{h}_{\mathfrak{P}}$: $\overline{\hat{K}_{\mathfrak{P}}^{\times}} \to C_l$. Since $\overline{I_{K,S}}/\overline{K_S}$ is a quotient of $C_K = I_{K,S}/K_S$ (Lemma 1.7), it suffices to find a prime $\mathfrak{q} \in \mathbb{P}(K_0) \smallsetminus S|_{K_0}$ that satisfies (a) and to construct a homomorphism g: $\overline{I_{K,S}} \to C_l$ such that

(3a) $g|_{\overline{\hat{K}_{\mathfrak{P}}^{\times}}} = \bar{h}_{\mathfrak{P}}$ for each $\mathfrak{P} \in S$,

(3b) there exists $\mathfrak{Q} \in \mathbb{P}(K)$ over $\mathfrak{q}$ with $g(\overline{U_{\mathfrak{Q}}}) = C_l$,

(3c) $g(\overline{U_{\mathfrak{P}}}) = \mathbf{1}$ for each $\mathfrak{P} \in \mathbb{P}(K) \smallsetminus (S \cup \{\mathfrak{Q}\})$, and

(3d) $g(\bar{a}_i) = 1$ for $i = 1, \dots, s$.

By (2) and (3d), g will induce a homomorphism $\bar{g}$: $\overline{I_{K,S}}/\overline{K_S} \to C_l$ that will compose with the quotient map $C_K \to \overline{I_{K,S}}/\overline{K_S}$ to the desired homomorphism h. By Part A, we don't have to care about the continuity of g.

Part C: *Presentation of $\bar{a}_i$ as an idele.* For each i between 1 and s and every $\mathfrak{P} \in \mathbb{P}(K)$, let $a_{i\mathfrak{P}}$ be a_i considered as an element of $\hat{K}_{\mathfrak{P}}^{\times}$ and let

$$\delta_i = \prod_{\mathfrak{P} \in S} \bar{h}_{\mathfrak{P}}(\bar{a}_{i\mathfrak{P}}). \tag{4}$$

If $\mathfrak{q} \in \mathbb{P}(K_0) \smallsetminus S|_{K_0}$ satisfies (a) and $\mathrm{char}(\bar{K}_{0,\mathfrak{q}}) \neq l$, we choose $\mathfrak{Q} \in \mathbb{P}(K)$ over $\mathfrak{q}$. Then, $\mathfrak{Q}$ totally splits in $L(\zeta_l)$. Hence, $a_1, \dots, a_s, \zeta_l \in U_{\mathfrak{Q}}$ and $\overline{U_{\mathfrak{Q}}} \cong C_l$ [GeJ98, p. 24, Lemma

4.1]. This allows us to choose a generator $\bar{u}_{\mathfrak{Q}}$ for $\overline{U_{\mathfrak{Q}}}$. Thus, for each i there exists an integer $0 \le \beta_i < l$ such that

$$\bar{a}_{i\mathfrak{Q}} = \bar{u}_{\mathfrak{Q}}^{\beta_i}. \tag{5}$$

The representation of $\bar{a}_i$ therefore takes the form

$$\bar{a}_i = \prod_{\mathfrak{P}\in S} \bar{a}_{i\mathfrak{P}} \cdot \bar{u}_{\mathfrak{Q}}^{\beta_i} \cdot \prod_{\mathfrak{P}\notin S\cup\{\mathfrak{Q}\}} \bar{a}_{i\mathfrak{P}}. \tag{6}$$

By their choice in Part B, the a_i's belong to $U_{\mathfrak{P}}$ for each $\mathfrak{P} \in \mathbb{P}(K) \smallsetminus S$. Hence, Conditions (3a) and (3c) force that

$$g(\bar{a}_{i\mathfrak{P}}) = \bar{h}_{\mathfrak{P}}(\bar{a}_{i\mathfrak{P}}) \text{ for } \mathfrak{P} \in S \text{ and } g(\bar{a}_{i\mathfrak{P}}) = 1 \text{ for } \mathfrak{P} \in \mathbb{P}(K) \smallsetminus (S \cup \{\mathfrak{Q}\}). \tag{7}$$

Condition (3b) is equivalent to $g(\bar{u}_{\mathfrak{Q}}) \neq 1$. Therefore we have to choose $\mathfrak{q}$ such that in addition to (8), (a) will hold, and to define $g(\bar{u}_{\mathfrak{Q}})$ as a non-unit element of C_l such that (3d) will be satisfied.

Let N be the Galois closure of $L(\zeta_n, \sqrt[l]{a_1}, \ldots, \sqrt[l]{a_s})$ over K_0. If $\delta_i = 1$ for $i = 1, \ldots, s$, we use the Chebotarev density theorem to choose $\mathfrak{q} \in \mathbb{P}(K_0) \smallsetminus S|_{K_0}$ such that

$$N \subseteq \hat{K}_{0,\mathfrak{q}}. \tag{8}$$

In particular, (a) holds. Then, we choose $\mathfrak{Q} \in \mathbb{P}(K)$ over $\mathfrak{q}$. By its choice, $\mathfrak{q}$ totally splits in K, so $\hat{K}_{\mathfrak{Q}} = \hat{K}_{0,\mathfrak{q}}$. It follows that $a_{i\mathfrak{Q}} \in U_{\mathfrak{Q}}^l$, so $\beta_i = 0$ for $i = 1, \ldots, s$. We therefore define $g(\bar{u}_{\mathfrak{Q}})$ to be a non-unit element of C_l and derive from (6), (4), and (7) that $g(\bar{a}_i) = \delta_i \cdot g(\bar{u}_{\mathfrak{Q}})^{\beta_i} = 1$ so that (3d) holds.

Part D: *The main case.* Having settled the case where $\delta_i = 1$ for $i = 1, \ldots, s$, we may and we will from now on assume that

$$\delta_1 \neq 1. \tag{9}$$

Under this assumption there exists an integer $0 \le \varepsilon_i < l$ such that

$$\delta_1^{\varepsilon_i} = \delta_i, \qquad i = 1, \ldots, s. \tag{10}$$

In particular, $\varepsilon_1 = 1$. Then, we set

$$b_1 = a_1 \text{ and } b_i = a_i/a_1^{\varepsilon_i} \text{ for } i = 2, \dots, s. \tag{11}$$

Then, N is also the Galois closure of $L(\zeta_n, \sqrt[l]{b_1}, \dots, \sqrt[l]{b_s})$ over K_0. Since $a_1, \dots, a_s$ are multiplicatively independent modulo K_S^l, so are $b_1, \dots, b_s$. By Lemma 2.2 applied to $M = K(\zeta_n)$ and to $b_1, \dots, b_s$ rather than to $a_1, \dots, a_s$ (so that $LM(\zeta_{l^m}, \sqrt[l]{b_i}) = L(\zeta_n, \sqrt[l]{b_i})$), the fields $L(\zeta_n, \sqrt[l]{b_1}), \dots, L(\zeta_n, \sqrt[l]{b_s})$ are linearly disjoint of degree l over $L(\zeta_n)$.

Part E: *Choosing* $\mathfrak{q}$. Part D allows us to choose $\sigma \in \mathrm{Gal}(N/L(\zeta_n))$ such that $(\sqrt[l]{a_1})^\sigma = \zeta_l \sqrt[l]{a_1}$ and $(\sqrt[l]{b_i})^\sigma = \sqrt[l]{b_i}$ for $i = 2, \dots, s$. The Chebotarev density theorem gives a prime $\mathfrak{q} \in \mathbb{P}(K_0) \smallsetminus S|_{K_0}$ such that $\left(\frac{N/K_0}{\mathfrak{q}}\right)$ is the conjugacy class of σ in $\mathrm{Gal}(N/K_0)$. In particular, $L(\zeta_n) \subseteq \hat{K}_{0,\mathfrak{q}}$, so (a) holds.

We choose $\mathfrak{Q} \in \mathbb{P}(K)$ over $\mathfrak{q}$. Since $\mathfrak{q}$ is unramified in N, so is $\mathfrak{Q}$. Hence, $\hat{K}_{\mathfrak{Q}}(\sqrt[l]{a_1})/\hat{K}_{\mathfrak{Q}}$ is an unramified extension. It follows that the Frobenius element of the latter extension acts on $\sqrt[l]{a_1}$ as σ. In particular, that Frobenius does not fix $\sqrt[l]{a_1}$. This implies that $[\hat{K}_{\mathfrak{Q}}(\sqrt[l]{a_1}) : \hat{K}_{\mathfrak{Q}}] = l$, so

$$a_1 \in U_{\mathfrak{Q}} \smallsetminus U_{\mathfrak{Q}}^l. \tag{12}$$

On the other hand, $b_i \in U_{\mathfrak{Q}}^l$, so by (11)

$$\bar{a}_{i\mathfrak{Q}} = \bar{a}_{1\mathfrak{Q}}^{\varepsilon_i}, \qquad i = 2, \dots, s. \tag{13}$$

Part F: *Definition of* g. By (5) and (12),

$$\bar{a}_{1\mathfrak{Q}} = \bar{u}_{\mathfrak{Q}}^\beta \text{ for some } 0 < \beta < l. \tag{14}$$

This allows us to define $g(\bar{u}_{\mathfrak{Q}})$ as the element of C_l that satisfies

$$g(\bar{u}_{\mathfrak{Q}})^\beta = \delta_1^{-1}. \tag{15}$$

In particular, by (9), $g(\bar{u}_{\mathfrak{Q}}) \neq 1$. By (13) and (14), $\bar{a}_{i\mathfrak{Q}} = \bar{a}_{1\mathfrak{Q}}^{\varepsilon_i} = \bar{u}_{\mathfrak{Q}}^{\beta\varepsilon_i}$, $i = 2, \dots, s$. This gives (6) the form

$$\bar{a}_i = \prod_{\mathfrak{P} \in S} \bar{a}_{i\mathfrak{P}} \cdot \bar{u}_{\mathfrak{Q}}^{\beta\varepsilon_i} \cdot \prod_{\mathfrak{P} \notin S \cup \{\mathfrak{Q}\}} \bar{a}_{i\mathfrak{P}}. \tag{16}$$

By (4) and (8),

$$\prod_{\mathfrak{P}\in S} g(\bar{a}_{i\mathfrak{P}}) = \delta_i \text{ and } \prod_{\mathfrak{P}\notin S\cup\{\mathfrak{Q}\}} g(\bar{a}_{i\mathfrak{P}}) = 1. \tag{17}$$

Finally, we apply g on (16) and use (17), (15), and (10) to get

$$g(\bar{a}_i) = \Big(\prod_{\mathfrak{P}\in S} g(\bar{a}_{i\mathfrak{P}})\Big) \cdot g(\bar{u}_{\mathfrak{Q}})^{\beta\varepsilon_i} \cdot \prod_{\mathfrak{P}\notin S\cup\{\mathfrak{Q}\}} g(\bar{a}_{i\mathfrak{P}}) = \delta_i\delta_1^{-\varepsilon_i} = 1.$$

Thus, (3d) holds and the proof is complete. ▮

3. Homomorphism from $\mathrm{Gal}(K)$ to C_l

GAL input, 11

We use class field theory to translate Lemma 2.3 into a result about the existence of a homomorphism from $\mathrm{Gal}(K)$ into C_l with local data and with a bound on the ramification. Again, we assume for the whole section that $l \neq \mathrm{char}(K_0)$.

We start with a presentation of the main result of class field theory.

Proposition 3.1: *Let K be a finite Galois extension of K_0, $\mathfrak{P}$ a prime of K, and L a finite abelian extension of K. Then, there exists a commutative diagram*

GALa input, 21

$$\begin{tikzcd}
1 \arrow[r] & N_{L/K}L^\times \arrow[r] & C_K \arrow[r, "{(\ ,L/K)}"] & \mathrm{Gal}(L/K) \arrow[r] & 1 \\
1 \arrow[r] & N_{\hat{L}_\mathfrak{P}/\hat{K}_\mathfrak{P}}\hat{L}_\mathfrak{P}^\times \arrow[r] \arrow[u] & \hat{K}_\mathfrak{P}^\times \arrow[r, "{(\ ,\hat{L}_\mathfrak{P}/\hat{K}_\mathfrak{P})}"] \arrow[u] & \mathrm{Gal}(\hat{L}_\mathfrak{P}/\hat{K}_\mathfrak{P}) \arrow[r] \arrow[u, "\lambda_\mathfrak{P}"'] & 1,
\end{tikzcd}$$

with exact rows. In this diagram

(a) *$\hat{K}_\mathfrak{P}$ is the completion of K at $\mathfrak{P}$, $\lambda_\mathfrak{P}$ is the embedding of K_{sep} into $\hat{K}_{\mathfrak{P},\mathrm{sep}}$ chosen in Subsection 1.4, and $\hat{L}_\mathfrak{P} = \lambda_\mathfrak{P}(L)\hat{K}_\mathfrak{P}$.*

(b) *$N_{L/K}$ and $N_{\hat{L}_\mathfrak{P}/\hat{K}_\mathfrak{P}}$ are the norm maps.*

(c) *$(\ ,L/K)$ and $(\ ,\hat{L}_\mathfrak{P}/\hat{K}_\mathfrak{P})$ are the global and local norm residue symbols. They are obtained from the inverses of the Artin reciprocity maps $r_{L/K}\colon \mathrm{Gal}(L/K) \to C_K/N_{L/K}L^\times$ and*

$$r_{\hat{L}_\mathfrak{P}/\hat{K}_\mathfrak{P}}\colon \mathrm{Gal}(\hat{L}_\mathfrak{P}/\hat{K}_\mathfrak{P}) \to \hat{K}_\mathfrak{P}^\times/N_{\hat{L}_\mathfrak{P}/\hat{K}_\mathfrak{P}}\hat{L}_\mathfrak{P}^\times,$$

respectively.

(d) *If $\mathfrak{P}$ is non-archimedean, then the map $(\ ,\hat{L}_{\mathfrak{P}}/\hat{K}_{\mathfrak{P}})$ maps the group of units $U_{\mathfrak{P}}$ of $\hat{K}_{\mathfrak{P}}$ onto the inertia group $I(\hat{L}_{\mathfrak{P}}/\hat{K}_{\mathfrak{P}})$ of $\hat{L}_{\mathfrak{P}}/\hat{K}_{\mathfrak{P}}$.*

In addition,

(e) *both the global and the local residue symbols are compatible with the restriction maps and*

(f) *the map $L \mapsto N_{L/K}C_L$ maps the set of finite abelian extensions L of K (in K_{sep}) onto the set of closed subgroups of C_K of finite index.*

References: The upper exact sequence is guaranteed by [Neu99, p. 391, Thm. 5.5] in the number field case, and by [CaF67, p. 172, Thm. 5.1(B)] in the general case. In both cases, the lower exact sequence is established by [Neu99, p. 320, Thm. 1.3]. Part (d) of the theorem is established in [CaF67, p. 142, Cor.] and in [Neu99, p. 354, Thm. 6.2]. The commutativity of the diagram is proved in [Neu99, p. 391, Prop. 5.6] in the number field case, and in [CaF67, pp. 174-176, Sec. VII.6] in the general case.

Statement (e) is established for global fields in [CaF67, p. 171, Prop. 4.3], and in [Neu99, p. 302, Prop. 6.4] in the number field case.

Finally, the "existence theorem" (f) is proved in [Neu99, p. 395, Thm. 6.1] for number fields, and [ArT52, p. 71, Thm. 3] in the general case. ∎

LEMMA 3.2: *Let A be a finite abelian group and let $\mathfrak{P}$ be a prime of K. Then, there is a commutative diagram* HOMd input, 105

(1)
$$\begin{tikzcd}
\mathrm{Hom}(\mathrm{Gal}(K),A) \arrow[r, "\psi"] \arrow[d, "\mathrm{res}_{\mathfrak{P}}"'] & \mathrm{Hom}(C_K,A) \arrow[d] \\
\mathrm{Hom}(\mathrm{Gal}(\hat{K}_{\mathfrak{P}}),A) \arrow[r, "\psi_{\mathfrak{P}}"] & \mathrm{Hom}(\hat{K}_{\mathfrak{P}}^{\times},A),
\end{tikzcd}$$

where $\mathrm{res}_{\mathfrak{P}}$ *is the map introduced in Subsection 1.4 (thus,* $\mathrm{res}_{\mathfrak{P}}(h)(\sigma) = h(\sigma^{\lambda_{\mathfrak{P}}^{-1}})$ *for each*

$$h \in \mathrm{Hom}(\mathrm{Gal}(K),A)$$

and $\sigma \in \mathrm{Gal}(\hat{K}_{\mathfrak{P}})$*), the right vertical map is the natural restriction map, and the horizontal maps are the isomorphisms induced by the global and local norm symbols* *cited in Proposition 3.1. Moreover, if $\mathfrak{P}$ is non-archimedean and $f \in \mathrm{Hom}(\mathrm{Gal}(\hat{K}_{\mathfrak{P}}), A)$, then $\psi_{\mathfrak{P}}(f)(U_{\mathfrak{P}}) = f(\hat{I}_{\mathfrak{P}})$.*

Proof: Our lemma is a consequence of Proposition 3.1. Since A is finite, Diagram (1) is the inverse limit of diagrams where $\mathrm{Gal}(K)$ is replaced by $\mathrm{Gal}(L/K)$ for finite abelian extensions L/K, and $\mathrm{Gal}(\hat{K}_{\mathfrak{P}})$ is replaced by the corresponding decomposition group in $\mathrm{Gal}(L/K)$. The maps ψ and $\psi_{\mathfrak{P}}$ are replaced in those diagrams by the corresponding global (resp. local) norm residue symbols. The latter are compatible with each other. Since both the global and the local reciprocity law are compatible under finite Galois extensions (Proposition 3.1(e)), an inverse limit argument gives the desired diagram (1). The injectivity of ψ follows from the surjectivity of the map $(\ ,L/K)\colon C_K \to \mathrm{Gal}(L/K)$. The surjectivity of ψ and $\psi_{\mathfrak{P}}$ are consequences of the existence theorem 3.1(f). ▮

COROLLARY 3.3: *Let $K_0 \subseteq K \subseteq L$ be a tower of finite Galois extensions of global fields such that L/K is an abelian l-extension and L/K_0 is Galois. Suppose $\zeta_l \notin K$. Let S be a finite set of primes of K that contains the basic set $S_{0,l}(K)$ chosen in Subsection 1.6. Let q and m be positive integers with $\mathrm{char}(K_0) \nmid q$ and set $n = ql^m$. For each $\mathfrak{P} \in S$ let $h_{\mathfrak{P}}\colon \mathrm{Gal}(\hat{K}_{\mathfrak{P}}) \to C_l$ be a homomorphism. Then, there exists a prime $\mathfrak{q} \in \mathbb{P}(K_0) \smallsetminus S|_{K_0}$ and there exists a homomorphism $h\colon \mathrm{Gal}(K) \to C_l$ such that the following holds:* HOMe input, 156

(a) *$\mathfrak{q}$ totally splits in $L(\zeta_n)$,*

(b) *$\mathrm{res}_{\mathfrak{P}}(h) = h_{\mathfrak{P}}$ for each $\mathfrak{P} \in S$,*

(c) *there exists $\mathfrak{Q} \in \mathbb{P}(K)$ over $\mathfrak{q}$ with $\mathrm{res}_{\mathfrak{Q}}(h)(\hat{I}_{\mathfrak{Q}}) = C_l$, and*

(d) *$\mathrm{res}_{\mathfrak{P}}(h)(\hat{I}_{\mathfrak{P}}) = \mathbf{1}$ for each $\mathfrak{P} \in \mathbb{P}(K) \smallsetminus (S \cup \{\mathfrak{Q}\})$.*

Proof: For each $\mathfrak{P} \in S$, let $h'_{\mathfrak{P}}\colon \hat{K}_{\mathfrak{P}}^{\times} \to C_l$ be the image of $h_{\mathfrak{P}}$ under the map $\psi_{\mathfrak{P}}$ of Diagram (1), applied to C_l rather than to A. By Lemma 2.3, there exist a prime $\mathfrak{q}$ of K_0 and a homomorphism $h'\colon C_K \to C_l$ that satisfy Conditions (a)–(d) of that lemma (with h' and $h'_{\mathfrak{P}}$ replacing h and $h_{\mathfrak{P}}$). Let $h\colon \mathrm{Gal}(K) \to C_l$ be the unique homomorphism given by Lemma 3.2 such that $\psi(h) = h'$. Then, by Proposition 3.1, $\mathfrak{q}$ and h satisfy Conditions (a)–(d) of our corollary. ▮

4. Homomorphism from $\mathrm{Gal}(K)$ to C_l^r

CLR input, 12

For each positive integer r, a repeated application of Corollary 3.3 yields a homomorphism h from $\mathrm{Gal}(K)$ into C_l^r with local data and with a bound on the ramification.

Remark 4.1: The construction of h: $\mathrm{Gal}(K) \to C_l^r$ uses the following basic argument: CLRa input, 18

Let $K_0 \subseteq K$ be a finite Galois extension and let $L_1, \ldots, L_r$ be finite abelian l-extensions of K. Let M be the Galois closure of $L_1 \cdots L_r/K_0$. Then, $M = \prod_{i=1}^r \prod_{\sigma_i} L_i^{\sigma_i}$, where σ_i ranges over the finitely many K_0-embeddings of L_i into K_{sep}. Hence, the corresponding restriction map $\mathrm{Gal}(M/K) \to \prod_{i=1}^r \prod_{\sigma_i} \mathrm{Gal}(L_i^{\sigma_i}/K)$ is an embedding. Since the right-hand side is an abelian l-extension, so is $\mathrm{Gal}(M/K)$. ∎

PROPOSITION 4.2: *Let $K_0 \subseteq K \subseteq L$ be a tower of finite Galois extensions of global fields such that L/K_0 is a Galois extension, $l \neq \mathrm{char}(K_0)$ is a prime number with $\zeta_l \notin K$, L/K is an abelian l-extension, r is a positive integer, and $A = C_{l,1} \times \cdots \times C_{l,r}$, where each $C_{l,i}$ is an isomorphic copy of C_l. Let $n = ql^m$ for some positive integers q and m with $\mathrm{char}(K_0) \nmid q$. Let S be a finite set of primes of K which contains $S_{0.l}(K)$. For each $\mathfrak{P} \in S$ let $h_{\mathfrak{P}}$: $\mathrm{Gal}(\hat{K}_{\mathfrak{P}}) \to A$ be a homomorphism.* CLRb input, 36

Then, there exist distinct primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_r \in \mathbb{P}(K_0) \smallsetminus S|_{K_0}$ and there exists a homomorphism h: $\mathrm{Gal}(K) \to A$ such that the following holds for each $1 \le i \le r$:

(a) *$\mathfrak{q}_i$ totally splits in $L(\zeta_n)$,*

(b) *$\mathrm{res}_{\mathfrak{Q}}(h)(\mathrm{Gal}(\hat{K}_{\mathfrak{Q}})) \le \mathbf{1} \times \cdots \times \mathbf{1} \times C_{l,i} \times \mathbf{1} \times \cdots \times \mathbf{1}$ for each $\mathfrak{Q} \in \mathbb{P}(K)$ over $\mathfrak{q}_i$, and*

(c) *there exists $\mathfrak{Q}_i \in \mathbb{P}(K)$ over $\mathfrak{q}_i$ such that $\mathrm{res}_{\mathfrak{Q}_i}(h)(\hat{I}_{\mathfrak{Q}_i}) = \mathbf{1} \times \cdots \times \mathbf{1} \times C_{l,i} \times \mathbf{1} \times \cdots \times \mathbf{1}$.*

(d) *Moreover, $\mathrm{res}_{\mathfrak{P}}(h) = h_{\mathfrak{P}}$ for each $\mathfrak{P} \in S$, and*

(e) *$\mathrm{res}_{\mathfrak{P}}(h)(\hat{I}_{\mathfrak{P}}) = \mathbf{1}_A$ for each $\mathfrak{P} \in \mathbb{P}(K) \smallsetminus (S \cup \{\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r\})$.*

Proof: For each $1 \le i \le r$ let π_i: $A \to C_{l,i}$ be the projection on the ith factor of A. For each $\mathfrak{P} \in S$ we set $h_{\mathfrak{P},i} = \pi_i \circ h_{\mathfrak{P}}$: $\mathrm{Gal}(\hat{K}_{\mathfrak{P}}) \to C_{l,i}$. Then,

$$(1) \qquad h_{\mathfrak{P}} = (h_{\mathfrak{P},1}, \ldots, h_{\mathfrak{P},r}).$$

We construct primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_r \in \mathbb{P}(K_0)$, homomorphisms h_i: $\mathrm{Gal}(K) \to C_{l,i}$ for $i = 1, \ldots, r$, and primes $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r \in \mathbb{P}(K)$ such that with L_i being the fixed field of $\mathrm{Ker}(h_i)$

in K_{sep} and M_{i-1} being the Galois closure of $LL_1 \cdots L_{i-1}/K_0$ (in particular, $M_0 = L$) the following conditions hold:

(2a) $\mathfrak{q}_i$ lies in $\mathbb{P}(K_0) \smallsetminus (S|_{K_0} \cup \{\mathfrak{q}_1, \dots, \mathfrak{q}_{i-1}\})$ and totally splits in $M_{i-1}(\zeta_n)$.

(2b) $\mathrm{res}_{\mathfrak{Q}}(h_i) = 1$ for each $\mathfrak{Q} \in \mathbb{P}(K)$ that lies over one of the primes $\mathfrak{q}_1, \dots, \mathfrak{q}_{i-1}$.

(2c) $\mathrm{res}_{\mathfrak{Q}_i}(h_i)(\hat{I}_{\mathfrak{Q}_i}) = C_{l,i}$.

(2d) $\mathrm{res}_{\mathfrak{Q}}(h_e)(\mathrm{Gal}(\hat{K}_{\mathfrak{Q}})) = \mathbf{1}$ for each $1 \le e \le i-1$ and for each $\mathfrak{Q} \in \mathbb{P}(K)$ that lies over $\mathfrak{q}_i$.

(2e) $\mathrm{res}_{\mathfrak{P}}(h_i) = h_{\mathfrak{P},i}$ for each $\mathfrak{P} \in S$.

(2f) $\mathrm{res}_{\mathfrak{P}}(h_i)(\hat{I}_{\mathfrak{P}}) = \mathbf{1}$ for each $\mathfrak{P} \in \mathbb{P}(K) \smallsetminus (S \cup \{\mathfrak{Q}_i\})$.

The rest of the proof breaks up into two parts.

Part A: *Induction.* Let $1 \le i \le r$ and inductively assume that $\mathfrak{q}_1, \dots, \mathfrak{q}_{i-1}$, $h_1, \dots, h_{i-1}$, and $\mathfrak{Q}_1, \dots, \mathfrak{Q}_{i-1}$ have been constructed such that they satisfy Condition (2). In particular, for each $1 \le e \le i-1$, the prime $\mathfrak{q}_e$ totally splits in K. Let $\mathcal{Q}_e$ be the set of primes of K that lie over $\mathfrak{q}_e$. For each $\mathfrak{Q} \in \mathcal{Q}_e$ let $g_{\mathfrak{Q}}\colon \mathrm{Gal}(\hat{K}_{\mathfrak{Q}}) \to C_{l,i}$ be the trivial homomorphism.

Note that $L/K, L_1/K, \dots, L_{i-1}/K$ are abelian l-extensions. Hence, by Remark 4.1, M_{i-1}/K is also an abelian l-extension. Thus, by Corollary 3.3 applied to $K_0 \subseteq K \subseteq M_{i-1}$, $S \cup \mathcal{Q}_1 \cup \cdots \cup \mathcal{Q}_{i-1}$, and the $h_{\mathfrak{P},i}, g_{\mathfrak{Q}}$'s rather than to $K_0 \subseteq K \subseteq L$, S and the $h_{\mathfrak{P}}$'s, there exists a prime $\mathfrak{q}_i \in \mathbb{P}(K_0) \smallsetminus (S|_{K_0} \cup \{\mathfrak{q}_1, \dots, \mathfrak{q}_{i-1}\})$ and there exists a homomorphism $h_i\colon \mathrm{Gal}(K) \to C_{l,i}$ such that

(3a) $\mathfrak{q}_i$ totally splits in $M_{i-1}(\zeta_n)$,

(3b) $\mathrm{res}_{\mathfrak{P}}(h_i) = h_{\mathfrak{P},i}$ for each $\mathfrak{P} \in S$ and $\mathrm{res}_{\mathfrak{Q}}(h_i) = g_{\mathfrak{Q}} = 1$ for each $\mathfrak{Q} \in \mathbb{P}(K)$ that lies over one of the primes $\mathfrak{q}_1, \dots, \mathfrak{q}_{i-1}$,

(3c) there exists $\mathfrak{Q}_i \in \mathbb{P}(K)$ over $\mathfrak{q}_i$ such that $\mathrm{res}_{\mathfrak{Q}_i}(h_i)(\hat{I}_{\mathfrak{Q}_i}) = C_{l,i}$, and

(3d) $\mathrm{res}_{\mathfrak{P}}(h_i)(\hat{I}_{\mathfrak{P}}) = \mathbf{1}$ for each $\mathfrak{P} \in \mathbb{P}(K) \smallsetminus (S \cup \mathcal{Q}_1 \cup \cdots \cup \mathcal{Q}_{i-1} \cup \{\mathfrak{Q}_i\})$.

In particular, Conditions (2a), (2b), (2c), and (2e) hold.

Next, we prove Condition (2d). Indeed, let $1 \le e \le i-1$. Since $\mathrm{Ker}(h_e) = \mathrm{Gal}(L_e)$ and $L_e \le M_{i-1}$, we have $h_e(\mathrm{Gal}(M_{i-1})) = \mathbf{1}$. Since $\mathfrak{q}_i$ totally splits in M_{i-1}, each

$\mathfrak{Q} \in \mathbb{P}(K)$ over $\mathfrak{q}_i$ totally splits in M_{i-1}. Hence, by Subsection 1.5, $M_{i-1} \subseteq K_{\mathfrak{Q}}$, so $h_e(\mathrm{Gal}(K_{\mathfrak{Q}})) = \mathbf{1}$. Finally, for each $\sigma \in \mathrm{Gal}(\hat{K}_{\mathfrak{Q}})$ we have $\sigma^{\lambda_{\mathfrak{P}}^{-1}} \in \mathrm{Gal}(K_{\mathfrak{Q}})$, so by the notation of Lemma 3.2, $\mathrm{res}_{\mathfrak{Q}}(h_e)(\sigma) = h_e(\sigma^{\lambda_{\mathfrak{P}}^{-1}}) = 1$, as claimed.

Finally, by (3b) and (3d), $\mathrm{res}_{\mathfrak{P}}(h_i)(\hat{I}_{\mathfrak{P}}) = 1$ for each $\mathfrak{P} \in \mathbb{P}(K) \smallsetminus (S \cup \{\mathfrak{Q}_i\})$, so (2f) holds. This concludes the induction.

Part B: *Conclusion of the proof.* We prove that the homomorphism

$$h = (h_1, \ldots, h_r)\colon \mathrm{Gal}(K) \to C_{l,1} \times \cdots \times C_{l,r}, \tag{4}$$

the primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ of K_0, and their corresponding extensions $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r$ to the primes of K chosen in Part A satisfy Conditions (a)–(e) of the proposition.

Indeed, let i be an integer between 1 and r. Then, (a) follows from (2a).

Next, let $\mathfrak{Q}$ be a prime of K over $\mathfrak{q}_i$. By (2d), $\mathrm{res}_{\mathfrak{Q}}(h_e)(\mathrm{Gal}(\hat{K}_{\mathfrak{Q}})) = \mathbf{1}$ for each $1 \le e \le i-1$. If $i+1 \le e' \le r$, then by (2b), with (e', i) replacing (i, e), we have $\mathrm{res}_{\mathfrak{Q}}(h_{e'})(\mathrm{Gal}(\hat{K}_{\mathfrak{Q}})) = \mathbf{1}$. Therefore, by (4), $\mathrm{res}_{\mathfrak{Q}}(h)(\mathrm{Gal}(\hat{K}_{\mathfrak{Q}})) \le \mathbf{1} \times \cdots \times \mathbf{1} \times C_{l,i} \times \mathbf{1} \times \cdots \times \mathbf{1}$, as (b) states. If $\mathfrak{Q} = \mathfrak{Q}_i$, then by (2c), $\mathrm{res}_{\mathfrak{Q}_i}(h_i)(\mathrm{Gal}(\hat{K}_{\mathfrak{Q}_i})) = C_{l,i}$. Therefore, $\mathrm{res}_{\mathfrak{Q}_i}(h)(\mathrm{Gal}(\hat{K}_{\mathfrak{Q}_i})) = \mathbf{1} \times \cdots \times \mathbf{1} \times C_{l,i} \times \mathbf{1} \times \cdots \times \mathbf{1}$, as stated by (c).

By (4), (2e), and (1), $\mathrm{res}_{\mathfrak{P}}(h) = (\mathrm{res}_{\mathfrak{P}}(h_1), \ldots, \mathrm{res}_{\mathfrak{P}}(h_r)) = (h_{\mathfrak{P},1}, \ldots, h_{\mathfrak{P},r}) = h_{\mathfrak{P}}$ for each $\mathfrak{P} \in S$, as (d) states.

Finally, for each $\mathfrak{P} \in \mathbb{P}(K) \smallsetminus (S \cup \{\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r\})$, Condition (2f) implies that $\mathrm{res}_{\mathfrak{P}}(h)(\hat{I}_{\mathfrak{P}}) = (\mathrm{res}_{\mathfrak{P}}(h_1)(\hat{I}_{\mathfrak{P}}), \ldots, \mathrm{res}_{\mathfrak{P}}(h_r)(\hat{I}_{\mathfrak{P}})) = \mathbf{1} \times \cdots \times \mathbf{1}$, as (e) claims. This completes the proof of the proposition. ∎

5. A Commutative Diagram

DGRM
input, 10

Let K/K_0 be a finite Galois extension of global fields, and let A be a finite multiplicative $\mathrm{Gal}(K_0)$-module. Our goal in this section is to prove that for every non-negative integer n, and every $\mathfrak{p} \in \mathbb{P}(K_0)$, the following diagram commutes.

(1)

$$\begin{tikzcd}
H^n(\mathrm{Gal}(K), A) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{cor}"'] & \prod_{\mathfrak{P}|\mathfrak{p}} H^n(\mathrm{Gal}(\hat{K}_{\mathfrak{P}}), A) \arrow[d, "\mathrm{Cor}"] \\
H^n(\mathrm{Gal}(K_0), A) \arrow[r, "\mathrm{res}_{\mathfrak{p}}"] & H^n(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A).
\end{tikzcd}$$

In this diagram

(2a) we identify $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ with the subgroup $\mathrm{Gal}(K_{0,\mathfrak{p}})$ of $\mathrm{Gal}(K_0)$ (as in Subsection 1.3), making A also a $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$-module,

(2b) for each prime $\mathfrak{P}$ of K over $\mathfrak{p}$, we let $\mathrm{Gal}(\hat{K}_{\mathfrak{P}})$ act on A by the rule $a^\tau = a^{\lambda_{\mathfrak{P}}^{-1}(\tau)}$ for $a \in A$ and $\tau \in \mathrm{Gal}(\hat{K}_{\mathfrak{P}})$, and where $\lambda_{\mathfrak{P}}\colon \mathrm{Gal}(K_{\mathfrak{P}}) \to \mathrm{Gal}(\hat{K}_{\mathfrak{P}})$ is the isomorphism introduced in Subsection 1.4; in particular, if $\mathrm{Gal}(K)$ acts trivially on A, then so does $\mathrm{Gal}(K_{\mathfrak{P}})$ and therefore also $\mathrm{Gal}(\hat{K}_{\mathfrak{P}})$,

(2c) the map cor: $H^n(\mathrm{Gal}(K), A) \to H^n(\mathrm{Gal}(K_0), A)$ is the corestriction map for the open subgroup $\mathrm{Gal}(K)$ of $\mathrm{Gal}(K_0)$,

(2d) the map $\mathrm{res}_{\mathfrak{p}}\colon H^n(\mathrm{Gal}(K_0), A) \to H^n(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ is the restriction map for the closed subgroup $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ of $\mathrm{Gal}(K_0)$,

(2e) the map Res is an abbreviation for the system of maps $(\mathrm{res}_{\mathfrak{P}})_{\mathfrak{P}|\mathfrak{p}}$, where for each $\mathfrak{P}|\mathfrak{p}$ the map $\mathrm{res}_{\mathfrak{P}}\colon H^n(\mathrm{Gal}(K), A) \to H^n(\mathrm{Gal}(\hat{K}_{\mathfrak{P}}), A)$ is defined for each homogeneous cochain $h\colon \mathrm{Gal}(K)^{n+1} \to A$ by $\mathrm{res}_{\mathfrak{P}}(h) = h_{\mathfrak{P}}$, where $h_{\mathfrak{P}}(\sigma_0, \dots, \sigma_n) = h(\sigma_0^{\lambda_{\mathfrak{P}}^{-1}}, \dots, \sigma_n^{\lambda_{\mathfrak{P}}^{-1}})$ for $\sigma_1, \dots, \sigma_n \in \mathrm{Gal}(\hat{K}_{\mathfrak{P}})$,

(2f) the map Cor is defined for each tuple $(h_{\mathfrak{P}})_{\mathfrak{P}|\mathfrak{p}} \in \prod_{\mathfrak{P}|\mathfrak{p}} H^n(\mathrm{Gal}(\hat{K}_{\mathfrak{P}}), A)$ by

$$\mathrm{Cor}((h_{\mathfrak{P}})_{\mathfrak{P}|\mathfrak{p}}) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{cor}_{\mathfrak{P}}(h_{\mathfrak{P}}),$$

where for each $\mathfrak{P}|\mathfrak{p}$ the map $\mathrm{cor}_{\mathfrak{P}}\colon H^n(\mathrm{Gal}(\hat{K}_{\mathfrak{P}}), A) \to H^n(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ is the corestriction map for the open subgroup $\mathrm{Gal}(\hat{K}_{\mathfrak{P}})$ of $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$.

Diagram (1) is used in the proof of Theorem 1 on page 145 of [Neu79] without a proof in the case where K is a number field.

5.1 Explicit definition of the corestriction map. We set $d = [K : K_0]$ DGRb input, 86 and $d_{\mathfrak{P}} = [\hat{K}_{\mathfrak{P}} : \hat{K}_{0,\mathfrak{p}}]$ for each $\mathfrak{P}|\mathfrak{p}$. Then, we choose $\varepsilon_1, \dots, \varepsilon_d \in \mathrm{Gal}(K_0)$ and $\varepsilon_{\mathfrak{P},1}, \dots, \varepsilon_{\mathfrak{P},d_{\mathfrak{P}}} \in \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ such that

$$\mathrm{Gal}(K_0) = \mathop{\dot{\bigcup}}_{j=1}^{d} \mathrm{Gal}(K)\varepsilon_j^{-1} \text{ and } \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) = \mathop{\dot{\bigcup}}_{k=1}^{d_{\mathfrak{P}}} \mathrm{Gal}(\hat{K}_{\mathfrak{p}})\varepsilon_{\mathfrak{P},k}^{-1}. \tag{3}$$

Then, in the notation of Subsection 1.4, the polynomial $f(X) = \prod_{j=1}^d (X - x^{\varepsilon_j^{-1}})$ is irreducible over K_0, the polynomial $f_{\mathfrak{P}}(X) = \prod_{k=1}^{d_{\mathfrak{P}}}(X - x_{\mathfrak{P}}^{\varepsilon_{\mathfrak{P},k}^{-1}})$ is irreducible over $\hat{K}_{0,\mathfrak{p}}$, and $f(X) = \prod_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}}(X)$. Therefore,

(4) there exists a bijection of sets β: $\bigcup_{\mathfrak{P}|\mathfrak{p}}\{(\mathfrak{P}, 1), \ldots, (\mathfrak{P}, d_{\mathfrak{P}})\} \to \{1, \ldots, d\}$ such that $\varepsilon_{\mathfrak{P},k}^{-1}|_K = \varepsilon_{\beta(\mathfrak{P},k)}^{-1}|_K$, hence

(5) there exists $\eta_{\mathfrak{P},k} \in \mathrm{Gal}(K)$ such that $\varepsilon_{\mathfrak{P},k}^{-1}|_{K_{0,\mathrm{sep}}} = \eta_{\mathfrak{P},k}\varepsilon_{\beta(\mathfrak{P},k)}^{-1}$ for $\mathfrak{P}|\mathfrak{p}$ and $k = 1, \ldots, d$.

For each $\sigma \in \mathrm{Gal}(K_0)$, let $\tilde{\sigma}$ be the unique element of $\{\varepsilon_1, \ldots, \varepsilon_d\}$ with $\mathrm{Gal}(K)\sigma^{-1} = \mathrm{Gal}(K)\tilde{\sigma}^{-1}$. Then, cor: $H^n(\mathrm{Gal}(K), A) \to H^n(\mathrm{Gal}(K_0), A)$ is defined for each homogeneous cochain h: $\mathrm{Gal}(K)^{n+1} \to A$, and for all $(\sigma_0, \ldots, \sigma_n) \in \mathrm{Gal}(K_0)^{n+1}$ by

$$\mathrm{cor}(h)(\sigma_0, \ldots, \sigma_n) = \prod_{j=1}^{d} h(\widetilde{\sigma_0\varepsilon_j}^{-1}\sigma_0\varepsilon_j, \ldots, \widetilde{\sigma_n\varepsilon_j}^{-1}\sigma_n\varepsilon_j)^{\varepsilon_j^{-1}}. \tag{6}$$

(Compare with the formula given on page 46 of [NSW00, Subsection 1.4], where the groups act on the additive modules from the left.) Similarly, for each $\mathfrak{P} \in \mathbb{P}(K)$ over $\mathfrak{p}$, and every $\sigma \in \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$, there is a unique $\tilde{\sigma} \in \{\varepsilon_{\mathfrak{P},1}, \ldots, \varepsilon_{\mathfrak{P},d_{\mathfrak{P}}}\}$ such that $\mathrm{Gal}(\hat{K}_{\mathfrak{P}})\sigma^{-1} = \mathrm{Gal}(\hat{K}_{\mathfrak{P}})\tilde{\sigma}^{-1}$. Again, we have for each homogeneous cochain h: $\mathrm{Gal}(\hat{K}_{\mathfrak{P}})^{n+1} \to A$ and every tuple $(\sigma_0, \ldots, \sigma_n) \in \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})^{n+1}$ that

$$\mathrm{cor}_{\mathfrak{P}}(h)(\sigma_0, \ldots, \sigma_n) = \prod_{k=1}^{d_{\mathfrak{P}}} h(\widetilde{\sigma_0\varepsilon_{\mathfrak{P},k}}^{-1}\sigma_0\varepsilon_{\mathfrak{P},k}, \ldots, \widetilde{\sigma_n\varepsilon_{\mathfrak{P},k}}^{-1}\sigma_n\varepsilon_{\mathfrak{P},k})^{\varepsilon_{\mathfrak{P},k}^{-1}}. \tag{7}$$

In particular,

(8) if $\hat{K}_{\mathfrak{P}} = \hat{K}_{0,\mathfrak{p}}$, then $d_{\mathfrak{P}} = 1$, and we may choose $\varepsilon_{\mathfrak{P},1} = 1$. Hence, by (7), $\mathrm{cor}_{\mathfrak{P}}(h) = h$.

The following lemma generalizes the well-known fact that the norm of an algebraic number is the product of its local norms [CaF67, p. 55, Cor.].

Lemma 5.2: *Diagram (1) commutes for $n = 0$.* DGRc input, 177

Proof: We know that $H^0(\mathrm{Gal}(K), A) = A^{\mathrm{Gal}(K)} = \{a \in A \mid a^\sigma = a \text{ for all } \sigma \in \mathrm{Gal}(K)\}$. By (6), the map cor: $H^0(\mathrm{Gal}(K), A) \to H^0(\mathrm{Gal}(K_0), A)$ is defined (in terms of inhomogeneous 0-cochains) for each $a \in A^{\mathrm{Gal}(K)}$ by $\mathrm{cor}(a) = \prod_{j=1}^{d} a^{\varepsilon_j^{-1}}$. Similarly, for each $\mathfrak{P}|\mathfrak{p}$ we have $H^0(\mathrm{Gal}(\hat{K}_{\mathfrak{P}}), A) = A^{\mathrm{Gal}(\hat{K}_{\mathfrak{P}})}$ and $\mathrm{cor}_{\mathfrak{P}}$: $H^0(\mathrm{Gal}(\hat{K}_{\mathfrak{P}}), A) \to$

$H^0(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}),A)$ is defined for each $a\in A^{\mathrm{Gal}(\hat{K}_{\mathfrak{P}})}$ by $\mathrm{cor}_{\mathfrak{P}}(a)=\prod_{k=1}^{d_{\mathfrak{P}}} a^{\varepsilon_{\mathfrak{P},k}^{-1}}$. Moreover, for each $a\in A^{\mathrm{Gal}(K)}$ and $\sigma\in\mathrm{Gal}(\hat{K}_{\mathfrak{P}})$ we have $a^{\sigma}=a^{\sigma^{\lambda_{\mathfrak{P}}^{-1}}}=a$, so $\mathrm{res}_{\mathfrak{P}}(a)=a$. Similarly, if $a\in A^{\mathrm{Gal}(K_0)}$ and $\sigma\in\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$, we have $a^{\sigma}=a^{\sigma|_{K_{0,\mathrm{sep}}}}=a$, so $\mathrm{res}_{\mathfrak{p}}(a)=a$.

Now, let $a\in A^{\mathrm{Gal}(K)}$. Then, by (2e), (2f), (7), and (5),

$$\begin{aligned}\mathrm{Cor}\big(\mathrm{Res}(a)\big)&=\mathrm{Cor}(a,\ldots,a)=\prod_{\mathfrak{P}|\mathfrak{p}}\mathrm{cor}_{\mathfrak{P}}(a)\\&=\prod_{\mathfrak{P}|\mathfrak{p}}\prod_{k=1}^{d_{\mathfrak{P}}} a^{\varepsilon_{\mathfrak{P},k}^{-1}|_{K_{0,\mathrm{sep}}}}=\prod_{\mathfrak{P}|\mathfrak{p}}\prod_{k=1}^{d_{\mathfrak{P}}} a^{\eta_{\mathfrak{P},k}\varepsilon_{\beta(\mathfrak{P},k)}^{-1}}\ .\end{aligned}$$

Since $\eta_{\mathfrak{P},k}\in\mathrm{Gal}(K)$ and $a\in A^{\mathrm{Gal}(K)}$, we have $a^{\eta_{\mathfrak{P},k}}=a$. Therefore, by (4) and (6), $\mathrm{Cor}(\mathrm{Res}(a))=\prod_{\mathfrak{P}|\mathfrak{p}}\prod_{k=1}^{d_{\mathfrak{P}}} a^{\varepsilon_{\beta(\mathfrak{P},k)}^{-1}}=\prod_{j=1}^{d} a^{\varepsilon_j^{-1}}=\mathrm{cor}(a)=\mathrm{res}_{\mathfrak{p}}(\mathrm{cor}(a))$, as claimed. ∎

Lemma 5.3: *Diagram (1) commutes for each $n\geq 0$.* DGRd input, 233

Proof: Each of the four vertices in Diagram (1) can be considered as a cohomological functor in the sense of [Rib70, p. 120, Def. 5.1]. Moreover, res: $H^n(G,A)\to H^n(H,A)$ commutes with the connecting homomorphism of the cohomology groups for every profinite group G, every closed subgroup H, and every finite G-module A [Rib70, p. 135]. The same holds for the maps induced by the conjugations with the $\lambda_{\mathfrak{P}}$'s [NSW00, p. 48, Prop. 1.5.4 and p. 58, Prop. 1.6.2]. Hence, both horizontal maps in Diagram (1) are morphisms of cohomological functors in the sense of [Rib70, p. 121, Def. 5.2]. The same holds for the corestriction maps in (1), with H now open in G [Rib70, p. 136]. By Lemma 5.2, Diagram (1) commutes for $n=0$. Therefore, by the method of dimension shifting of cohomology theory (in particular, [Rib70, p. 124, Cor. 5.6]), Diagram (1) commutes for each $n\geq 0$. ∎

6. On the First Cohomology Group

IMAGE input, 12

As in Section 5, we consider a finite Galois extension K of K_0, and a finite multiplicative $\mathrm{Gal}(K_0)$-module A. We apply commutative diagram (1) of Section 5 to the case $n=1$.

6.1 Crossed homomorphisms. Recall that if G is a profinite group that acts on A (from the right), then each element x of $H^1(G,A)$ can be represented by an inhomogeneous chain of dimension 1. The latter is a **multiplicative crossed homomorphism** $\chi\colon G \to A$, i.e., a map that satisfies the rule $\chi(\sigma\tau) = \chi(\sigma)^\tau\chi(\tau)$ for all $\sigma, \tau \in G$. If $\chi'\colon G \to A$ is another crossed homomorphism that represents x, then χ' differs from χ by a **coboundary**. Thus, there exists $a \in A$ such that $\chi'(\sigma) = \chi(\sigma)a^\sigma a^{-1}$ for all $\sigma \in G$.

CRSs
input, 22

In particular, if the action of G on A is trivial, then $\chi' = \chi$ and $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$ for all $\sigma, \tau \in G$, so χ is just a homomorphism. Thus, in this case, we may consider x as a homomorphism from G to A.

Lemma 6.2: *If a prime $\mathfrak{p}$ of K_0 totally splits in K, then the map*

IMAa
input, 47

$$\mathrm{Cor}\colon \prod_{\mathfrak{P}|\mathfrak{p}} H^1(\mathrm{Gal}(\hat{K}_{\mathfrak{P}}), A) \to H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$$

is surjective.

Proof: Indeed, for each $\mathfrak{P}$ we have $\hat{K}_{\mathfrak{P}} = \hat{K}_{0,\mathfrak{p}}$ (Subsection 1.5). Hence, by (8) in Subsection 5.1, $\mathrm{cor}_{\mathfrak{P}}\colon H^1(\mathrm{Gal}(\hat{K}_{\mathfrak{P}}), A) \to H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ is the identity map. Now, consider $h \in H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$, and choose a prime $\mathfrak{P}$ of K over $\mathfrak{p}$. Then, set $h_{\mathfrak{P}} = h$ and $h_{\mathfrak{P}'} = 1$ for each $\mathfrak{P}' \in \mathbb{P}(K)$ over $\mathfrak{p}$ with $\mathfrak{P}' \neq \mathfrak{P}$. Then, by (2f) of Section 5, $\mathrm{Cor}((h_{\mathfrak{P}'})_{\mathfrak{P}'|\mathfrak{p}}) = \prod_{\mathfrak{P}'|\mathfrak{p}} \mathrm{cor}_{\mathfrak{P}'}(h_{\mathfrak{P}'}) = h \cdot 1 \cdots 1 = h$, as desired. ■

If H is a closed subgroup of a profinite group G, A is a finite G-module, and $h \in H^n(G,A)$, then we write $h|_H$ for the image of h under the restriction map res: $H^n(G,A) \to H^n(H,A)$.

Lemma 6.3: *Let $\mathfrak{p}$ be a prime of K_0 which is unramified in K. For each $\mathfrak{P} \in \mathbb{P}(K)$ that lies over $\mathfrak{p}$, consider $h_{\mathfrak{P}} \in H^1(\mathrm{Gal}(\hat{K}_{\mathfrak{P}}), A)$ such that $h_{\mathfrak{P}}(\hat{I}_{\mathfrak{P}}) = 1$. Let $u_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{cor}_{\mathfrak{P}}(h_{\mathfrak{P}})$. Then, $u_{\mathfrak{p}}|_{\hat{I}_{\mathfrak{p}}} = 1$.*

IMAb
input, 82

Proof: For each $\mathfrak{P}|\mathfrak{p}$ we consider $h_{\mathfrak{P}}$ also as a homogeneous cochain $h_{\mathfrak{P}}\colon \mathrm{Gal}(\hat{K}_{\mathfrak{P}}) \times \mathrm{Gal}(\hat{K}_{\mathfrak{P}}) \to A$. By assumption we then have

$$h_{\mathfrak{P}}(\hat{I}_{\mathfrak{P}} \times \hat{I}_{\mathfrak{P}}) = \mathbf{1}. \tag{1}$$

Similarly, we consider $u_{\mathfrak{p}}$ as a homogeneous cochain $u_{\mathfrak{p}}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \times \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to A$. Since $\mathfrak{p}$ is unramified in K, we have $\hat{I}_{\mathfrak{P}} = \hat{I}_{\mathfrak{p}}$ for each $\mathfrak{P}|\mathfrak{p}$ (Subsection 1.5). Hence, since $\hat{I}_{\mathfrak{p}}$ is normal in $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$, so is $\hat{I}_{\mathfrak{P}}$.

We write $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) = \dot{\bigcup}_{\tau\in T_{\mathfrak{P}}} \mathrm{Gal}(\hat{K}_{\mathfrak{P}})\tau^{-1} = \dot{\bigcup}_{\tau\in T_{\mathfrak{P}}} \tau\mathrm{Gal}(\hat{K}_{\mathfrak{P}})$ for an appropriate subset $T_{\mathfrak{P}}$ of $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$. By the preceding paragraph,

(2) $\tau^{-1}\sigma\tau \in \hat{I}_{\mathfrak{P}} \le \mathrm{Gal}(\hat{K}_{\mathfrak{P}})$ for all $\mathfrak{P}|\mathfrak{p}$, $\tau \in T_{\mathfrak{P}}$, and $\sigma \in \hat{I}_{\mathfrak{P}}$.

Moreover, in the notation of Subsection 5.1, we have by (2)

$$\widetilde{\sigma\tau}\mathrm{Gal}(\hat{K}_{\mathfrak{P}}) = \sigma\tau\mathrm{Gal}(\hat{K}_{\mathfrak{P}}) = \tau(\tau^{-1}\sigma\tau)\mathrm{Gal}(\hat{K}_{\mathfrak{P}}) = \tau\mathrm{Gal}(\hat{K}_{\mathfrak{P}}).$$

Hence, by the definition of $T_{\mathfrak{P}}$, we have $\widetilde{\sigma\tau} = \tau$, so, by (2), $\widetilde{\sigma\tau}^{-1}\sigma\tau = \tau^{-1}\sigma\tau \in \hat{I}_{\mathfrak{P}}$. Thus, by (7) in Subsection 5.1, we have for all $\sigma_0, \sigma_1 \in \hat{I}_{\mathfrak{p}}$ that

$$\begin{aligned}\mathrm{cor}_{\mathfrak{P}}(h_{\mathfrak{P}})(\sigma_0,\sigma_1) &= \prod_{\tau\in T_{\mathfrak{P}}} h_{\mathfrak{P}}(\widetilde{\sigma_0\tau}^{-1}\sigma_0\tau, \widetilde{\sigma_1\tau}^{-1}\sigma_1\tau)^{\tau^{-1}} \\ &= \prod_{\tau\in T_{\mathfrak{P}}} h_{\mathfrak{P}}(\tau^{-1}\sigma_0\tau, \tau^{-1}\sigma_1\tau)^{\tau^{-1}}.\end{aligned} \tag{3}$$

By (2) and (1), we have $h_{\mathfrak{P}}(\tau^{-1}\sigma_0\tau, \tau^{-1}\sigma_1\tau) = 1$ for each $\mathfrak{P}|\mathfrak{p}$. Hence, by (3), $\mathrm{cor}_{\mathfrak{P}}(h_{\mathfrak{P}})(\sigma_0,\sigma_1) = 1$. It follows that $u_{\mathfrak{p}}(\sigma_0,\sigma_1) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{cor}_{\mathfrak{P}}(h_{\mathfrak{P}})(\sigma_0,\sigma_1) = 1$, as claimed. ∎

7. Classes of Homomorphisms

CLAS
input, 13

It turns out that many of the properties of homomorphisms we consider are preserved under a natural equivalence relation that we explain in this section.

7.1 Embedding problems. An **embedding problem** for a profinite group $\hat{G}$ is a pair

PREd
input, 21

$$(\rho\colon \hat{G} \to \Gamma,\ \alpha\colon G \to \Gamma), \tag{1}$$

where G and Γ are profinite groups and ρ and α are epimorphisms. A **weak solution** of (1) is a homomorphism $\psi\colon \hat{G} \to G$ such that $\alpha \circ \psi = \rho$. We say that ψ is a **proper solution** if, in addition, ψ is surjective.

7.2 Conjugate Homomorphisms. Let $\Gamma, G, \hat{G}$ be profinite groups, and consider the homomorphisms $\rho\colon \hat{G} \to \Gamma$ and $\alpha\colon G \to \Gamma$. We write $\mathrm{Hom}_{\Gamma,\rho,\alpha}(\hat{G}, G)$ for the set of all homomorphisms $\psi\colon \hat{G} \to G$ that satisfy $\alpha \circ \psi = \rho$. Note that if both ρ and α are epimorphisms, then ψ is a weak solution of Embedding problem (1). PREe input, 38

Two elements ψ, ψ' of $\mathrm{Hom}_{\Gamma,\rho,\alpha}(\hat{G}, G)$ are said to be $\mathrm{Ker}(\alpha)$**-conjugate** if there exists $a \in \mathrm{Ker}(\alpha)$ such that $\psi'(\hat{g}) = a^{-1}\psi(\hat{g})a$ for each $\hat{g} \in \hat{G}$. A quick check confirms that $\mathrm{Ker}(\alpha)$-conjugacy is an equivalent relation on $\mathrm{Hom}_{\Gamma,\rho,\alpha}(\hat{G}, G)$. We denote the quotient set of $\mathrm{Hom}_{\Gamma,\rho,\alpha}(\hat{G}, G)$ under $\mathrm{Ker}(\alpha)$-conjugacy by $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\alpha}(\hat{G}, G)$. We denote the $\mathrm{Ker}(\alpha)$-conjugacy class of ψ by $[\psi]$. In general, when we consider an element $[\psi]$ of $\mathcal{H}_{\Gamma,\rho,\alpha}(\hat{G}, G)$, we tacitly assume that $\psi \in \mathrm{Hom}_{\Gamma,\rho,\alpha}(\hat{G}, G)$.

We denote the subset of $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\alpha}(\hat{G}, G)$ that consists of all elements $[\psi]$ that are surjective by $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\alpha}(\hat{G}, G)_{\mathrm{sur}}$.

Given a closed subgroup $\hat{G}_0$ of $\hat{G}$, we set $\rho_0 = \rho|_{\hat{G}_0}$. Then, the map $\psi \mapsto \psi|_{\hat{G}_0}$ induces a natural map $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\alpha}(\hat{G}, G)$ into $\mathcal{H}\mathrm{om}_{\Gamma,\rho_0,\alpha}(\hat{G}_0, G)$. Moreover, we also set $\psi_0 = \psi|_{\hat{G}_0}$, $\Gamma_0 = \rho_0(\hat{G}_0)$, $G_0 = \alpha^{-1}(\Gamma_0)$, $\alpha_0 = \alpha|_{G_0}$, and consider ρ_0 also as a homomorphism from $\hat{G}_0$ into Γ_0. Then, $\mathrm{Ker}(\alpha_0) = \mathrm{Ker}(\alpha)$ and $\mathrm{Im}(\psi_0) \leq G_0$. Hence, we may identify $\mathcal{H}\mathrm{om}_{\Gamma,\rho_0,\alpha}(\hat{G}_0, G)$ with $\mathcal{H}\mathrm{om}_{\Gamma_0,\rho_0,\alpha_0}(\hat{G}_0, G_0)$.

$$\begin{tikzcd}
 & & & \hat{G} \arrow[ddl, "\psi"'] \arrow[dd, "\rho"] \arrow[dr, dash] & \\
 & & & & \hat{G}_0 \arrow[ddl, "\psi_0"'] \arrow[dd, "\rho_0"] \\
\mathbf{1} \arrow[r] & \mathrm{Ker}(\alpha) \arrow[r] \arrow[dr, equal] & G \arrow[r, "\alpha"] \arrow[dr, dash] & \Gamma \arrow[dr, dash] & \\
 & \mathbf{1} \arrow[r] & \mathrm{Ker}(\alpha_0) \arrow[r] & G_0 \arrow[r, "\alpha_0"] & \Gamma_0.
\end{tikzcd}$$

By construction, both $\rho_0\colon \hat{G}_0 \to \Gamma_0$ and $\alpha_0\colon G_0 \to \Gamma_0$ are surjective.

7.3 Finite embedding problems over K_0. A **finite embedding problem** for a finite Galois extension K of K_0 is a pair GLOa input, 116

$$(\rho\colon \mathrm{Gal}(K_0) \to \Gamma,\ \alpha\colon G \to \Gamma), \tag{2}$$

where G is a finite group, $\Gamma = \mathrm{Gal}(K/K_0)$, $\alpha\colon G \to \Gamma$ is an epimorphism, and ρ is the restriction map $\mathrm{res}_{K_{0,\mathrm{sep}}/K}$. Thus, $\mathrm{Gal}(K) = \mathrm{Ker}(\rho)$. If $\psi\colon \mathrm{Gal}(K_0) \to G$ is a weak solution of Embedding problem (2), then the fixed field of $\mathrm{Ker}(\psi)$ in K_{sep} is said to be a **solution field** of (2).

For each $\mathfrak{p} \in \mathbb{P}(K_0)$, (global) embedding problem (2) gives rise to a **local embedding problem**

$$(3) \qquad (\rho_{\mathfrak{p}}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to \Gamma_{\mathfrak{p}},\ \alpha_{\mathfrak{p}}\colon G_{\mathfrak{p}} \to \Gamma_{\mathfrak{p}}),$$

where $\Gamma_{\mathfrak{p}} = \rho(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}))$, $\rho_{\mathfrak{p}} = \rho|_{\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})}$, $G_{\mathfrak{p}} = \alpha^{-1}(\Gamma_{\mathfrak{p}})$, and $\alpha_{\mathfrak{p}} = \alpha|_{G_{\mathfrak{p}}}$. Note that $\mathrm{Ker}(\alpha_{\mathfrak{p}}) = \mathrm{Ker}(\alpha)$.

As in Subsection 7.2, we consider $\rho_{\mathfrak{p}}$ also as a homomorphism from $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ into Γ, and identify $\mathcal{H}\mathrm{om}_{\Gamma_{\mathfrak{p}},\rho_{\mathfrak{p}},\alpha_{\mathfrak{p}}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G_{\mathfrak{p}})$ with $\mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$, thereby somewhat simplifying the notation.

Again, as in Subsection 7.2, if ψ is a weak solution of Embedding problem (2), then $\psi_{\mathfrak{p}} = \psi|_{\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})}$ is a weak solution of Embedding problem (3). When $\psi, \psi'\colon \mathrm{Gal}(K_0) \to G$ are $\mathrm{Ker}(\alpha)$-conjugate weak solutions of (2), then for each $\mathfrak{p} \in \mathbb{P}(K_0)$, the $G_{\mathfrak{p}}$-homomorphisms $\psi_{\mathfrak{p}}, \psi'_{\mathfrak{p}}$ are also $\mathrm{Ker}(\alpha)$-conjugate. This gives a canonical map

$$\mathcal{H}\mathrm{om}_{\Gamma,\rho,\alpha}(\mathrm{Gal}(K_0), G) \to \prod_{\mathfrak{p}} \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G),$$

that maps each $[\psi]$ to the family $([\psi_{\mathfrak{p}}])_{\mathfrak{p}}$.

7.4 Properties of homomorphisms. Let ψ be a homomorphism of $\mathrm{Gal}(K_0)$ into a finite group G, let L be the fixed field of $\mathrm{Ker}(\psi)$ in $K_{0,\mathrm{sep}}$, and let $\mathfrak{p} \in \mathbb{P}(K_0)$. PREf input, 177

We say that ψ **totally splits at** $\mathfrak{p}$, if $\psi(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})) = \mathbf{1}$, that is $\psi(\mathrm{Gal}(K_{0,\mathfrak{p}})) = \mathbf{1}$, which means that $L \subseteq K_{0,\mathfrak{p}}$. In this case $\mathfrak{p}$ totally splits in L, which means that L has $[L : K_0]$ primes that lie over $\mathfrak{p}$. Conversely, if $\mathfrak{p}$ totally splits in L, then $L \subseteq K_{0,\mathfrak{p}}$ (Subsection 1.5), so $\psi(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})) = \psi(\mathrm{Gal}(K_{0,\mathfrak{p}})) = \mathbf{1}$.

We say that ψ is **unramified** at $\mathfrak{p}$, if $\mathfrak{p}$ is unramified in L. If $\mathfrak{p}$ is non-archimedean, this means that $\psi(\hat{I}_{\mathfrak{p}}) = \mathbf{1}$. When $\mathfrak{p}$ is archimedean, this means that $\psi(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})) = \mathbf{1}$, alternatively $\mathfrak{p}$ totally splits in L (Subsection 1.5).

We denote the set of primes at which ψ ramifies, by $\mathrm{Ram}(\psi)$, and observe that $\mathrm{Ram}(\psi) = \mathrm{Ram}(L/K_0)$ is the set of primes of K_0 that ramify in L.

Note that if $\psi, \psi'\colon \mathrm{Gal}(K_0) \to G$ are $\mathrm{Ker}(\alpha)$-conjugate weak solutions of (2), and ψ has one of the above-mentioned properties, then ψ' also has that property. In addition, $\mathrm{Im}(\psi') = \mathrm{Im}(\psi)$, so if ψ is surjective, then so is ψ'. Finally, if ψ is trivial, then so is ψ'.

We therefore say that a conjugate class in $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\alpha}(\mathrm{Gal}(K_0), G)$ **totally splits**, is **unramified at $\mathfrak{p}$**, **surjective**, or **trivial** if one (alternatively, each) representative of that class has the corresponding property.

Similar observations and definitions (except for total splitting) apply to conjugate classes in

$$\mathcal{H}\mathrm{om}_{\Gamma,\rho_\mathfrak{p},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G),$$

for each $\mathfrak{p}$ in $\mathbb{P}(K_0)$.

8. Two Embedding Problems

EMBEDD
input, 11

The results we prove in this section ensure the weak solvability of local embedding problems in each of the cases that occur in the induction step of the solution of our global embedding problem.

LEMMA 8.1: *Let $\lambda\colon G \to \bar{G}$ be an epimorphism of profinite groups, $\mathfrak{p} \in \mathbb{P}(K_0)$, and*

PREg
input, 17

$$\bar{\psi}_\mathfrak{p}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to \bar{G}$$

an unramified homomorphism. Then, there exists an unramified homomorphism $\psi_\mathfrak{p}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to G$ such that $\lambda \circ \psi_\mathfrak{p} = \bar{\psi}_\mathfrak{p}$. If $\bar{\psi}_\mathfrak{p}$ is the trivial homomorphism and $\mathrm{Ker}(\lambda) \neq \mathbf{1}$, *we can choose $\psi_\mathfrak{p}$ such that in addition* $\mathrm{Ker}(\lambda) \cap \mathrm{Im}(\psi_\mathfrak{p}) \neq \mathbf{1}$.

Proof: If $\mathfrak{p}$ is archimedean, then $\bar{\psi}_\mathfrak{p}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})) = \mathbf{1}$ (Subsection 7.4). Then, the trivial homomorphism $\psi_\mathfrak{p}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to G$ is unramified and satisfies $\lambda \circ \psi_\mathfrak{p} = \bar{\psi}_\mathfrak{p}$.

Now assume that $\mathfrak{p}$ is non-archimedean. Let $\pi\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to \mathrm{Gal}(\hat{K}_{0,\mathfrak{p},\mathrm{ur}}/\hat{K}_{0,\mathfrak{p}})$ be the restriction map. By assumption, $\bar{\psi}_\mathfrak{p}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p},\mathrm{ur}})) = \bar{\psi}_\mathfrak{p}(\hat{I}_\mathfrak{p}) = \mathbf{1}$. Hence, there exists a homomorphism $\bar{\kappa}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p},\mathrm{ur}}/\hat{K}_{0,\mathfrak{p}}) \to \bar{G}$ such that $\bar{\psi}_\mathfrak{p} = \bar{\kappa} \circ \pi$. By [CaF67, p. 28], $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p},\mathrm{ur}}/\hat{K}_{0,\mathfrak{p}}) \cong \hat{\mathbb{Z}}$. Let z be a generator of $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p},\mathrm{ur}}/\hat{K}_{0,\mathfrak{p}})$, and choose $a \in G$

such that $\lambda(a) = \bar{\kappa}(z)$. Let κ: $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p},\mathrm{ur}}/\hat{K}_{0,\mathfrak{p}}) \to G$ be the unique homomorphism with $\kappa(z) = a$, so $\lambda\circ\kappa = \bar{\kappa}$, and consider the homomorphism $\psi_\mathfrak{p} = \kappa\circ\pi$: $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to G$. It satisfies $\lambda \circ \psi_\mathfrak{p} = \bar{\psi}_\mathfrak{p}$ and $\psi_\mathfrak{p}(\hat{I}_\mathfrak{p}) = \mathbf{1}$, so $\psi_\mathfrak{p}$ is an unramified homomorphism.

If $\bar{\psi}_\mathfrak{p}$ is the trivial homomorphism and $\mathrm{Ker}(\lambda) \neq \mathbf{1}$, then we choose $\tilde{z} \in \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ with $z = \pi(\tilde{z})$. Then, $\bar{\kappa}(z) = \bar{\kappa}(\pi(\tilde{z})) = \bar{\psi}_\mathfrak{p}(\tilde{z}) = 1$. Hence, we may choose a above to be a non-unit element of $\mathrm{Ker}(\lambda)$. In particular, the unramified homomorphism $\psi_\mathfrak{p}$ now satisfies $\psi_\mathfrak{p}(\tilde{z}) = a$, so $\mathrm{Ker}(\lambda) \cap \mathrm{Im}(\psi_\mathfrak{p}) \neq \mathbf{1}$, as desired. ∎

Definition 8.2: A homomorphism λ: $G \to \bar{G}$ of profinite groups is said to be a C_l-homomorphism, for a prime number l, if $\mathrm{Im}(\lambda)$ is contained in a subgroup of $\bar{G}$ which is isomorphic to C_l. ∎ CLIs input, 81

Lemma 8.3: *Let λ: $G \to \bar{G}$ be an epimorphism of finite groups. Let l be a prime number, and suppose that $C_l \leq \bar{G}$, set $e = |\mathrm{Ker}(\lambda)|$, and let n be a multiple of el with $\mathrm{char}(K_0) \nmid n$. Also, consider $\mathfrak{p} \in \mathbb{P}(K_0)$ such that $\mathfrak{p} \nmid l, \infty$ and $\zeta_n \in \hat{K}_{0,\mathfrak{p}}$. Let $\bar{\psi}_\mathfrak{p}$: $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to \bar{G}$ be a ramified C_l-homomorphism (thus, $\bar{\psi}_\mathfrak{p}(\hat{I}_\mathfrak{p}) \neq \mathbf{1}$). Then, there exists a homomorphism $\psi_\mathfrak{p}$: $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to G$ such that $\lambda \circ \psi_\mathfrak{p} = \bar{\psi}_\mathfrak{p}$.* PREh input, 89

Proof: Let $N_\mathfrak{p}$ be the fixed field of $\mathrm{Ker}(\bar{\psi}_\mathfrak{p})$ in $\hat{K}_{0,\mathfrak{p},\mathrm{sep}}$. Since $\mathrm{Im}(\bar{\psi}_\mathfrak{p}) \leq C_l$ and $\bar{\psi}_\mathfrak{p}(\hat{I}_\mathfrak{p}) \neq \mathbf{1}$, we have $\mathrm{Im}(\bar{\psi}_\mathfrak{p}) = C_l$. Hence, $N_\mathfrak{p}/\hat{K}_{0,\mathfrak{p}}$ is a cyclic ramified extension of degree l, and we identify $\mathrm{Gal}(N_\mathfrak{p}/\hat{K}_{0,\mathfrak{p}})$ with $\mathrm{Im}(\bar{\psi}_\mathfrak{p})$. Since $\mathfrak{p} \nmid l$, the ramification of $N_\mathfrak{p}/\hat{K}_{0,\mathfrak{p}}$ is tame. Since $\zeta_n \in \hat{K}_{0,\mathfrak{p}}$, we have $\zeta_l \in \hat{K}_{0,\mathfrak{p}}$. By [CaF67, p. 32, Prop. 1(i)], there exists a prime element π of $\hat{K}_{0,\mathfrak{p}}$ with $N_\mathfrak{p} = \hat{K}_{0,\mathfrak{p}}(\sqrt[l]{\pi})$. Let $\bar{\sigma}$ be a generator of $\mathrm{Gal}(N_\mathfrak{p}/\hat{K}_{0,\mathfrak{p}})$ and choose $\sigma \in G$ with $\lambda(\sigma) = \bar{\sigma}$.

We denote the order of σ by d, let $\lambda' = \lambda|_{\langle\sigma\rangle}$, and set $e' = |\mathrm{Ker}(\lambda')|$. Since $\mathrm{Ker}(\lambda')$ is a subgroup of $\mathrm{Ker}(\lambda)$, we have $e'|e$. Since $d = e'l$, $e'|e$, and $el|n$, we have $d|n$. Since $\zeta_n \in \hat{K}_{0,\mathfrak{p}}$, we have $\zeta_d \in \hat{K}_{0,\mathfrak{p}}$. Thus, $N'_\mathfrak{p} = \hat{K}_{0,\mathfrak{p}}(\sqrt[d]{\pi})$ is a (tamely ramified) cyclic extension of $\hat{K}_{0,\mathfrak{p}}$ of degree d that contains $N_\mathfrak{p}$. Since $N_\mathfrak{p}$ is the fixed field of $\mathrm{Ker}(\bar{\psi}_\mathfrak{p})$, there exists an epimorphism $\bar{\varphi}_\mathfrak{p}$: $\mathrm{Gal}(N'_\mathfrak{p}/\hat{K}_{0,\mathfrak{p}}) \to \mathrm{Gal}(N_\mathfrak{p}/\hat{K}_{0,\mathfrak{p}})$ such that $\bar{\psi}_\mathfrak{p} = \bar{\varphi}_\mathfrak{p} \circ \mathrm{res}_{\hat{K}_{0,\mathfrak{p},\mathrm{sep}}/N'_\mathfrak{p}}$.

Finally we choose a generator τ of $\mathrm{Gal}(N'_\mathfrak{p}/\hat{K}_{0,\mathfrak{p}})$ such that $\bar{\varphi}_\mathfrak{p}(\tau) = \bar{\sigma}$, and define a homomorphism h: $\mathrm{Gal}(N'_\mathfrak{p}/\hat{K}_{0,\mathfrak{p}}) \to G$, by setting $h(\tau) = \sigma$. Then, the homomorphism

$\psi_{\mathfrak{p}} = h \circ \mathrm{res}_{\hat{K}_{0,\mathfrak{p},\mathrm{sep}}/N'_{\mathfrak{p}}}$ satisfies $\lambda \circ \psi_{\mathfrak{p}} = \bar{\psi}_{\mathfrak{p}}$, as desired.

$$\begin{tikzcd}
 & \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \arrow[dl, "\mathrm{res}"'] \arrow[d, "\mathrm{res}"'] \arrow[dd, bend left, "\bar{\psi}_{\mathfrak{p}}"] \\
\mathrm{Gal}(N'_{\mathfrak{p}}/\hat{K}_{0,\mathfrak{p}}) \arrow[r, "\bar{\varphi}_{\mathfrak{p}}"] \arrow[d, "h"'] & \mathrm{Gal}(N_{\mathfrak{p}}/\hat{K}_{0,\mathfrak{p}}) \arrow[d] \\
G \arrow[r, "\lambda"] & \bar{G}
\end{tikzcd}$$ ∎

9. An Element of $H^1(\mathrm{Gal}(K_0), A)$ that Satisfies Local Conditions

NEUK input, 12

For a simple $\mathrm{Gal}(K_0)$-module $A \cong C_l^r$, we establish the existence of an element of $H^1(\mathrm{Gal}(K_0), A)$ that satisfies finitely many local conditions, and is otherwise unramified except at most r additional primes of K_0.

9.1 Ramification of cohomology classes. Let A be a finite $\mathrm{Gal}(K_0)$-module and consider $\mathfrak{p} \in \mathbb{P}_{\mathrm{nonarch}}(K_0)$. By [NSW00, p. 64, Prop. 1.6.6], the inflation-restriction sequence for the inertia subgroup $\hat{I}_{\mathfrak{p}}$ of $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ NEUa input, 21

$$(1) \qquad 1 \longrightarrow H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})/\hat{I}_{\mathfrak{p}}, A^{\hat{I}_{\mathfrak{p}}}) \xrightarrow{\mathrm{inf}} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A) \xrightarrow{\mathrm{res}} H^1(\hat{I}_{\mathfrak{p}}, A),$$

is exact. An element $x \in H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ is **unramified** if $x \in \mathrm{Im}(\mathrm{inf})$, alternatively, if $\mathrm{res}(x) = 1$.

If $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ acts trivially on A, then $x\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to A$ is a homomorphism (Subsection 6.1). In this case, x is unramified as an element of $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$, if and only if x is unramified as a homomorphism, that is $x(\hat{I}_{\mathfrak{p}}) = \mathbf{1}$ (Subsection 7.4).

Lemma 9.2: *Let K be a finite Galois extension of K_0 and $l \neq \mathrm{char}(K_0)$ a prime number with $\zeta_l \notin K$. Let $A = C_l^r$ be a simple $\mathrm{Gal}(K_0)$-module on which $\mathrm{Gal}(K)$ acts trivially. Let T be a finite set of primes of K_0, and for each $\mathfrak{p} \in T$ consider an element $y_{\mathfrak{p}} \in H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$. Then, there exists an element $z \in H^1(\mathrm{Gal}(K_0), A)$ such that* NEUc input, 53

(a) $\mathrm{res}_{\mathfrak{p}}(z) = y_{\mathfrak{p}}$ *for each $\mathfrak{p} \in T$, and*

(b) *if $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus T$ and $\mathrm{res}_\mathfrak{p}(z)$ is ramified, then $\mathfrak{p}$ totally splits in $K(\zeta_l)$.*

On the proof: Our result appears as Lemma 3 on page 143 of [Neu79] for the case where K_0 is a number field. The proof of that lemma relies on [Neu79, p. 142, Lemma 2]. Both proofs generalize mutatis mutandis to the case where K_0 is a global field. We supply more detailed proofs of both lemmas in the appendix of this work. $\blacksquare$

NEUe input, 80

PROPOSITION 9.3: *Let $K_0 \subseteq K \subseteq L$ be a tower of finite Galois extensions of global fields such that L/K is an abelian l-extension for which $l \neq \mathrm{char}(K_0)$ and $\zeta_l \notin K$. Let $A = C_l^r$ be a simple $\mathrm{Gal}(K_0)$-module on which $\mathrm{Gal}(K)$ acts trivially. Let n be a positive integer such that $l|n$ and $\mathrm{char}(K_0) \nmid n$ and let T be a finite subset of $\mathbb{P}(K_0)$ that contains $\mathrm{Ram}(K/K_0)$. We suppose that $S_{0,l}(K) \subseteq T_K$ (Subsection 1.6). For each $\mathfrak{p} \in T$, let $y_\mathfrak{p} \in H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$.*

Then, there exist distinct primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_r \in \mathbb{P}(K_0) \smallsetminus T$, and there exists $x \in H^1(\mathrm{Gal}(K_0), A)$ such that

(a) *for each $\mathfrak{p} \in T$ we have $\mathrm{res}_\mathfrak{p}(x) = y_\mathfrak{p}$,*

(b) *for each $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus (T \cup \{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\})$, the element $\mathrm{res}_\mathfrak{p}(x)$ of $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ is unramified, and*

(c) *for $i = 1, \ldots, r$, the prime $\mathfrak{q}_i$ totally splits in $L(\zeta_n)$ and $\mathrm{res}_{\mathfrak{q}_i}(x)\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \to A$ is a C_l-homomorphism (Definition 8.2).*

(d) *Moreover, let G and $\bar{G}$ be finite groups such that $A \leq \bar{G}$ and let $\lambda\colon G \to \bar{G}$ be an epimorphism. Suppose that $|\mathrm{Ker}(\lambda)| \cdot l$ divides n. Then, for each $1 \leq i \leq r$ there exists a homomorphism $x'_{\mathfrak{q}_i}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \to G$ such that $\lambda \circ x'_{\mathfrak{q}_i} = \mathrm{res}_{\mathfrak{q}_i}(x)$.*

Proof: We choose an element $z \in H^1(\mathrm{Gal}(K_0), A)$ that satisfies Conditions (a) and (b) of Lemma 9.2, and we break up the rest of the proof into three parts.

PART A: *Definition of $\eta_\mathfrak{p}$.* Let $V = T \cup \{\mathfrak{p} \in \mathbb{P}(K_0) \mid \mathrm{res}_\mathfrak{p}(z) \text{ is ramified}\}$. For each $\mathfrak{p} \in V$ we define an element $\eta_\mathfrak{p} \in H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ as follows:

$$\eta_\mathfrak{p} = 1 \text{ for } \mathfrak{p} \in T \text{ and } \eta_\mathfrak{p} = \mathrm{res}_\mathfrak{p}(z)^{-1} \text{ for } \mathfrak{p} \in V \smallsetminus T. \tag{2}$$

CLAIM: For each $\mathfrak{p} \in V$, the element $\eta_\mathfrak{p}$ lies in the image of the map

$$\mathrm{Cor}\colon \prod_{\mathfrak{P}|\mathfrak{p}} H^1(\mathrm{Gal}(\hat{K}_\mathfrak{P}), A) \to H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A). \tag{3}$$

Indeed, the claim holds for $\mathfrak{p} \in T$, because by (2), $\eta_\mathfrak{p} = 1$ for $\mathfrak{p} \in T$ and $\mathrm{Cor} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{cor}_\mathfrak{P}$ is a homomorphism of groups. If $\mathfrak{p} \in V \smallsetminus T$, then by the definition of V, $\mathrm{res}_\mathfrak{p}(z)$ is ramified. Hence, by (b) of Lemma 9.2, $\mathfrak{p}$ totally splits in $K(\zeta_l)$, so $\mathfrak{p}$ totally splits in K. Therefore, by Lemma 6.2, Cor is surjective. In particular, $\eta_\mathfrak{p}$ belongs to the image of Cor, as claimed.

PART B: *Shifting the $\eta_\mathfrak{p}$'s.* By Part A, we choose for each $\mathfrak{p} \in V$ and each $\mathfrak{P} \in \mathbb{P}(K)$ over $\mathfrak{p}$, an element $\tilde{\eta}_\mathfrak{P} \in H^1(\mathrm{Gal}(\hat{K}_\mathfrak{P}), A)$ such that

$$\eta_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{cor}_\mathfrak{P}(\tilde{\eta}_\mathfrak{P}). \tag{4}$$

Since $\mathrm{Gal}(K)$ acts trivially on A, the group $\mathrm{Gal}(\hat{K}_\mathfrak{P})$ acts trivially on A (by (2b) of Section 5), hence $\tilde{\eta}_\mathfrak{P}\colon \mathrm{Gal}(\hat{K}_\mathfrak{P}) \to A$ is a homomorphism for each $\mathfrak{P}|\mathfrak{p}$ (Subsection 6.1). Likewise

(5) $z' = z|_{\mathrm{Gal}(K)}\colon \mathrm{Gal}(K) \to A$ is a homomorphism.

Let L' be the fixed field of $\mathrm{Ker}(z')$ in K_{sep}. Then, L' is a finite abelian l-extension of K, hence so is LL'. Hence, by Remark 4.1, the Galois closure L'' of LL' over K_0 is also a finite abelian l-extension of K. Then, Proposition 4.2 applied to the tower of global fields $K_0 \subseteq K \subseteq L''$, the set of primes V_K (Subsection 1.4), and the system of homomorphisms $(\eta_\mathfrak{P})_{\mathfrak{P}\in V_K}$ give distinct primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_r \in \mathbb{P}(K_0) \smallsetminus V$, primes $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r \in \mathbb{P}(K)$ over $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$, respectively, and a homomorphism $h\colon \mathrm{Gal}(K) \to A$ such that

(6a) $\mathfrak{q}_i$ totally splits in $L''(\zeta_n)$ for $i = 1, \ldots, r$,

(6b) $\mathrm{res}_\mathfrak{Q}(h)(\mathrm{Gal}(\hat{K}_\mathfrak{Q})) \le \mathbf{1} \times \cdots \times \mathbf{1} \times C_{l,i} \times \mathbf{1} \times \cdots \times \mathbf{1}$ for each $\mathfrak{Q} \in \mathbb{P}(K)$ over $\mathfrak{q}_i$.

(6c) $\mathrm{res}_\mathfrak{P}(h) = \tilde{\eta}_\mathfrak{P}$ for each $\mathfrak{P} \in V_K$, and

(6d) $\mathrm{res}_\mathfrak{P}(h)(\hat{I}_\mathfrak{P}) = \mathbf{1}_A$ for each $\mathfrak{P} \in \mathbb{P}(K) \smallsetminus (V_K \cup \{\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r\})$.

We consider $u = \mathrm{cor}(h) \in H^1(\mathrm{Gal}(K_0), A)$, where cor is the corestriction map that appears in Diagram (1) of Section 5 for $n = 1$. By the commutativity of that diagram (Lemma 5.3), by (6c), and by (4), we have for each $\mathfrak{p} \in V$

$$\begin{aligned} \mathrm{res}_\mathfrak{p}(u) &= \mathrm{res}_\mathfrak{p}(\mathrm{cor}(h)) = \mathrm{Cor}(\mathrm{Res}(h)) = \mathrm{Cor}\big((\mathrm{res}_\mathfrak{P}(h))_{\mathfrak{P}|\mathfrak{p}}\big) \\ &= \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{cor}_\mathfrak{P}(\mathrm{res}_\mathfrak{P}(h)) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{cor}_\mathfrak{P}(\tilde{\eta}_\mathfrak{P}) = \eta_\mathfrak{p}. \end{aligned} \tag{7}$$

PART B': *A C_l-homomorphism.* We prove for $i = 1, \dots, r$ that

(8) $\mathrm{res}_{\mathfrak{q}_i}(u) = \prod_{\mathfrak{Q}|\mathfrak{q}_i} \mathrm{cor}_{\mathfrak{Q}}(\mathrm{res}_{\mathfrak{Q}}(h))\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \to A$ is a C_l-homomorphism.

Indeed, let $\mathfrak{Q}$ be a prime of K over $\mathfrak{q}_i$. Since $\mathfrak{q}_i$ totally splits in K (by (6a)), $\mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i}) = \mathrm{Gal}(\hat{K}_{\mathfrak{Q}})$ (Subsection 1.5). For each $\hat{\sigma} \in \mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i})$ we observe that $\sigma = \hat{\sigma}^{\lambda_{\mathfrak{Q}}^{-1}} \in \mathrm{Gal}(K_{\mathfrak{Q}}) \le \mathrm{Gal}(K)$ (Subsection 1.4). Since $\mathrm{Gal}(K)$ acts trivially on A, we have, by Convention (2a) of Section 5, that $a^{\hat{\sigma}} = a^{\sigma} = a$ for each $a \in A$. Hence, by Subsection 6.1, $\mathrm{res}_{\mathfrak{q}_i}(u)\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \to A$ is a homomorphism.

Since $\mathfrak{q}_i$ totally splits in K, we have $\mathrm{cor}_{\mathfrak{Q}}(\mathrm{res}_{\mathfrak{Q}}(h)) = \mathrm{res}_{\mathfrak{Q}}(h)$ for each $\mathfrak{Q}|\mathfrak{q}_i$ (Statement (8) of Section 5). By (6b), $\mathrm{res}_{\mathfrak{Q}}(h)(\mathrm{Gal}(\hat{K}_{\mathfrak{Q}})) \le \mathbf{1} \times \cdots \times \mathbf{1} \times C_{l,i} \times \mathbf{1} \times \cdots \times \mathbf{1}$, so $\mathrm{res}_{\mathfrak{q}_i}(u)(\mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i})) \le \mathbf{1} \times \cdots \times \mathbf{1} \times C_{l,i} \times \mathbf{1} \times \cdots \times \mathbf{1}$, as claimed.

PART C: *The element x.* We prove that the element $x = uz \in H^1(\mathrm{Gal}(K_0), A)$ satisfies Conditions (a)–(d) of the proposition.

Proof of (a): For each $\mathfrak{p} \in T$ we have by (7), (a) of Lemma 9.2, and (2) that $\mathrm{res}_{\mathfrak{p}}(x) = \mathrm{res}_{\mathfrak{p}}(u)\mathrm{res}_{\mathfrak{p}}(z) = \eta_{\mathfrak{p}} y_{\mathfrak{p}} = y_{\mathfrak{p}}$, as Condition (a) claims.

Proof of (b): Let $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus (T \cup \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\})$. If $\mathfrak{p} \in V$, then by (7) and (2), we have $\mathrm{res}_{\mathfrak{p}}(x) = \mathrm{res}_{\mathfrak{p}}(u)\mathrm{res}_{\mathfrak{p}}(z) = \eta_{\mathfrak{p}} \cdot \mathrm{res}_{\mathfrak{p}}(z) = \mathrm{res}_{\mathfrak{p}}(z)^{-1} \cdot \mathrm{res}_{\mathfrak{p}}(z) = 1$. In particular, $\mathrm{res}_{\mathfrak{p}}(x)$ is unramified (Subsection 9.1). If $\mathfrak{p} \notin V$, then by the definition of V in Part A, $\mathrm{res}_{\mathfrak{p}}(z)$ is unramified, thus $\mathrm{res}_{\mathfrak{p}}(z)|_{\hat{I}_{\mathfrak{p}}} = 1$. Since $\mathrm{Ram}(K/K_0) \subseteq T \subseteq V$, we have that $\mathfrak{p}$ is unramified in K. By (6d), $\mathrm{res}_{\mathfrak{P}}(h)(\hat{I}_{\mathfrak{P}}) = \mathbf{1}_A$ for each $\mathfrak{P}|\mathfrak{p}$ and by (7), $\mathrm{res}_{\mathfrak{p}}(u) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{cor}_{\mathfrak{P}}(\mathrm{res}_{\mathfrak{P}}(h))$. Hence, by Lemma 6.3, $\mathrm{res}_{\mathfrak{p}}(x)|_{\hat{I}_{\mathfrak{p}}} = \mathrm{res}_{\mathfrak{p}}(u)|_{\hat{I}_{\mathfrak{p}}} \mathrm{res}_{\mathfrak{p}}(z)|_{\hat{I}_{\mathfrak{p}}} = 1$, so $\mathrm{res}_{\mathfrak{p}}(x)$ is unramified, as asserted by (b).

Proof of (c): Consider an i between 1 and r. By (8), $\mathrm{res}_{\mathfrak{q}_i}(u) \in H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i}), A)$ is a C_l-homomorphism.

By (6a), $\mathfrak{q}_i$ totally splits in K. Hence, $\mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i}) = \mathrm{Gal}(\hat{K}_{\mathfrak{Q}})$ for each prime $\mathfrak{Q}$ of K over $\mathfrak{q}_i$. In particular, this is the case for the prime $\mathfrak{Q}$ of K that lies over $\mathfrak{q}_i$ such that $\lambda_{\mathfrak{Q}}$ is the inclusion map (Subsection 1.4). Since $\mathrm{Gal}(K)$ acts trivially on A, the group $\mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i})$ acts trivially on A. Hence, $\mathrm{res}_{\mathfrak{q}_i}(z) \in H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i}), A)$ is a homomorphism (Subsection 9.1). Moreover, with $z' = z|_{\mathrm{Gal}(K)}$ being the homomorphism introduced in (5), we have by the choice of $\mathfrak{Q}$, that $\mathrm{res}_{\mathfrak{q}_i}(z) = \mathrm{res}_{\mathfrak{Q}}(z')$. Again, by (6a), $\mathfrak{Q}$ totally splits in L'. Since $\mathrm{Gal}(L') = \mathrm{Ker}(z')$ (Part B), the homomorphism $\mathrm{res}_{\mathfrak{q}_i}(z)\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \to A$ is trivial. Hence, $L' \subseteq \hat{K}_{\mathfrak{Q}}$. Then, $\mathrm{res}_{\mathfrak{q}_i}(x) = \mathrm{res}_{\mathfrak{q}_i}(u)$, so by the preceding paragraph, $\mathrm{res}_{\mathfrak{q}_i}(x)$ is a C_l-homomorphism as (c) claims.

Proof of (d): We fix an i between 1 and r. By (c), $\mathrm{res}_{\mathfrak{q}_i}(x)\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \to A$ is a C_l-homomorphism. If $\mathrm{res}_{\mathfrak{q}_i}(x)$ is unramified, then by Lemma 8.1, there exists a homomorphism $x'_{\mathfrak{q}_i}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \to G$ such that $\lambda \circ x'_{\mathfrak{q}_i} = \mathrm{res}_{\mathfrak{q}_i}(x)$. Otherwise, $\mathrm{res}_{\mathfrak{q}_i}(x)$ is ramified. By (c), $\zeta_n \in \hat{K}_{0,\mathfrak{q}_i}$. Since $\mathfrak{q}_i \in \mathbb{P}(K_0) \smallsetminus T$, $\mathfrak{q}_i \nmid l, \infty$. Hence, the result follows from Lemma 8.3. ∎

10. Principal Homogeneous Spaces

PHSP
input, 12

We describe how to shift a weak solution of our global embedding problem by an element of the first cohomology group.

10.1 An embedding problem. Let K be a finite Galois extension of K_0. We set $\Gamma = \mathrm{Gal}(K/K_0)$, $\rho = \mathrm{res}_{K_{0,\mathrm{sep}}/K}\colon \mathrm{Gal}(K_0) \to \Gamma$ (so $\mathrm{Gal}(K) = \mathrm{Ker}(\rho)$), and consider an embedding problem

MODa
input, 20

$$(1) \qquad (\rho\colon \mathrm{Gal}(K_0) \to \Gamma,\ \bar{\alpha}\colon \bar{G} \to \Gamma),$$

where $\bar{G}$ is a finite group, $\bar{\alpha}$ is an epimorphism, and $A = \mathrm{Ker}(\bar{\alpha})$ is abelian. The latter assumption implies that the action of $\bar{G}$ on A by conjugation induces an action of Γ on A (from the right). Thus, for all $a \in A$, $\gamma \in \Gamma$, and $\bar{g} \in \bar{G}$ with $\bar{\alpha}(\bar{g}) = \gamma$, we have $a^\gamma = \bar{g}^{-1} a \bar{g}$. We lift that action to an action of $\mathrm{Gal}(K_0)$ on A via ρ, making A a multiplicative $\mathrm{Gal}(K_0)$-**module**. In other words, for each $a \in A$, $\sigma \in \mathrm{Gal}(K_0)$, and $\bar{g} \in \bar{G}$ with $\bar{\alpha}(\bar{g}) = \rho(\sigma)$, we have $a^\sigma = \bar{g}^{-1} a \bar{g}$. Under this action $\mathrm{Gal}(K)$ acts trivially on A. In particular,

(2) if ψ is a weak solution of embedding problem (1), then $a^\sigma = \psi(\sigma)^{-1} a \psi(\sigma)$ for all $a \in A$ and $\sigma \in \mathrm{Gal}(K_0)$.

As usual, one says that A is a **simple** $\mathrm{Gal}(K_0)$**-module** if A has no submodule except itself and $\mathbf{1}$.

LEMMA 10.2: *Under the above assumptions, let ψ be a weak solution of embedding problem (1) and let χ: $\mathrm{Gal}(K_0) \to A$ be a crossed homomorphism. Then, the map $\psi\cdot\chi$: $\mathrm{Gal}(K_0) \to \bar{G}$ defined by $(\psi\cdot\chi)(\sigma) = \psi(\sigma)\chi(\sigma)$ for each $\sigma \in \mathrm{Gal}(K_0)$ is also a weak solution of embedding problem (1).* PHSa input, 57

Proof: We set $\psi^* = \psi\cdot\chi$ and observe by (2) that for all $\sigma_1, \sigma_2 \in \mathrm{Gal}(K_0)$

$$\begin{aligned}\psi^*(\sigma_1\sigma_2) &= \psi(\sigma_1\sigma_2)\chi(\sigma_1\sigma_2) = \psi(\sigma_1)\psi(\sigma_2)\chi(\sigma_1)^{\sigma_2}\chi(\sigma_2). \\ &= \psi(\sigma_1)\psi(\sigma_2)\psi(\sigma_2)^{-1}\chi(\sigma_1)\psi(\sigma_2)\chi(\sigma_2) = \psi^*(\sigma_1)\psi^*(\sigma_2).\end{aligned}$$

Thus, ψ^*: $\mathrm{Gal}(K_0) \to \bar{G}$ is a homomorphism. Since $\chi(\sigma) \in A$, we also have $\bar{\alpha}(\psi^*(\sigma)) = \bar{\alpha}(\psi(\sigma))\bar{\alpha}(\chi(\sigma)) = \rho(\sigma)$, for all $\sigma \in \mathrm{Gal}(K_0)$, as claimed. ∎

10.3 AN ACTION ON $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), \bar{G})$. The product defined in Lemma 10.2 gives rise to a right action of $H^1(\mathrm{Gal}(K_0), A)$ on $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), \bar{G})$. Indeed, ACTi input, 95

(3) if $[\psi] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), \bar{G})$ and $x \in H^1(\mathrm{Gal}(K_0), A)$, we choose a crossed homomorphism

χ: $\mathrm{Gal}(K_0) \to A$ that represents x and set $[\psi]^x = [\psi\cdot\chi]$.

By Lemma 10.2, $[\psi\cdot\chi] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), \bar{G})$. We claim that the class $[\psi\cdot\chi]$ does not depend on ψ nor on χ.

Indeed, if ψ': $\mathrm{Gal}(K_0) \to \bar{G}$ is an additional weak solution of embedding problem (1) with $[\psi'] = [\psi]$, then there exists $a \in A$ such that for each $\sigma \in \mathrm{Gal}(K_0)$ we have $\psi'(\sigma) = a^{-1}\psi(\sigma)a$ (Subsection 7.2). Also, if χ': $\mathrm{Gal}(K_0) \to A$ is another crossed homomorphism that represents x, there exists $b \in A$ such that for all $\sigma \in \mathrm{Gal}(K_0)$ we have $\chi'(\sigma) = b^\sigma b^{-1}\chi(\sigma) = \psi(\sigma)^{-1}b\psi(\sigma)b^{-1}\chi(\sigma)$ (Subsection 6.1). Since A is normal in $\bar{G}$, we have $\psi(\sigma)a\psi(\sigma)^{-1} \in A$. Hence, since A is abelian, we have $(\psi(\sigma)a\psi(\sigma)^{-1})b = b\psi(\sigma)a\psi(\sigma)^{-1}$. Therefore, using Lemma 10.2, the weak solution $\psi'' = \psi'\cdot\chi'$ of (1) satisfies for each $\sigma \in \mathrm{Gal}(K_0)$ that

$$\begin{aligned}\psi''(\sigma) = \psi'(\sigma)\chi'(\sigma) &= a^{-1}(\psi(\sigma)a\psi(\sigma)^{-1})b\psi(\sigma)b^{-1}\chi(\sigma) \\ &= a^{-1}b\psi(\sigma)a\psi(\sigma)^{-1}\psi(\sigma)b^{-1}\chi(\sigma) = a^{-1}b\psi(\sigma)ab^{-1}\chi(\sigma) \\ &= a^{-1}b\psi(\sigma)\chi(\sigma)ab^{-1} = (ab^{-1})^{-1}\psi'(\sigma)(ab^{-1}),\end{aligned}$$

hence $[\psi''] = [\psi']$, as claimed.

In a similar way, for each $\mathfrak{p} \in \mathbb{P}(K_0)$ the cohomology group $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ acts on

$$\mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), \bar{G}).$$

Both actions are compatible with the restriction from $\mathrm{Gal}(K_0)$ to $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$. In other words,

(4) $[\psi]^x|_{\mathfrak{p}} = [\psi_{\mathfrak{p}}]^{\mathrm{res}_{\mathfrak{p}}(x)}$ for $[\psi] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), \bar{G})$, $x \in H^1(\mathrm{Gal}(K_0), A)$, and $\mathfrak{p} \in \mathbb{P}(K_0)$.

Recall that a **principal homogeneous space** X over a group H is a set X on which H acts **freely** and **transitively** (from the right). This means that if $x \in X$ and $\eta \in H$ satisfy $x^\eta = x$, then $\eta = 1$; moreover for all $y \in X$ there exists $\tau \in H$ such that $x^\tau = y$.

LEMMA 10.4: *The set $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), \bar{G})$ (resp. $\mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), \bar{G})$) is a principal homogeneous space over $H^1(\mathrm{Gal}(K_0), A)$ (resp. over $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$).*

PHSb
input, 174

Proof: Consider $[\varphi], [\psi] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), \bar{G})$. Let $\chi\colon \mathrm{Gal}(K_0) \to \bar{G}$ be the map defined by $\chi(\sigma) = \varphi(\sigma)^{-1}\psi(\sigma)$ for each $\sigma \in \mathrm{Gal}(K_0)$. Then, $\bar{\alpha}(\varphi(\sigma)^{-1})\bar{\alpha}(\psi(\sigma)) = \rho(\sigma)^{-1}\rho(\sigma) = 1$, hence $\varphi(\sigma)^{-1}\psi(\sigma) \in A$, so χ maps $\mathrm{Gal}(K_0)$ into A. Next observe that

$$\chi(\sigma)^\tau\chi(\tau) = \big(\varphi(\tau)^{-1}\varphi(\sigma)^{-1}\psi(\sigma)\varphi(\tau)\big)\big(\varphi(\tau)^{-1}\psi(\tau)\big) = \varphi(\sigma\tau)^{-1}\psi(\sigma\tau) = \chi(\sigma\tau),$$

so $\chi\colon \mathrm{Gal}(K_0) \to A$ is a crossed homomorphism. Let $x \in H^1(\mathrm{Gal}(K_0), A)$ be the cohomology class of χ. Then, by (3), $[\psi] = [\varphi]^x$, so the action of $H^1(\mathrm{Gal}(K_0), A)$ on $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), \bar{G})$ is transitive.

Now suppose that $[\varphi]^x = [\varphi]$ for some $x \in H^1(\mathrm{Gal}(K_0), A)$. Let $\chi\colon \mathrm{Gal}(K_0) \to A$ be a crossed homomorphism that represents x. Then, by Subsection 7.2, there exists $a \in A$ such that $\varphi(\sigma)\chi(\sigma) = a^{-1}\varphi(\sigma)a$ for each $\sigma \in \mathrm{Gal}(K_0)$. Hence, $\chi(\sigma) = \varphi(\sigma)^{-1}a^{-1}\varphi(\sigma)a = (a^{-1})^\sigma a$. Thus, χ is a coboundary, i.e. $x = 1$. Therefore, the action of $H^1(\mathrm{Gal}(K_0), A)$ on the set $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), \bar{G})$ is free, as claimed.

The proof of the local statement is similar. ∎

LEMMA 10.5: *Let $\mathfrak{p} \in \mathbb{P}_{\mathrm{nonarch}}(K_0)$, let $[\psi] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0),\bar{G})$, and let $x \in H^1(\mathrm{Gal}(K_0),A)$. Suppose that $[\psi]$ is unramified at $\mathfrak{p}$ and the element $\mathrm{res}_{\mathfrak{p}}(x)$ of $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}),A)$ is unramified. Then, $[\psi'] = [\psi]^x$ is unramified at $\mathfrak{p}$.* PHSc input, 232

Proof: By assumption, $\psi(\sigma) = 1$ for each $\sigma \in \hat{I}_{\mathfrak{p}}$. Let χ be a representative of x. Then, the restriction $\chi_{\mathfrak{p}}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to A$ of χ to $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ is a crossed homomorphism that represents $\mathrm{res}_{\mathfrak{p}}(x)$. By Subsection 7.4, we may assume that $\psi' = \psi \cdot \chi$. Since $\mathrm{res}_{\mathfrak{p}}(x)$ is unramified, $\mathrm{res}_{\mathfrak{p}}(x)|_{\hat{I}_{\mathfrak{p}}} = 1$, so there exists $a_{\mathfrak{p}} \in A$ such that $\chi_{\mathfrak{p}}(\sigma) = a_{\mathfrak{p}}^{\sigma} a_{\mathfrak{p}}^{-1}$ for all $\sigma \in \hat{I}_{\mathfrak{p}}$. Hence, by (2), we have for each $\sigma \in \hat{I}_{\mathfrak{p}}$ that $\psi'(\sigma) = \psi(\sigma) a_{\mathfrak{p}}^{\sigma} a_{\mathfrak{p}}^{-1} = a_{\mathfrak{p}}^{\sigma} a_{\mathfrak{p}}^{-1} = \psi(\sigma)^{-1} a_{\mathfrak{p}} \psi(\sigma) a_{\mathfrak{p}}^{-1} = a_{\mathfrak{p}} a_{\mathfrak{p}}^{-1} = 1$. Therefore, $[\psi']$ is unramified at $\mathfrak{p}$. ∎

The following local-global principle of Jürgen Neukirch plays a central role in the proof of our main result. It appears in the case where K is a number field as Lemma 4 on page 149 of [Neu79] and in the general case as Lemma 9.5.6 on page 565 of [NSW15]. We recapitulate the proof in the appendix to this paper (Lemma 15.8).

LEMMA 10.6: *Suppose under the assumptions of Subsection 10.1 that $A = \mathrm{Ker}(\alpha)$ is a simple $\mathrm{Gal}(K_0)$-module which is isomorphic to C_l^r, where $l \neq \mathrm{char}(K_0)$ is a prime number with $\zeta_l \notin K$. Then,* PHSd input, 278

$$\mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0),\bar{G}) \neq \emptyset \textit{ if and only if } \prod_{\mathfrak{p}} \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}),\bar{G}) \neq \emptyset.$$

11. Embedding Problems whose Kernel is a Simple $\mathrm{Gal}(K_0)$-Module

SIMP input, 13

We show in this section how to choose local conditions for our global embedding problem such that every weak solution of the problem is proper and the condition on the roots of unity in the solution field is preserved.

Setup 11.1: Again, we consider a finite Galois extension K of K_0 and an embedding problem SIMPa input, 19

(1) $$(\rho\colon \mathrm{Gal}(K_0) \to \Gamma,\ \bar{\alpha}\colon \bar{G} \to \Gamma),$$

where $\Gamma = \mathrm{Gal}(K/K_0)$, $\bar{G}$ is a finite group, $\bar{\alpha}$ is an epimorphism, and $\rho = \mathrm{res}_{K_{0,\mathrm{sep}}/K}$. Let $l \neq \mathrm{char}(K_0)$ be a prime number such that $\zeta_l \notin K$. Let $A = \mathrm{Ker}(\bar{\alpha})$ and assume that $A \cong C_l^r$ is a simple $\mathrm{Gal}(K_0)$-module under the action defined in Subsection 10.1. In particular, $\mathrm{Gal}(K)$ acts trivially on A.

We denote the finite group of roots of unity in K by $\mu(K)$. ∎

Recall that if $h\colon \mathrm{Gal}(K_0) \to A$ is a homomorphism and $\mathfrak{p} \in \mathbb{P}(K_0)$, then $h_{\mathfrak{p}}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to A$ is the restriction of h to $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ (Subsection 1.3).

Lemma 11.2: *Under Setup 11.1, let n be a positive integer with $\gcd(n, |\mu(K)|) = 1$ and $\mathrm{char}(K) \nmid n$, let m be the minimal number of generators of $\mathrm{Gal}(K(\zeta_n)/K)$, and let T be a finite set of primes of K_0. Then, there exist distinct non-archimedean primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q} \in \mathbb{P}(K_0) \smallsetminus T$ that totally split in K such that for each $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q}\}$ there exists $[\varphi_{\mathfrak{p}}] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), \bar{G})$ such that if an element $[\bar{\psi}] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), \bar{G})$ satisfies $[\bar{\psi}_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ in $\mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), \bar{G})$ for each $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q}\}$, then* SIMPb input, 46

(a) *$[\bar{\psi}]$ is unramified at $\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q}$,*

(b) *if $\bar{N}$ is the fixed field of $\mathrm{Ker}(\bar{\psi})$ in $K_{0,\mathrm{sep}}$, then $\gcd(n, |\mu(\bar{N})|) = 1$, and*

(c) *$\bar{\psi}$ is surjective.*

Proof: Although $\mathfrak{q}$ satisfies the same conditions as $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ in the lemma, $\mathfrak{q}$ plays a special role in the proof, namely to insure that $\bar{\psi}$ is surjective.

We break the proof into three parts.

Part A: *Choosing $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$.* Let $\sigma_1, \ldots, \sigma_m$ be generators of $\mathrm{Gal}(K(\zeta_n)/K)$. Then, we apply the Chebotarev density theorem and inductively choose non-archimedean primes

$$\mathfrak{Q}_1, \ldots, \mathfrak{Q}_m \in \mathbb{P}(K(\zeta_n)) \smallsetminus T_{K(\zeta_n)}$$

which are unramified over K_0 such that $\left[\frac{K(\zeta_n)/K}{\mathfrak{Q}_i}\right] = \sigma_i$ for $i = 1, \ldots, m$ and the primes

$$\mathfrak{p}_1 = \mathfrak{Q}_1|_{K_0}, \ldots, \mathfrak{p}_m = \mathfrak{Q}_m|_{K_0} \in \mathbb{P}(K_0) \smallsetminus T$$

are distinct. For each $i = 1, \ldots, m$ we set $\mathfrak{P}_i = \mathfrak{Q}_i|_K$. Then, $\left[\frac{K/K_0}{\mathfrak{P}_i}\right] = \sigma_i|_K = 1$, hence $K \subseteq \hat{K}_{0,\mathfrak{p}_i}$ (Subsection 1.5). Since $\mathrm{Gal}(K) = \mathrm{Ker}(\rho)$ (Subsection 10.1), it follows that the homomorphism $\rho_{\mathfrak{p}_i}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}_i}) \to \Gamma$ is trivial. Hence, setting

$\varphi_{\mathfrak{p}_i}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}_i}) \to \bar{G}$ to be the trivial homomorphism, we find that $[\varphi_{\mathfrak{p}_i}]$ is an element of $\mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}_i},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}_i}),\bar{G})$ for $i = 1,\dots,m$.

Part B: *Choosing* $\mathfrak{q}$. We apply the Chebotarev density theorem again in order to choose

$$\mathfrak{q} \in \mathbb{P}_{\mathrm{nonarch}}(K_0) \smallsetminus (T \cup \{\mathfrak{p}_1,\dots,\mathfrak{p}_m\})$$

which totally splits in K. By Lemma 7.4, $\rho_{\mathfrak{q}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{q}})) = \mathbf{1}$, in particular $\rho_{\mathfrak{q}}$ is unramified. Hence, by Lemma 8.1, there exists an unramified homomorphism $\varphi_{\mathfrak{q}}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{q}}) \to \bar{G}$ such that $\bar{\alpha}\circ\varphi_{\mathfrak{q}} = \rho_{\mathfrak{q}}$ (thus $[\varphi_{\mathfrak{q}}] \in \mathcal{H}_{\Gamma,\rho_{\mathfrak{q}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{q}}),\bar{G})$) and $A \cap \mathrm{Im}(\varphi_{\mathfrak{q}}) \neq \mathbf{1}$.

Part C: *Conclusion of the proof.* Let $\bar{\psi}$ be a weak solution of embedding problem (1) such that $[\bar{\psi}_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ for each $\mathfrak{p} \in \{\mathfrak{p}_1,\dots,\mathfrak{p}_m,\mathfrak{q}\}$.

Proof of (a): By Part A, for each $\mathfrak{p} \in \{\mathfrak{p}_1,\dots,\mathfrak{p}_m\}$, the homomorphism $\varphi_{\mathfrak{p}}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to \bar{G}$ is trivial, so $\varphi_{\mathfrak{p}}$ is unramified. Hence, $[\bar{\psi}]$ is unramified at $\mathfrak{p}$. Also, by Part B, $[\varphi_{\mathfrak{q}}]$ is unramified, hence $[\psi]$ is unramified at $\mathfrak{q}$.

Proof of (b): Since $\bar{\alpha}\circ\bar{\psi} = \rho$, we have $\mathrm{Ker}(\bar{\psi}) \le \mathrm{Ker}(\rho) = \mathrm{Gal}(K)$. Hence, the fixed field $\bar{N}$ of $\mathrm{Ker}(\bar{\psi})$ contains K, so $K \subseteq \bar{N}\cap K(\zeta_n)$. In addition, for each $i \in \{1,\dots,m\}$ we have $[\bar{\psi}_{\mathfrak{p}_i}] = [\varphi_{\mathfrak{p}_i}]$, that is $\bar{\psi}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}_i})) = \mathbf{1}$, so $\bar{N} \subseteq \hat{K}_{0,\mathfrak{p}_i}$. Hence, $\mathfrak{p}_i$ totally splits in $\bar{N}$ (Subsection 1.5), in particular $\mathfrak{p}_i$ totally splits also in $\bar{N}\cap K(\zeta_n)$. Therefore, with $\mathfrak{P}'_i$ being the prime of $\bar{N}\cap K(\zeta_n)$ that lies under $\mathfrak{Q}_i$, the automorphisms $\bar{\sigma}_i = \left[\frac{\bar{N}\cap K(\zeta_n)/K}{\mathfrak{P}'_i}\right]$, $i = 1,\dots,m$, which generate the Galois group $\mathrm{Gal}(\bar{N}\cap K(\zeta_n)/K)$, are all the identity maps (Subsection 1.5), so $\bar{N}\cap K(\zeta_n) = K$.

Now let $d = \gcd(n, |\mu(\bar{N})|)$. Then, $\zeta_d \in \bar{N}\cap K(\zeta_n) = K$, so d divides $\gcd(n,|\mu(K)|)$. By assumption, $\gcd(n,|\mu(K)|) = 1$, hence $d = 1$, as claimed.

Proof of (c): Since $[\bar{\psi}_{\mathfrak{q}}] = [\varphi_{\mathfrak{q}}]$, we have $\mathrm{Im}(\bar{\psi}_{\mathfrak{q}}) = \mathrm{Im}(\varphi_{\mathfrak{q}})$ (Subsection 7.4). Hence, $A\cap\mathrm{Im}(\varphi_{\mathfrak{q}}) = A\cap\mathrm{Im}(\bar{\psi}_{\mathfrak{q}}) \le A\cap\mathrm{Im}(\bar{\psi})$. By Part B, $A\cap\mathrm{Im}(\varphi_{\mathfrak{q}}) \neq \mathbf{1}$, hence the $\mathrm{Gal}(K_0)$-module $A\cap\mathrm{Im}(\bar{\psi})$ is non-trivial. Since A is a simple $\mathrm{Gal}(K_0)$-module, we obtain $A\cap\mathrm{Im}(\bar{\psi}) = A$. Since $\bar{\alpha}(\bar{\psi}(\mathrm{Gal}(K_0)) = \rho(\mathrm{Gal}(K_0)) = \Gamma$, we conclude from the exactness of (1) that $\bar{\psi}(\mathrm{Gal}(K_0)) = \bar{G}$, as claimed. ∎

12. Bounding the Ramification

BOUN input, 13

The preparations done in the previous sections lead now to the essential step toward the solution of our embedding problem. This is the case where the kernel of the problem is a simple $\mathrm{Gal}(K_0)$-module. We properly solve the problem with a bound on the ramification and such that the necessary conditions for the existence of a solution in the next step will hold.

Notation 12.1: Recall that for each positive integer n, one writes $\Omega(n)$ for the number of prime divisors of n, counted with multiplicity. Thus, if $n = \prod_{i=1}^{m} l_i^{r_i}$ with distinct prime numbers $l_1, \ldots, l_m$, then $\Omega(n) = \sum_{i=1}^{m} r_i$. In particular, $\Omega(nn') = \Omega(n) + \Omega(n')$ [HaW62, p. 354, Sec. 22.10]. ∎ BOUa input, 22

Setup 12.2: An extended embedding problem. As in Section 11, let K be a finite Galois extension of K_0. We set $\Gamma = \mathrm{Gal}(K/K_0)$ and let $\rho\colon \mathrm{Gal}(K_0) \to \Gamma$ be the restriction map. We also consider a prime number $l \neq \mathrm{char}(K_0)$ with $\zeta_l \notin K$. Then, we consider a diagram of profinite groups, BOUb input, 35

(1)
$$\begin{tikzcd} & & G \arrow[d, "\gamma"] & \mathrm{Gal}(K_0) \arrow[d, "\rho"] & \\ \mathbf{1} \arrow[r] & A \arrow[r] & \bar{G} \arrow[r, "\bar{\alpha}"] & \Gamma \arrow[r] & \mathbf{1}, \end{tikzcd}$$

with an exact short sequence. As in Setup 11.1, $A \cong C_l^r$ is a simple $\mathrm{Gal}(K_0)$-module under the action defined in Subsection 10.1, in particular $\mathrm{Gal}(K)$ acts trivially on A. In addition $\gamma\colon G \to \bar{G}$ is an epimorphism of finite groups. ∎

PROPOSITION 12.3: *Under Setup 12.2 let n be a positive integral multiple of $l \cdot |\mathrm{Ker}(\gamma)|$. Let T be a finite set of primes of K_0 that contains $\mathrm{Ram}(K/K_0)$. Suppose $\gcd(n, |\mu(K)|) = 1$, $\mathrm{char}(K_0) \nmid n$, and $\prod_{\mathfrak{p}} \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), \bar{G}) \neq \emptyset$. For each $\mathfrak{p} \in T$ we consider $[\varphi_{\mathfrak{p}}] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), \bar{G})$.* BOUd input, 65

Then, there exists a finite set $R \subseteq \mathbb{P}_{\mathrm{nonarch}}(K_0) \smallsetminus T$ with $|R| = \Omega(|A|) = r$, and there exists $[\bar{\psi}] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), \bar{G})_{\mathrm{sur}}$ such that

(a) *$[\bar{\psi}_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ in $\mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), \bar{G})$ for each $\mathfrak{p} \in T$,*

(b) $[\bar\psi]$ *is unramified at each* $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus (T \cup R)$*, so if* $\bar N$ *is the solution field of* $\bar\psi$ *(i.e. the fixed field of* $\mathrm{Ker}(\bar\psi)$*), then* $\mathrm{Ram}(\bar N/K_0) \subseteq T \cup R$*,*

(c) *for each* $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus T$ *we have* $\mathcal{H}\mathrm{om}_{\bar G, \bar\psi_\mathfrak{p}, \gamma}(\mathrm{Gal}(\hat K_{0,\mathfrak{p}}), G) \neq \emptyset$*, and*

(d) $\gcd(n, |\mu(\bar N)|) = 1$.

Proof: Let $\mathfrak{s}_1, \ldots, \mathfrak{s}_k$ be the elements of $S_{0,l}(K)|_{K_0} \smallsetminus T$. Since $\mathrm{Ram}(K/K_0) \subseteq T$, the primes $\mathfrak{s}_1, \ldots, \mathfrak{s}_k$ are unramified in K. Hence, by Lemma 8.1, for each $1 \leq i \leq k$, there exists an unramified homomorphism $\varphi_{\mathfrak{s}_i} \colon \mathrm{Gal}(\hat K_{0,\mathfrak{s}_i}) \to \bar G$ such that $\bar\alpha \circ \varphi_{\mathfrak{s}_i} = \rho_{\mathfrak{s}_i}$. Therefore,

(2) if an element $[\bar\psi] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar\alpha}(\mathrm{Gal}(K_0), \bar G)$ satisfies $[\bar\psi_\mathfrak{p}] = [\varphi_\mathfrak{p}]$ for each $\mathfrak{p} \in \{\mathfrak{s}_1, \ldots, \mathfrak{s}_k\}$, then $[\bar\psi]$ is unramified on $\{\mathfrak{s}_1, \ldots, \mathfrak{s}_k\}$.

Since $\mathbb{P}_{\mathrm{arch}}(K_0) \subseteq S_{0,l}(K)|_{K_0} \subseteq T \cup \{\mathfrak{s}_1, \ldots, \mathfrak{s}_k\}$,

(3) each $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus (T \cup \{\mathfrak{s}_1, \ldots, \mathfrak{s}_k\})$ is non-archimedean.

We break up the rest of the proof into four parts.

Part A: *The surjectivity and the number of roots of unity.* Let m be the minimal number of generators of $\mathrm{Gal}(K(\zeta_n)/K)$. We choose distinct $\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q} \in \mathbb{P}(K_0) \smallsetminus (T \cup \{\mathfrak{s}_1, \ldots, \mathfrak{s}_k\})$ and elements

$$[\varphi_\mathfrak{p}] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho_\mathfrak{p},\bar\alpha}(\mathrm{Gal}(\hat K_{0,\mathfrak{p}}), \bar G)$$

for $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q}\}$ that satisfy the conditions of Lemma 11.2. Thus, if $[\bar\psi] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar\alpha}(\mathrm{Gal}(K_0), \bar G)$ satisfies $[\bar\psi_\mathfrak{p}] = [\varphi_\mathfrak{p}]$ for each $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q}\}$, then

(4a) $[\bar\psi]$ is unramified at $\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q}$,

(4b) the fixed field $\bar N$ in $K_{0,\mathrm{sep}}$ of $\mathrm{Ker}(\bar\psi)$ satisfies $\gcd(n, |\mu(\bar N)|) = 1$, and

(4c) $[\bar\psi]$ is surjective.

Part B: *Strategy of the proof.* Since $\prod_\mathfrak{p} \mathcal{H}\mathrm{om}_{\Gamma,\rho_\mathfrak{p},\bar\alpha}(\mathrm{Gal}(\hat K_{0,\mathfrak{p}}), \bar G) \neq \emptyset$, there exists by Lemma 10.6, an element $[\psi_0] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar\alpha}(\mathrm{Gal}(K_0), \bar G)$. We are going to find $x \in H^1(\mathrm{Gal}(K_0), A)$ such that $[\bar\psi] = [\psi_0]^x$ satisfies the conclusions (a), (b), and (c) of the proposition.

To this end, let N_0 be the fixed field of $\mathrm{Ker}(\psi_0)$ in $K_{0,\mathrm{sep}}$. Then, $\rho(\mathrm{Gal}(N_0)) = \bar\alpha(\psi_0(\mathrm{Gal}(N_0)) = \mathbf{1}$, so $\mathrm{Gal}(N_0) \leq \mathrm{Ker}(\rho) = \mathrm{Gal}(K)$, hence $K \subseteq N_0$. Moreover

$\psi_0|_{\mathrm{Gal}(K)}$ induces an embedding

$$\psi_0'\colon \mathrm{Gal}(N_0/K) \to \bar{G}$$

such that $\bar{\alpha}(\psi_0'(\mathrm{Gal}(N_0/K)) = \mathbf{1}$, so $\mathrm{Gal}(N_0/K)$ is isomorphic to a subgroup of A, hence N_0/K is an abelian l-extension.

Part C: *The sets T^* and T^{**}.* We set $T^* = T \cup \{\mathfrak{s}_1, \dots, \mathfrak{s}_k\} \cup \{\mathfrak{p}_1, \dots, \mathfrak{p}_m, \mathfrak{q}\}$ and let $\mathfrak{r}_1, \dots, \mathfrak{r}_s$ be the primes that belong to $\mathbb{P}(K_0) \smallsetminus T^*$ at which ψ_0 ramifies. Then, we set $T^{**} = T^* \cup \{\mathfrak{r}_1, \dots, \mathfrak{r}_s\}$ and have that

(5) ψ_0 is unramified at each $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus T^{**}$.

Next observe that since $\mathrm{Ram}(K/K_0) \subseteq T \subseteq T^*$, each $\mathfrak{p} \in \{\mathfrak{r}_1, \dots, \mathfrak{r}_s\}$ is unramified in K, so

$$\rho_{\mathfrak{p}}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to \Gamma$$

is unramified (Subsection 7.4). Hence, by Lemma 8.1,

(6) there exists an unramified element $[\varphi_{\mathfrak{p}}] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), \bar{G})$.

Then, we consider the system $\big([\varphi_{\mathfrak{p}}] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), \bar{G})\big)_{\mathfrak{p}\in T^{**}}$. For each $\mathfrak{p} \in T^{**}$, Lemma 10.4 supplies a unique element $y_{\mathfrak{p}} \in H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ that satisfies

$$[\psi_{0,\mathfrak{p}}]^{y_{\mathfrak{p}}} = [\varphi_{\mathfrak{p}}]. \tag{7}$$

By Setup 12.2, A is a simple $\mathrm{Gal}(K_0)$-module on which $\mathrm{Gal}(K)$ acts trivially.

Since $T \subseteq T^*$ and $S_{0,l}(K)|_{K_0} \subseteq T^*$, we have $S_{0,l}(K)|_{K_0} \subseteq T^* \subseteq T^{**}$. Hence, the set T^{**}_K of all primes of K that lie over T^{**} contains $S_{0,l}(K)$. Also, $\mathrm{Ram}(K/K_0) \subseteq T \subseteq T^{**}$. By Setup 12.2, $\zeta_l \notin K$. Since N_0/K is an abelian l-extension (Part B), Proposition 9.3, applied to T^{**} rather than to T, yields an element $x \in H^1(\mathrm{Gal}(K_0), A)$ and primes $\mathfrak{q}_1, \dots, \mathfrak{q}_r \in \mathbb{P}(K_0) \smallsetminus T^{**}$ such that

(8a) $\mathrm{res}_{\mathfrak{p}}(x) = y_{\mathfrak{p}}$ for each $\mathfrak{p} \in T^{**}$,

(8b) $\mathrm{res}_{\mathfrak{p}}(x)$ is unramified at each $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus (T^{**} \cup \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\})$,

(8c) for $i = 1, \dots, r$, the prime $\mathfrak{q}_i$ totally splits in $N_0(\zeta_n)$ and $\mathrm{res}_{\mathfrak{q}_i}(x)\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \to A$ is a C_l-homomorphism, and

(8d) for $i = 1, \dots, r$ the homomorphism $\mathrm{res}_{\mathfrak{q}_i}(x)$ can be lifted to a $\bar{G}$-homomorphism $x'_{\mathfrak{q}_i}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{q}_i}) \to G$ (i.e. $\gamma \circ x'_{\mathfrak{q}_i} = \mathrm{res}_{\mathfrak{q}_i}(x)$).

Since $S_{0,l}(K) \subseteq T^{**}$, the primes $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ are non-archimedean (Subsection 1.6).

Part D: *The solution* $\bar\psi$. We consider the element $[\bar\psi] = [\psi_0]^x$ of $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar\alpha}(\mathrm{Gal}(K_0), \bar G)$.▮ For each $\mathfrak{p} \in T^{**}$ we have by (8a) and (7) that

$$[\bar\psi_{\mathfrak{p}}] = [\psi_{0,\mathfrak{p}}]^{\mathrm{res}_{\mathfrak{p}}(x)} = [\psi_{0,\mathfrak{p}}]^{y_{\mathfrak{p}}} = [\varphi_{\mathfrak{p}}] \tag{9}$$

in $\mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar\alpha}(\mathrm{Gal}(\hat K_{0,\mathfrak{p}}), \bar G)$. In particular, (9) holds for each $\mathfrak{p} \in T$, so Conclusion (a) of the proposition holds.

Also, by Part A, $[\bar\psi]$ satisfies Conditions (4a), (4b), and (4c). In particular, by (4b), $\gcd(n, |\mu(\bar N)|) = 1$. By (4c), $\bar\psi$ is an epimorphism. We prove that $\bar\psi$ also satisfies conclusions (b) and (c) of the proposition.

Proof of (b): We set $R = \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$. Let $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus (T \cup R)$. If $\mathfrak{p} \in \{\mathfrak{s}_1, \dots, \mathfrak{s}_k\} \cup \{\mathfrak{p}_1, \dots, \mathfrak{p}_m, \mathfrak{q}\}$, then by (9), $[\bar\psi_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$. Hence, by (2) and (4a), $[\bar\psi]$ is unramified at $\mathfrak{p}$. If $\mathfrak{p} \in \{\mathfrak{r}_1, \dots, \mathfrak{r}_s\}$, then by (6), $[\varphi_{\mathfrak{p}}]$ is unramified. Hence, by (9), $\bar\psi$ is unramified at $\mathfrak{p}$ (Subsection 7.4). Thus, $\bar\psi$ is unramified at each $\mathfrak{p} \in T^{**} \smallsetminus T$.

Finally if $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus (T^{**} \cup \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\})$, then by (5) and (8b), $[\psi_{0,\mathfrak{p}}]$ and $\mathrm{res}_{\mathfrak{p}}(x)$ are unramified. By (3), $\mathfrak{p}$ is non-archimedean. Hence, by Lemma 10.5, $[\bar\psi_{\mathfrak{p}}] = [\psi_{0,\mathfrak{p}}]^{\mathrm{res}_{\mathfrak{p}}(x)}$ is unramified. Thus, Condition (b) holds.

Proof of (c): Let $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus T$. If $\mathfrak{p} \notin R$, then by (b), $[\bar\psi_{\mathfrak{p}}]$ is unramified. Hence, by Lemma 8.1, $\bar\psi_{\mathfrak{p}}$ can be lifted to an unramified element of $\mathcal{H}\mathrm{om}_{\bar G,\bar\psi_{\mathfrak{p}},\gamma}(\mathrm{Gal}(\hat K_{0,\mathfrak{p}}), G)$. If $\mathfrak{p} \in R$, then by (8c), $\mathfrak{p}$ totally splits in $N_0(\zeta_n)$, hence also in N_0. Therefore, $\psi_{0,\mathfrak{p}}\colon \mathrm{Gal}(\hat K_{0,\mathfrak{p}}) \to \bar G$ is the trivial homomorphism (Subsection 7.4). Also, since $\mathfrak{p} = \mathfrak{q}_i$ for some $1 \le i \le r$, we have by (8c) that $\mathrm{res}_{\mathfrak{p}}(x)\colon \mathrm{Gal}(\hat K_{0,\mathfrak{p}}) \to A$ is a C_l-homomorphism, hence $\mathrm{res}_{\mathfrak{p}}(x)$ represents its own cohomology class. Therefore, $[\bar\psi_{\mathfrak{p}}] = [\psi_{0,\mathfrak{p}}]^{\mathrm{res}_{\mathfrak{p}}(x)} = [\psi_{0,\mathfrak{p}} \cdot \mathrm{res}_{\mathfrak{p}}(x)] = [\mathrm{res}_{\mathfrak{p}}(x)]$.

By (8d), $\mathrm{res}_{\mathfrak{p}}(x)$ can be lifted to a $\bar G$-homomorphism $x'_{\mathfrak{p}}$. Hence, also $\bar\psi_{\mathfrak{p}}$ has the same property. This implies that $\mathcal{H}\mathrm{om}_{\bar G,\bar\psi_{\mathfrak{p}},\gamma}(\mathrm{Gal}(\hat K_{0,\mathfrak{p}}), G) \neq \emptyset$, as (c) states. ■

13. Embedding Problems with Solvable Kernel

SOLV input, 12

Following Proposition 12.3, we now prove the main result of this work by induction on the order of the kernel of the given embedding problem.

Construction 13.1: We wish to solve a finite embedding problem SOLa input, 17

$$(1)\qquad (\rho\colon \mathrm{Gal}(K_0) \to \Gamma,\ \alpha\colon G \to \Gamma),$$

where $H = \mathrm{Ker}(\alpha)$ is a solvable group and $\mathrm{char}(K_0) \nmid |H|$. Without loss we may assume that $H \neq \mathbf{1}$. For each weak solution $\varphi\colon \mathrm{Gal}(K_0) \to G$ of (1) and every $a \in H$, we let $\varphi^a\colon \mathrm{Gal}(K_0) \to G$ be the homomorphism defined for each $\sigma \in \mathrm{Gal}(K_0)$ by $\varphi^a(\sigma) = a^{-1}\varphi(\sigma)a$. Thus, φ and φ^a are $\mathrm{Ker}(\alpha)$-conjugate.

Since H is solvable, it has a normal subgroup H_1 such that H/H_1 is a non-trivial abelian group. As in Remark 4.1, the subgroup $\bigcap_{g\in G} H_1^g$ of G is normal, contained in H, and $H/\bigcap_{g\in G} H_1^g$ is abelian. Therefore, replacing H_1 by $\bigcap_{g\in G} H_1^g$, we may assume that H_1 is normal in G. Furthermore, replacing H_1 by a larger subgroup of H, we may assume that H_1 is a maximal subgroup of H with the property that H_1 is normal in G and H/H_1 is non-trivial and abelian. As in Subsection 10.1, H/H_1 becomes a simple $\mathrm{Gal}(K_0)$-module via ρ. Thus, there exist a prime number l_1 and a positive integer r_1 such that $H/H_1 \cong C_{l_1}^{r_1}$. In particular $l_1|H_1|$ divides $|H|$ and $\mathrm{char}(K_0) \neq l_1$. Moreover, we have the commutative diagram

(2)
$$\begin{tikzcd}
 & H_1 \arrow[r, equal] \arrow[d] & H_1 \arrow[d] & \mathrm{Gal}(K_0) \arrow[d, "\rho"] & \\
\mathbf{1} \arrow[r] & H \arrow[r] \arrow[d, "\pi"] & G \arrow[r, "\alpha"] \arrow[d, "\pi"] & \Gamma \arrow[r] \arrow[d, equal] & \mathbf{1} \\
\mathbf{1} \arrow[r] & H/H_1 \arrow[r] & G/H_1 \arrow[r, "\bar{\alpha}"] & \Gamma \arrow[r] & \mathbf{1}
\end{tikzcd}$$

with exact horizontal sequences such that both maps π are quotient maps. ∎

Strategy 13.2: Note that $|H| = |H/H_1| \cdot |H_1|$. Hence, by Notation 12.1, SOLb input, 77

$$\Omega(|H|) = \Omega(|H/H_1|) + \Omega(|H_1|).$$

Using Proposition 12.3, we first find a proper solution ψ_1 for the lower Embedding problem in (2) with the accompanying conditions. Then, we apply induction on the order of the kernel to find a proper solution ψ to the embedding problem (ψ_1: $\mathrm{Gal}(K_0) \to G/H_1$, π: $G \to G/H_1$), that satisfies the accompanying conditions. Finally, we prove that ψ is the desired solution of Embedding problem (1). ∎

SOLc input, 96

THEOREM 13.3: *Let K/K_0 be a finite Galois extension of global fields and consider the finite embedding problem (1) with the solvable kernel H, where $\Gamma = \mathrm{Gal}(K/K_0)$ and $\rho = \mathrm{res}_{K_{0,\mathrm{sep}}/K}$. Let T be a finite set of primes of K_0 that contains $\mathrm{Ram}(K/K_0)$. Suppose that $\mathrm{char}(K_0) \nmid |H|$, $\gcd(|H|, |\mu(K)|) = 1$, and $\prod_{\mathfrak{p}} \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G) \neq \emptyset$ (notation of Subsection 7.3). For each $\mathfrak{p} \in T$ let $[\varphi_{\mathfrak{p}}] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$.*

Then, there exists an element $[\psi] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho,\alpha}(\mathrm{Gal}(K_0), G)_{\mathrm{sur}}$ and there exists a set

$$R \subseteq \mathbb{P}_{\mathrm{nonarch}}(K_0) \smallsetminus T$$

with $|R| = \Omega(|H|)$ such that

(a) $[\psi_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ *in* $\mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$ *for each* $\mathfrak{p} \in T$ *and*

(b) $[\psi]$ *is unramified at each* $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus (T \cup R)$*, that is the fixed field N of* $\mathrm{Ker}(\psi)$ *in* $K_{0,\mathrm{sep}}$ *satisfies* $\mathrm{Ram}(N/K_0) \subseteq T \cup R$.

Proof: Let H_1 be the normal subgroup of G contained in H with H/H_1 being a simple $\mathrm{Gal}(K_0)$-module (Construction 13.1). We break up the rest of the proof into three parts.

PART A: *An embedding problem whose kernel is a simple* $\mathrm{Gal}(K_0)$*-module.* We consider Diagram (2). If $\mathfrak{p} \in \mathbb{P}(K_0)$ and $[\eta_{\mathfrak{p}}] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$, then $[\pi \circ \eta_{\mathfrak{p}}] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G/H_1)$. Hence, $\prod_{\mathfrak{p}} \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G/H_1) \neq \emptyset$. For each $\mathfrak{p} \in T$ we have that

$$\bar{\varphi}_{\mathfrak{p}} = \pi \circ \varphi_{\mathfrak{p}} \in \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G/H_1).$$

Since $H/H_1 \cong C_{l_1}^{r_1}$ is a simple $\mathrm{Gal}(K_0)$-module, $|H|$ is a multiple of $l_1|H_1|$ (Construction 13.1), $\mathrm{char}(K_0) \nmid |H|$, and $\gcd(|H|, |\mu(K)|) = 1$, Proposition 12.3 with $n = |H|$ provides a finite set $T_1 \subseteq \mathbb{P}_{\mathrm{nonarch}}(K_0) \smallsetminus T$ with $|T_1| = \Omega(|H/H_1|)$ and an element

(3) $[\psi_1] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho,\bar{\alpha}}(\mathrm{Gal}(K_0), G/H_1)_{\mathrm{sur}}$ such that

(4a) $[\psi_{1,\mathfrak{p}}] = [\bar{\varphi}_{\mathfrak{p}}]$ in $\mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\bar{\alpha}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G/H_1)$ for each $\mathfrak{p} \in T$,

(4b) $[\psi_1]$ is unramified at each $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus (T \mathbin{\dot\cup} T_1)$, so if N_1 is the fixed field of $\mathrm{Ker}(\psi_1)$, then $\mathrm{Ram}(N_1/K_0) \subseteq T \mathbin{\dot\cup} T_1$,

(4c) for each $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus T$ we have $\mathcal{H}\mathrm{om}_{G/H_1,\psi_{1,\mathfrak{p}},\pi}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G) \neq \emptyset$, and

(4d) $\gcd(|H|, |\mu(N_1)|) = 1$.

Part B: *The induction step.* This gives rise to an embedding problem

$$(5) \qquad (\psi_1\colon \mathrm{Gal}(K_0) \to G/H_1,\ \pi\colon G \to G/H_1)$$

with a finite solvable kernel H_1.

For each $\mathfrak{p} \in T$ there exists, by (4a), an element $a_{\mathfrak{p}} \in H$ such that for each $\sigma \in \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$

$$\psi_{1,\mathfrak{p}}(\sigma) = \pi(a_{\mathfrak{p}})^{-1}\bar{\varphi}_{\mathfrak{p}}(\sigma)\pi(a_{\mathfrak{p}}) = \pi(a_{\mathfrak{p}}^{-1})\pi(\varphi_{\mathfrak{p}}(\sigma))\pi(a_{\mathfrak{p}}) = \pi(a_{\mathfrak{p}}^{-1}\varphi_{\mathfrak{p}}(\sigma)a_{\mathfrak{p}}) = (\pi \circ \varphi_{\mathfrak{p}}^{a_{\mathfrak{p}}})(\sigma),$$

(6) so $[\varphi_{\mathfrak{p}}^{a_{\mathfrak{p}}}] \in \mathcal{H}\mathrm{om}_{G/H_1,\psi_{1,\mathfrak{p}},\pi}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$ for every $\mathfrak{p} \in T$.

It follows from (4c) and (6) that $\prod_{\mathfrak{p}} \mathcal{H}\mathrm{om}_{G/H_1,\psi_{1,\mathfrak{p}},\pi}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G) \neq \emptyset$. Moreover, $\mathrm{char}(K_0) \nmid |H_1|$ and (4d) implies that $\gcd(|H_1|, |\mu(N_1)|) = 1$.

For each $\mathfrak{p} \in T$ we set $\varphi_{1,\mathfrak{p}} = \varphi_{\mathfrak{p}}^{a_{\mathfrak{p}}}$. Then, for each $\mathfrak{p} \in T_1$ we use (4c) to choose $[\varphi_{1,\mathfrak{p}}] \in \mathcal{H}\mathrm{om}_{G/H_1,\psi_{1,\mathfrak{p}},\pi}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$.

Since H_1 is solvable and $|H_1| < |H|$, an induction hypothesis on the order of the kernel of the embedding problem gives a set $R_1 \subseteq \mathbb{P}_{\mathrm{nonarch}}(K_0) \smallsetminus (T \mathbin{\dot\cup} T_1)$ and an element

(7) $[\psi] \in \mathcal{H}_{G/H_1,\psi_1,\pi}(\mathrm{Gal}(K_0), G)_{\mathrm{sur}}$

such that $|R_1| = \Omega(|H_1|)$ and

(8a) $[\psi_{\mathfrak{p}}] = [\varphi_{1,\mathfrak{p}}]$ in $\mathcal{H}\mathrm{om}_{G/H_1,\psi_{1,\mathfrak{p}},\pi}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$, for each $\mathfrak{p} \in T \mathbin{\dot\cup} T_1$,

(8b) $[\psi]$ is unramified at each $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus (T \mathbin{\dot\cup} T_1 \mathbin{\dot\cup} R_1)$, that is if N is the solution field of embedding problem (5), then $\mathrm{Ram}(N/K_0) \subseteq T \mathbin{\dot\cup} T_1 \mathbin{\dot\cup} R_1$.

We set $R = T_1 \mathbin{\dot\cup} R_1$. Then, by Notation 12.1, $|R| = |T_1| + |R_1| = \Omega(|H/H_1|) + \Omega(|H_1|) = \Omega(|H|)$.

Part C: *Conclusion of the proof.* We prove that $[\psi]$ satisfies the conclusion of the theorem. Indeed, by (2), (7), and (3) we have $\alpha\circ\psi=\bar\alpha\circ\pi\circ\psi=\bar\alpha\circ\psi_1=\rho$, so $[\psi]\in\mathcal{H}\mathrm{om}_{\Gamma,\rho,\alpha}(\mathrm{Gal}(K_0),G)_{\mathrm{sur}}$.

$$\begin{tikzcd}
 & & \mathbf{1} \arrow[d] & & \\
 & & H_1 \arrow[d] & \mathrm{Gal}(K_0) \arrow[dl, "\psi"'] \arrow[ddl, "\psi_1"] \arrow[dd, "\rho"] & \\
\mathbf{1} \arrow[r] & H \arrow[r] \arrow[d] & G \arrow[d, "\pi"'] \arrow[dr, "\alpha"] & & \\
1 \arrow[r] & H/H_1 \arrow[r] & G/H_1 \arrow[r, "\bar\alpha"] \arrow[d] & \Gamma \arrow[r] & \mathbf{1} \\
 & & \mathbf{1}. & &
\end{tikzcd}$$

Moreover, by (8a), for each $\mathfrak{p}\in T$ there exists $b_\mathfrak{p}\in H_1$ such that for each $\sigma\in\mathrm{Gal}(\hat K_{0,\mathfrak{p}})$ we have $\psi_\mathfrak{p}(\sigma)=b_\mathfrak{p}^{-1}\varphi_{1,\mathfrak{p}}(\sigma)b_\mathfrak{p}=b_\mathfrak{p}^{-1}a_\mathfrak{p}^{-1}\varphi_\mathfrak{p}(\sigma)a_\mathfrak{p}b_\mathfrak{p}=(a_\mathfrak{p}b_\mathfrak{p})^{-1}\varphi_\mathfrak{p}(\sigma)(a_\mathfrak{p}b_\mathfrak{p})$. Since $a_\mathfrak{p}\in H$ and $b_\mathfrak{p}\in H_1$, we have $a_\mathfrak{p}b_\mathfrak{p}\in H$. Therefore, $[\psi_\mathfrak{p}]=[\varphi_\mathfrak{p}]$ in $\mathcal{H}\mathrm{om}_{\Gamma,\rho_\mathfrak{p},\alpha}(\mathrm{Gal}(\hat K_{0,\mathfrak{p}}),G)$ for each $\mathfrak{p}\in T$, as desired. ∎

14. Embedding Problems with Solvable Kernel in $K_{0,\mathrm{tot},S}$

APPL
input, 12

In this section we provide some applications of the main theorem of this work. We consider our basic global field K_0 and let S be a finite set of primes of K_0. Then, $K_{0,\mathrm{tot},S}$ denotes the union of all finite Galois extensions of K_0 in which each $\mathfrak{p}\in S$ totally splits. Thus,

$$K_{0,\mathrm{tot},S}=\bigcap_{\mathfrak{p}\in S}\bigcap_{\tau\in\mathrm{Gal}(K_0)}K_{0,\mathfrak{p}}^{\tau}. \tag{1}$$

The field $K_{0,\mathrm{tot},S}$ has several distinguished properties. First of all $K_{0,\mathrm{tot},S}$ is $\mathbf{P}S\mathbf{C}$. That is, if V is an absolutely integral variety over $K_{0,\mathrm{tot},S}$ with a simple $K_{0,\mathfrak{p}}^{\tau}$-rational point for each $\mathfrak{p}\in S$ and $\tau\in\mathrm{Gal}(K_0)$, then V has a $K_{0,\mathrm{tot},S}$-rational point [Jar11, p. 75, Example 5.6.5 (with citation to original works)]. In particular, $K_{0,\mathrm{tot},S}$ is **ample** [Jar11,

p. 67, Lemma 5.3.1]. The latter implies among other things that if t is a transcendental element over $K_{0,\mathrm{tot},S}$, then every finite group occurs as a Galois group over $K_{0,\mathrm{tot},S}(t)$ [a consequence of Jar11, p. 88, Thm. 5.9.2]. Finally, by [Pop96, p. 3, Thm. 3], $\mathrm{Gal}(K_{0,\mathrm{tot},S})$ is a "free product of groups of the form $\mathrm{Gal}(K_{0,\mathfrak{p}}^{\tau})$ in the sense of Melnikov and Haran with $\mathfrak{p}$ and τ as above".

Setup 14.1: Again, with K_0 and S as above, we let K be a finite Galois extension of our global field K_0 and set $\Gamma = \mathrm{Gal}(K/K_0)$ and $\rho = \mathrm{res}_{K_{0,\mathrm{sep}}/K}$. Then we consider a finite embedding problem SETP input, 44

$$(2) \qquad (\rho\colon \mathrm{Gal}(K_0) \to \Gamma,\ \alpha\colon G \to \Gamma),$$

where $H = \mathrm{Ker}(\alpha)$ is a solvable group. ▮

For each prime number p we write $\mathbb{Q}_{\mathrm{tot},p}$ rather than $\mathbb{Q}_{\mathrm{tot},\{p\}}$. The thesis [Ram13] conjectures that every finite group that occurs as a Galois group over $\mathbb{Q}$ is a quotient of $\mathrm{Gal}(\mathbb{Q}_{\mathrm{tot},p}/\mathbb{Q})$. The conjecture is verified in [Ram13] for finite abelian groups, symmetric groups, and alternating groups.

In this section we go even further as far as solvable groups are concerned. We use Theorem 13.3 to solve Embedding problem (2) with local data and bounded ramification in $K_{0,\mathrm{tot},S}$ once the kernel H is solvable, $\gcd(|H|, |\mu(K)|) = 1$, $\mathrm{char}(K_0) \nmid |H|$, $K \subseteq K_{0,\mathrm{tot},S}$, and each of the corresponding local embedding problems is solvable.

Remark 14.2: Let K_0 and S be as above. If S' is a subset of $\mathbb{P}(K_0)$ that contains S, then by Definition (1), $K_{0,\mathrm{tot},S'} \subseteq K_{0,\mathrm{tot},S}$. CNGa input, 76

Now, consider the set S_K of all primes of K that lie over S. For each $\mathfrak{p} \in S$ we choose $\mathfrak{P}_{\mathfrak{p}} \in S_K$ that lies over $\mathfrak{p}$ such that $K_{0,\mathfrak{p}} \subseteq K_{\mathfrak{P}_{\mathfrak{p}}}$ (Subsection 1.4). Then, $K_{0,\mathrm{tot},S} = \bigcap_{\mathfrak{p}\in S} \bigcap_{\tau\in\mathrm{Gal}(K_0)} K_{0,\mathfrak{p}}^{\tau} \subseteq \bigcap_{\mathfrak{P}\in S_K} \bigcap_{\tau\in\mathrm{Gal}(K)} K_{\mathfrak{P}}^{\tau} = K_{\mathrm{tot},S_K}$. ▮

THEOREM 14.3: *Under Setup 14.1 we assume that* $K \subseteq K_{0,\mathrm{tot},S}$. *Suppose that* $\gcd(|H|, |\mu(K)|) =$ ABEPa input, 98 1, $\mathrm{char}(K_0) \nmid |H|$, *and* $\prod_{\mathfrak{p}} \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G) \neq \emptyset$. *Let* $T \subseteq \mathbb{P}(K_0) \smallsetminus S$ *be a finite set such that* $\mathrm{Ram}(K/K_0) \subseteq T$. *For each* $\mathfrak{p} \in T$ *we consider* $[\varphi_{\mathfrak{p}}] \in \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$.

Then, there exists a proper solution ψ *of Embedding problem (2) and there exists a finite set* $R \subseteq \mathbb{P}_{\mathrm{nonarch}}(K_0) \smallsetminus (S \cup T)$ *with* $|R| = \Omega(|H|)$ *such that if we denote*

$\psi_{\mathfrak{p}} = \psi|_{\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})}$, *then*

(a) $[\psi_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ *for each* $\mathfrak{p} \in T$,

(b) *the fixed field* N *of* $\mathrm{Ker}(\psi)$ *satisfies* $N \subseteq K_{0,\mathrm{tot},S}$, *and*

(c) $\mathrm{Ram}(N/K_0) \subseteq R \cup T$, *so* $|\mathrm{Ram}(N/K_0)| \leq \Omega(|H|) + |T|$.

Proof: Since $K \subseteq K_{0,\mathrm{tot},S}$, each $\mathfrak{p} \in S$ totally splits in K, in particular $\mathfrak{p}$ is unramified in K (if $\mathfrak{p}$ is non-archimedean) and $\rho_{\mathfrak{p}}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to \Gamma$ is the trivial homomorphism (Subsection 7.4). Hence, the $\mathrm{Ker}(\alpha)$-conjugacy class $[\varphi_{\mathfrak{p}}]$ of the trivial homomorphism $\varphi_{\mathfrak{p}}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to G$ is an element of $\mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$.

By Theorem 13.3 applied to $S \cup T$ rather than to T, there exists a proper solution ψ of Embedding problem (2) and there exists a set $R \subseteq \mathbb{P}_{\mathrm{nonarch}}(K_0) \smallsetminus (S \cup T)$ with $|R| = \Omega(|H|)$ such that

(3a) $[\psi_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$ for each $\mathfrak{p} \in S \cup T$ and

(3b) the solution field N of ψ satisfies $\mathrm{Ram}(N/K_0) \subseteq R \cup S \cup T$.

In particular, (3a) implies (a). Also, for each $\mathfrak{p} \in S$ we have $[\psi_{\mathfrak{p}}] = [\varphi_{\mathfrak{p}}]$. Since $\varphi_{\mathfrak{p}}$ is the trivial homomorphism, so is $\psi_{\mathfrak{p}}$ (Subsection 7.4). Hence, since $\mathrm{Gal}(N) = \mathrm{Ker}(\psi)$, each $\mathfrak{p} \in S$ totally splits in N (Subsection 7.4). Therefore $N \subseteq K_{0,\mathrm{tot},S}$, as (b) claims.

Finally, each non-archimedean $\mathfrak{p} \in S$ is unramified in N. It follows from (3b) that $\mathrm{Ram}(N/K_0) \subseteq R \cup T$, as asserted by (c). ∎

COROLLARY 14.4: *Let* S *be a finite subset of* $\mathbb{P}(K_0)$ *and let* G *be a finite solvable group with* APPb input, 171

$$\gcd(|G|, |\mu(K_0)|) = 1 \text{ and } \mathrm{char}(K_0) \nmid |G|.$$

Then, K_0 *has a Galois extension* N *in* $K_{0,\mathrm{tot},S}$ *and there exists a finite set* $R \subseteq \mathbb{P}_{\mathrm{nonarch}}(K_0) \smallsetminus S$ *with* $|R| = \Omega(|G|)$ *such that* $\mathrm{Gal}(N/K_0) \cong G$, $\mathrm{Ram}(N/K_0) \subseteq R$, *and* $|\mathrm{Ram}(N/K_0)| \leq \Omega(|G|)$.

Proof: We let Γ in (2) be the trivial group and let both ρ, α be the trivial homomorphisms. Then, $H = \mathrm{Ker}(\alpha) = G$. Moreover, for each $\mathfrak{p} \in \mathbb{P}(K_0)$ the $\mathrm{Ker}(\alpha)$-conjugacy class of the trivial homomorphism $\varphi_{\mathfrak{p}}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to G$ is an element of $\mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G)$. We set $K = K_0$ and let T be the empty set. Then, by Theorem 14.3, K_0 has a Galois extension N in $K_{0,\mathrm{tot},S}$ and there exists a finite set $R \subseteq$

$\mathbb{P}_{\mathrm{nonarch}}(K_0) \smallsetminus S$ with $|R| \le \Omega(|G|)$ such that $\mathrm{Gal}(N/K_0) \cong G$, and $\mathrm{Ram}(N/K_0) \subseteq R$. Thus, $|\mathrm{Ram}(N/K_0)| \le \Omega(|G|)$. ∎

COROLLARY 14.5: *Suppose that K_0 is a number field, let S be a finite subset of $\mathbb{P}(K_0)$, and let G be a finite group of odd order. Then, K_0 has a Galois extension N in $K_{0,\mathrm{tot},S}$ such that* $\mathrm{Gal}(N/K_0) \cong G$ *and* $|\mathrm{Ram}(N/K_0)| \le [K_0 : \mathbb{Q}] \cdot \Omega(|G|)$. APPc input, 208

Proof: By the celebrated theorem of Feit and Thompson [FeT63], G is solvable. Since $\mu(\mathbb{Q}) = \{1, -1\}$, we have $|\mu(\mathbb{Q})| = 2$, hence $\gcd(|G|, |\mu(\mathbb{Q})|) = 1$. By Corollary 14.4 applied to $\mathbb{Q}$ and $S|_{\mathbb{Q}}$ (Subsection 1.4) rather than to K_0 and S, there exists a Galois extension N_0 of $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{tot},S|_{\mathbb{Q}}\cup\mathrm{Ram}(K_0/\mathbb{Q})}$ with $\mathrm{Gal}(N_0/\mathbb{Q}) \cong G$ and there exists a finite set $R \in \mathbb{P}_{\mathrm{nonarch}}(\mathbb{Q}) \smallsetminus (S|_{\mathbb{Q}} \cup \mathrm{Ram}(K_0/\mathbb{Q}))$ with $|R| = \Omega(|G|)$ such that $\mathrm{Ram}(N_0/\mathbb{Q}) \subseteq R$. Let $N = K_0N_0$. Then, if $\mathfrak{p} \in \mathbb{P}_{\mathrm{nonarch}}(K_0)$ and the prime number p that lies under $\mathfrak{p}$ is unramified in N_0, then $\mathfrak{p}$ is unramified in N. Since over each prime number there lie at most $[K_0 : \mathbb{Q}]$ primes of K_0, we conclude from $\mathrm{Ram}(N/K_0) \subseteq R_{K_0}$ (Subsection 1.4) that $|\mathrm{Ram}(N/K_0)| \le [K_0 : \mathbb{Q}] \cdot |R| \le [K_0 : \mathbb{Q}] \cdot \Omega(|G|)$, as claimed.

Moreover, $\mathrm{Ram}(K_0 \cap N_0/\mathbb{Q}) \subseteq \mathrm{Ram}(K_0/\mathbb{Q}) \cap \mathrm{Ram}(N_0/\mathbb{Q}) \subseteq \mathrm{Ram}(K_0/\mathbb{Q}) \cap R = \emptyset$. Thus, $K_0 \cap N_0$ is an unramified extension of $\mathbb{Q}$. By a corollary to a theorem of Hermite-Minkowski, $K_0 \cap N_0 = \mathbb{Q}$ [Neu99, p. 207, Thm. 2.18]. Therefore, the Galois extension $N = K_0N_0$ of K_0 satisfies $\mathrm{Gal}(N_0/K_0) \cong G$. Moreover, since $S \subseteq (S|_{\mathbb{Q}})_{K_0}$, it follows from Remark 14.2 that $\mathbb{Q}_{\mathrm{tot},S|_{\mathbb{Q}}\cup\mathrm{Ram}(K_0/\mathbb{Q})} \subseteq \mathbb{Q}_{\mathrm{tot},S|_{\mathbb{Q}}} \subseteq K_{0,\mathrm{tot},(S|_{\mathbb{Q}})_{K_0}} \subseteq K_{0,\mathrm{tot},S}$. Hence, by the preceding paragraph, $N = K_0N_0 \subseteq K_{0,\mathrm{tot},S}$. ∎

Remark 14.6: The interest in Corollary 14.5 lies in the fact that in contrast to previous results of this work, we impose the condition $\gcd(|G|, 2) = 1$ on G, rather than the stronger condition $\gcd(|G|, |\mu(K_0)|) = 1$. Of course, this comes with a price, namely the usual upper bound $\Omega(|G|)$ for the number of ramified primes of the extension must now be multiplied by $[K_0 : \mathbb{Q}]$. Nevertheless, the latter factor is independent of G. ∎ APPd input, 262

COROLLARY 14.7: *Under Setup 14.1 we assume that* $K \subseteq K_{0,\mathrm{tot},S}$, $\mathrm{char}(K_0) \nmid |H|$ *and* $\gcd(|H|, |\mu(K)|) = 1$. *In addition, we assume that one of the following conditions holds:* APPe input, 273

(a) α **splits**, *that is there exists a homomorphism* $\alpha' \colon \Gamma \to G$ *such that* $\alpha \circ \alpha' = \mathrm{id}_\Gamma$.

(b) *Embedding problem (3) has a weak solution.*

Then, Embedding problem (3) has a proper solution with a solution field N in $K_{0,\mathrm{tot},S}$ such that $|\mathrm{Ram}(N/K_0)| \le |\mathrm{Ram}(K/K_0)| + \Omega(|H|)$.

Proof: First note that Condition (a) of the Corollary implies Condition (b). If ψ is a weak solution of (3), then for each $\mathfrak{p} \in \mathbb{P}(K_0)$ the homomorphism $\psi_\mathfrak{p}\colon \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \to G$ satisfies $\alpha \circ \psi_\mathfrak{p} = \rho_\mathfrak{p}$. Hence, by Theorem 14.3, with $T = \mathrm{Ram}(K/K_0)$, the field K_0 has a Galois extension N in $K_{0,\mathrm{tot},S}$ as asserted by the corollary. ∎

Recall that a finite extension N/K of number fields is **tame** if every prime divisor of K is tamely ramified in N. In his survey paper [Bir94], Bryan Birch asks whether for each finite group G there exists a tame Galois extension L of $\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) = G$. Among others, he suspects that this is the case for each finite solvable group. Our last application of 14.3 is a contribution to Birch's problem.

COROLLARY 14.8: *Let K be a number field, G a finite solvable group, and S a finite set* APPf input, 316
of primes of K that contain all prime divisors of $|G|$. Suppose that $\gcd(|G|, |\mu(K)|) = 1$. *Then, K has a tame Galois extension N in $K_{\mathrm{tot},S}$ with* $\mathrm{Gal}(N/K) \cong G$ *and* $|\mathrm{Ram}(N/K)| \le \Omega(|G|)$.

Proof: We consider the embedding problem $\mathbf{1} \longrightarrow G \to G \xrightarrow{\alpha} \mathbf{1} \longrightarrow \mathbf{1}$, where α is the trivial map. Without loss we enlarge S to include all primes of K that divide $|G|$. By Theorem 14.3 with $K_0 = K$ and $T = \emptyset$, the field K has a Galois extension N with Galois group G and there exists a set $R \subseteq \mathbb{P}(K) \smallsetminus S$ with $|R| = \Omega(|G|)$ such that $\mathrm{Ram}(N/K) \subseteq R$. In particular no $\mathfrak{P} \in \mathbb{P}(K)$ over R divides the order of G. Hence, N/K is a tame extension, as claimed. ∎

15. Appendix

APND input, 12

For the convenience of the readers, in this appendix we prove a few results about the pairing of cohomology groups attached to global and local fields, originally proved in [Neu79] for number fields.

Remark 15.1: Perfect pairing. Let l be a prime number and let G and G' be locally compact abelian multiplicative groups of exponent l. Suppose $\omega\colon G \times G' \to \mu_l$ is a non-degenerate bilinear map (also called a **perfect pairing** in [NSW00]). To each $\sigma \in G$ we attach the homomorphism $\chi_\sigma\colon G' \to \mu_l$ defined by $\chi_\sigma(\sigma') = \omega(\sigma, \sigma')$. Similarly, to each $\sigma' \in G'$ we attach the homomorphism $\chi'_{\sigma'}\colon G \to \mu_l$ defined by $\chi'_{\sigma'}(\sigma) = \omega(\sigma, \sigma')$. Note that since $\sigma^l = 1$ and $(\sigma')^l = 1$ for all $\sigma \in G$ and $\sigma' \in G'$, we can actually identify the group of homomorphisms of G (resp. G', resp. $G \times G'$) into the unit circle $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ with the corresponding groups of homomorphisms into μ_l. We may therefore replace μ_l throughout by $\mathbb{T}$ in order to cite the results of [Pon46]. In particular, by the Pontryagin duality theorem [Pon46, p. 134, Thm. 32], for each homomorphism $\chi\colon G \to \mu_l$ (resp. $\chi'\colon G' \to \mu_l$) there exists a unique $\sigma' \in G'$ (resp. $\sigma \in G$) such that $\chi = \chi'_{\sigma'}$ (resp. $\chi' = \chi_\sigma$). PONt input, 20

Next recall that for each closed subgroup H of G the **orthogonal complement** of H is defined as $H^\perp = \{\sigma' \in G' \mid \omega(\eta, \sigma') = 1 \text{ for all } \eta \in H\}$. Similarly, for each closed subgroup H' of G' we let $(H')^\perp = \{\sigma \in G \mid \omega(\sigma, \eta') = 1 \text{ for all } \eta' \in H'\}$.

If H_1 and H_2 are closed subgroups of G, then the bilinearity of ω implies that $(H_1H_2)^\perp = H_1^\perp \cap H_2^\perp$. Similarly, if H_1' and H_2' are closed subgroups of G', then $(H_1'H_2')^\perp = (H_1')^\perp \cap (H_2')^\perp$.

Less obvious, but still true, is the relation $(H^\perp)^\perp = H$ for each closed subgroup of G (resp. of G') [Pon46, p. 136, Thm. 3.3]. By definition, $\mathbf{1}_G^\perp = G'$. Hence, $\mathbf{1}_G = \mathbf{1}_G^{\perp\perp} = (G')^\perp$. Similarly, $\mathbf{1}_{G'} = G^\perp$. ∎

Remark 15.2: The dual module. We consider our fixed global field K_0, a prime number $l \neq \mathrm{char}(K_0)$, and a finite simple $\mathrm{Gal}(K_0)$-module $A = C_l^r$, for some positive integer r. Let μ_l be the group of roots of unity of order l in $K_{0,\mathrm{sep}}$. We also consider the **dual module** $A' = \mathrm{Hom}(A, \mu_l)$. The group $\mathrm{Gal}(K_0)$ acts on A' by the rule $h^\sigma(a) = h(a^{\sigma^{-1}})^\sigma$ for all $h \in A'$, $\sigma \in \mathrm{Gal}(K_0)$, and $a \in A$. Note that for each $a \in A \smallsetminus \mathbf{1}$ there exists $h \in A'$ such that $h(a) \neq 1$. Hence, the map $(a, h) \mapsto h(a)$ for $a \in A$ and $h \in A'$ is a perfect pairing. In particular, APNa input, 72

(1) A' is isomorphic as a group to C_l^r.

Moreover,

(2) A' is a simple $\mathrm{Gal}(K_0)$-module.

Indeed, if B is a submodule of A' and $B^\perp = \{a \in A \mid h(a) = 1 \text{ for all } h \in B\}$, then $B^\perp$ is a submodule of A. Since A is simple, $B^\perp = \mathbf{1}_A$ or $B^\perp = A$. Hence, by Remark 15.1, $B = A'$ or $B = \mathbf{1}_{A'}$, so A' is simple.

Note that if $\chi\colon \mathrm{Gal}(K_0) \to A$ or $\chi\colon \mathrm{Gal}(K_0) \to A'$ is a crossed homomorphism and $\sigma \in \mathrm{Gal}(K_0)$, then $\chi^l(\sigma) = \chi(\sigma)^l = 1$.

We also recall the following rule:

(3) If a profinite group G acts on A (resp. A'), then $H^i(G,A)^l = \mathbf{1}$ (resp. $H^i(G,A')^l = \mathbf{1}$) for each $i \geq 0$.

Indeed, if $f\colon G^i \to A$ (resp. $f\colon G^i \to A'$) is a cochain of degree i and $\boldsymbol{\sigma} \in G^i$, then $f^l(\boldsymbol{\sigma}) = f(\boldsymbol{\sigma})^l = 1$. ∎

The following result is a generalization of [Neu79, Lemma 2] to global fields.

APNb input, 126

Lemma 15.3: *In the notation of Remark 15.2, let K be a finite Galois extension of K_0 such that $\mathrm{Gal}(K)$ acts trivially on A and $\zeta_l \notin K$. Let P be a subset of $\mathbb{P}(K_0)$ that consists of all but finitely many primes which totally split in $K(\zeta_l)$. Then, the homomorphism $H^1(\mathrm{Gal}(K_0), A') \to \prod_{\mathfrak{p}\in P} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')$ defined as the direct product of the restriction map $H^1(\mathrm{Gal}(K_0), A') \to H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')$, is injective.*

Proof: We set $\Gamma = \mathrm{Gal}(K/K_0)$, $\Delta = \mathrm{Gal}(K(\zeta_l)/K)$, and $Z = \mathrm{Gal}(K(\zeta_l)/K_0)$. Then, we note that if $h \in A'$, $\sigma \in \mathrm{Gal}(K(\zeta_l))$, and $a \in A$, then $a^{\sigma^{-1}} = a$ and $h^\sigma(a) = h(a^{\sigma^{-1}})^\sigma = h(a)$. Hence,

(4) $\mathrm{Gal}(K(\zeta_l))$ acts trivially on A'.

Hence, the action of $\mathrm{Gal}(K_0)$ on A' induces an action of Z, hence also of Δ, on A'. Since $\#\Delta|(l-1)$ (Here we use the assumption that $l \neq \mathrm{char}(K_0)$.), we have

(5) $l \nmid \#\Delta$.

Claim A: *$H^i(\Delta, A') = \mathbf{1}$ for all $i \geq 1$.* Indeed, by (3), each $x \in H^i(\Delta, A')$ satisfies $x^l = 1$. On the other hand, by [Rib70, p. 138, Cor. 6.7], $\mathrm{ord}(x)|\#\Delta$. Hence, by (5), $l \nmid \mathrm{ord}(x)$. It follows that $x = 1$, as claimed.

Claim B: *$H^n(\Gamma,(A')^\Delta) \cong H^n(Z,A')$ for all $n \geq 1$.* Indeed, Claim A, applied to $i=1,\ldots,n-1$, yields an exact inflation-restriction sequence

$$\begin{tikzcd} \mathbf{1} \arrow[r] & H^n(\Gamma,(A')^\Delta) \arrow[r, "\mathrm{inf}"] & H^n(Z,A') \arrow[r, "\mathrm{res}"] & H^n(\Delta,A')^\Gamma \end{tikzcd} \tag{6}$$

that corresponds to the short exact sequence $\mathbf{1}\to\Delta\to Z\to\Gamma\to\mathbf{1}$ [NSW00, p. 64, Prop. 1.6.6]. Again, by Claim A, $H^n(\Delta,A')=\mathbf{1}$. Hence, by (6), inf: $H^n(\Gamma,(A')^\Delta)\to H^n(Z,A')$ is an isomorphism, as claimed.

Claim C: *$H^n(Z,A')=\mathbf{1}$ for all $n\geq 1$.* Indeed, since $\zeta_l\notin K$, the group Δ acts nontrivially on μ_l, so Δ acts nontrivially on A'. Therefore, $(A')^\Delta$ is a proper Z-module of A'. Since by (2), A' is a simple $\mathrm{Gal}(K_0)$-module, A' is also a simple Z-module, so $(A')^\Delta=\mathbf{1}$. It follows from Claim B that $H^n(Z,A')\cong H^n(\Gamma,(A')^\Delta)=\mathbf{1}$, as claimed.

Claim D: *The map* res: $H^1(\mathrm{Gal}(K_0),A')\to H^1(\mathrm{Gal}(K(\zeta_l)),A')^Z$ *is an isomorphism.* Indeed, as in the proof of Claim B, the beginning of the five-term exact sequence attached to the short exact sequence $\mathbf{1}\to\mathrm{Gal}(K(\zeta_l))\to\mathrm{Gal}(K_0)\to Z\to\mathbf{1}$ takes the following form:

$$\begin{tikzcd} \mathbf{1} \arrow[r] & H^1(Z,(A')^{\mathrm{Gal}(K(\zeta_l))}) \arrow[r, "\mathrm{inf}"] & H^1(\mathrm{Gal}(K_0),A') \\ {} \arrow[r, "\mathrm{res}"] & H^1(\mathrm{Gal}(K(\zeta_l)),A')^Z \arrow[r, "\mathrm{tg}"] & H^2(Z,(A')^{\mathrm{Gal}(K(\zeta_l))}). \end{tikzcd} \tag{7}$$

By (4), $(A')^{\mathrm{Gal}(K(\zeta_l))}=A'$. Hence, by Claim C, the second and the fifth terms of (7) are trivial, so res: $H^1(\mathrm{Gal}(K_0),A')\to H^1(\mathrm{Gal}(K(\zeta_l)),A')^Z$ is an isomorphism, as claimed.

Next we consider the commutative diagram

$$\begin{tikzcd} H^1(\mathrm{Gal}(K_0),A') \arrow[r] \arrow[d] & \prod_{\mathfrak{p}\in P} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}),A') \arrow[d] \\ H^1(\mathrm{Gal}(K(\zeta_l)),A')^Z \arrow[r] & \prod_{\mathfrak{p}\in P}\prod_{\mathfrak{P}|\mathfrak{p}} H^1(\mathrm{Gal}(\widehat{K(\zeta_l)}_{\mathfrak{P}}),A'), \end{tikzcd} \tag{8}$$

where all of the arrows are restriction maps or appropriate direct products of restriction maps.

Claim E: *The lower horizontal map in (8) is injective.* Indeed, let x be an element of

$$H^1(\mathrm{Gal}(K(\zeta_l)), A')^Z.$$

By (4), $\mathrm{Gal}(K(\zeta_l))$ acts trivially on A', hence $x\colon \mathrm{Gal}(K(\zeta_l)) \to A'$ is a homomorphism. Let N be the fixed field of $\mathrm{Ker}(x)$ in $K_{0,\mathrm{sep}}$. Then, N is a finite Galois extension of $K(\zeta_l)$. We prove that N is a Galois extension of K_0.

Indeed, we consider $\sigma \in \mathrm{Gal}(K_0)$ and set $\bar\sigma = \mathrm{res}_{K_{0,\mathrm{sep}}/K(\zeta_l)}(\sigma) \in Z$. Then, by definition, $x^{\bar\sigma}$ is the element of $H^1(\mathrm{Gal}(K(\zeta_l)), A')$ defined by $x^{\bar\sigma}(\tau) = x(\tau^{\sigma^{-1}})^\sigma$ for each $\tau \in \mathrm{Gal}(K(\zeta_l))$ [NSW00, p. 44, 1. Conjugation]. Since, by our choice, $x^{\bar\sigma} = x$, we have $x(\tau)^{\sigma^{-1}} = x(\tau^{\sigma^{-1}})$. In particular, if $\tau \in \mathrm{Gal}(N) = \mathrm{Ker}(x)$, then $1 = x(\tau^{\sigma^{-1}})$, so $\tau^{\sigma^{-1}} \in \mathrm{Ker}(x)$. This implies that $\mathrm{Ker}(x)$ is a normal subgroup of $\mathrm{Gal}(K_0)$, which proves our claim.

Now assume that for each $\mathfrak{p} \in P$ and every $\mathfrak{P} \in \mathbb{P}(K(\zeta_l))$ over $\mathfrak{p}$ we have $\mathrm{res}_{\mathfrak{P}}(x) = 1$. Thus, $x(\tau) = 1$ for each $\tau \in \mathrm{Gal}(K(\zeta_l)_{\mathfrak{P}})$, so $N \subseteq K(\zeta_l)_{\mathfrak{P}}$. It follows that $\mathfrak{p}$ totally splits in N. Conversely, since $K(\zeta_l) \subseteq N$, every prime of K_0 that totally splits in N also totally splits in $K(\zeta_l)$. Thus, for almost all $\mathfrak{p} \in \mathbb{P}(K_0)$ we have that $\mathfrak{p}$ totally splits in $K(\zeta_l)$ if and only if $\mathfrak{p}$ totally splits in N. By a theorem of Bauer $N = K(\zeta_l)$ (see [Neu99, p. 548, Prop. 13.9] for number fields and [FrJ08, pp. 129-130, Exercise 5] for global fields). Consequently, $x = 1$, as claimed.

Conclusion of the proof: By Claims D and E, both the left vertical arrow and the lower horizontal arrow of the commutative Diagram (8) are injective. It follow that the upper horizontal arrow of that diagram is injective, as claimed by the lemma. ∎

For each $\mathfrak{p} \in \mathbb{P}_{\mathrm{nonarch}}(K_0)$ and for $i = 1, 2$ we denote the image of the map

$$\mathrm{inf}\colon H^i(\mathrm{Gal}(\hat K_{0,\mathfrak{p},\mathrm{ur}}/\hat K_{0,\mathfrak{p}}), A) \to H^i(\mathrm{Gal}(\hat K_{0,\mathfrak{p}}), A)$$

by $H^i_{\mathrm{ur}}(\mathrm{Gal}(\hat K_{0,\mathfrak{p}}), A)$. In particular, $H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat K_{0,\mathfrak{p}}), A)$ is the subgroup of unramified elements of

$$H^1(\mathrm{Gal}(\hat K_{0,\mathfrak{p}}), A)$$

(Subsection 9.1). Similar notation applies to A' rather than to A.

Lemma 15.4: *In the notation of Remark 15.2, let $x \in H^1(\mathrm{Gal}(K_0), A)$. Then,* APNc input, 316

$$\mathrm{res}_{\mathfrak{p}}(x) \in H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$$

for almost all $\mathfrak{p} \in \mathbb{P}_{\mathrm{nonarch}}(K_0)$.

Proof: Let χ be a crossed homomorphism that represents x. As such, χ is continuous. Hence, there exists a finite Galois extension K' of K_0 that contains K such that χ is trivial on $\mathrm{Gal}(K')$. If χ' is another representative of χ, then there exists $a \in A$ such that $\chi'(\sigma) = a^\sigma a^{-1}\chi(\sigma)$ for each $\sigma \in \mathrm{Gal}(K_0)$. Let K'' be a finite Galois extension of K_0 that contains K' such that $\mathrm{Gal}(K'')$ acts trivially on A. Then, for each $\sigma \in \mathrm{Gal}(K'')$ we have $\chi'(\sigma) = a^\sigma a^{-1}\chi(\sigma) = \chi(\sigma) = 1$. Thus, the restriction of x to $H^1(\mathrm{Gal}(K''), A)$ is trivial.

Now recall that almost all $\mathfrak{p} \in \mathbb{P}(K_0)$ are unramified in K''. In other words, $K'' \subseteq \hat{K}_{0,\mathfrak{p},\mathrm{ur}}$ (Subsection 1.5). Hence, by the preceding paragraph, the restriction of x to $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p},\mathrm{ur}})$ is trivial. This means that $\mathrm{res}_{\mathfrak{p}}(x) \in H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$, as desired. ∎

Next we generalize [Neu79, Lemma 3] to global fields.

Lemma 15.5: *In the notation of Remark 15.2, let K be a finite Galois extension of K_0 such that $\mathrm{Gal}(K)$ acts trivially on A and $\zeta_l \notin K$. Let S be a finite set of primes of K_0 and for each $\mathfrak{p} \in S$ consider $y_{\mathfrak{p}} \in H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$. Then, there exists $z \in H^1(\mathrm{Gal}(K_0), A)$ such that* APNd input, 353

(a) $\mathrm{res}_{\mathfrak{p}}(z) = y_{\mathfrak{p}}$ *for each $\mathfrak{p} \in S$ and*

(b) *if $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus S$ and $\mathrm{res}_{\mathfrak{p}}(z)$ is ramified, then $\mathfrak{p}$ totally splits in $K(\zeta_l)$.*

Proof: Let S' be a finite subset of $\mathbb{P}(K_0)$ that contains S. For each $\mathfrak{p} \in S' \smallsetminus S$ let $y_{\mathfrak{p}}$ be the unit element of $H^1(\mathrm{Gal}(K_{0,\mathfrak{p}}), A)$. In particular, if $\mathfrak{p}$ is non-archimedean, then $y_{\mathfrak{p}}$ is unramified (Subsection 9.1). Thus, if the lemma holds for S', then it holds for S. It follows that we may assume without loss that S contains (in the number field case) all prime divisors of l and all infinite primes of K_0.

We denote the set of all $\mathfrak{p} \in \mathbb{P}(K_0)$ that totally split in $K(\zeta_l)$ by $\mathrm{Splt}(K(\zeta_l)/K_0)$ and set $P = S \cup \mathrm{Splt}(K(\zeta_l)/K_0)$. The rest of the proof breaks up into several parts.

Part A: *A local-global principle for the first cohomology groups.* By Lemma 15.3, the product

$$H^1(\mathrm{Gal}(K_0), A') \to \prod_{\mathfrak{p}\in P \smallsetminus S} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')$$

of the restriction maps is injective. Hence, so is the map

$$\begin{aligned}(9)\qquad H^1(\mathrm{Gal}(K_0), A') \to \prod_{\mathfrak{p}\in P \smallsetminus S} & H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A') \\ & \times \prod_{\mathfrak{p}\notin P} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')/H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A').\end{aligned}$$

Part B: *Restricted products.* The cohomology groups $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ and $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')$ are equipped with discrete topology [NSW00, p. 324]. In particular, each subgroup of those groups is open. Thus, it makes sense to consider the restricted products

(10) $X = \prod'_{\mathfrak{p}} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ and $X' = \prod'_{\mathfrak{p}} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')$ with respect to the subgroups

$H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ and $H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')$, respectively.

Let Y be the image of $H^1(\mathrm{Gal}(K_0), A)$ in $\prod_{\mathfrak{p}} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ under the map $x \mapsto (\mathrm{res}_{\mathfrak{p}}(x))_{\mathfrak{p}}$. By Lemma 15.4, $Y \subseteq X$. Similarly, the image Y' of $H^1(\mathrm{Gal}(K_0), A')$ in $\prod_{\mathfrak{p}} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')$ under the map $x \mapsto (\mathrm{res}_{\mathfrak{p}}(x))_{\mathfrak{p}}$ is contained in X'.

Part C: *Duality.* For each $\mathfrak{p} \in \mathbb{P}(K_0)$ the cup product gives a perfect pairing

$$(11)\qquad H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A) \times H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A') \to \bigcup_{\substack{n=1\\ p\nmid n}}^{\infty} \mu_n,$$

where $p = \mathrm{char}(K_0)$ [NSW00, p. 327, Thm. 7.2.6]. By (3), the exponent of each of the groups on the left-hand side of (11) divides l. Hence, we actually have a perfect pairing $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A) \times H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A') \to \mu_l$.

If $x \in X$ and $x' \in X'$, then by definition, for almost all $\mathfrak{p} \in \mathbb{P}(K_0)$ we have

$$\mathrm{res}_{\mathfrak{p}}(x) \in H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A) \text{ and } \mathrm{res}_{\mathfrak{p}}(x') \in H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A').$$

Moreover, ignoring the finitely many $\mathfrak{p}$'s that ramify in $K(\zeta_l)$, we have $A^{\hat{I}_{\mathfrak{p}}} = A$ and $(A')^{\hat{I}_{\mathfrak{p}}} = A'$ (by (4)). Hence, by [NSW00, p. 333, Thm. 7.2.15], $(\mathrm{res}_{\mathfrak{p}}(x), \mathrm{res}_{\mathfrak{p}}(x')) = 1$

for all of those $\mathfrak{p}$'s. It follows that the expression $(x, x') = \prod_{\mathfrak{p}} (\mathrm{res}_{\mathfrak{p}}(x), \mathrm{res}_{\mathfrak{p}}(x'))$ is a well-defined element of μ_l. This defines a perfect pairing $X \times X' \to \mu_l$.

By [NSW00, p. 412, Prop. 8.5.2], Y and Y' are mutually orthogonal complements in $X \times X'$. That is $Y = (Y')^{\perp} = \{y \in X \mid (y, y') = 1 \text{ for all } y' \in Y'\}$ and $Y' = Y^{\perp} = \{y' \in X' \mid (y, y') = 1 \text{ for all } y \in Y\}$.

Part D: *The subgroup W.* We consider the following subgroup of X:

(12) $W = \prod_{\mathfrak{p} \in S} \mathbf{1}_{\mathfrak{p}} \times \prod_{\mathfrak{p} \in P \smallsetminus S} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A) \times \prod_{\mathfrak{p} \notin P} H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$,

where $\mathbf{1}_{\mathfrak{p}}$ is the trivial subgroup of $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$.

By Part C, $\mathbf{1}_{\mathfrak{p}}^{\perp} = H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')$ for each $\mathfrak{p} \in S$ (actually, for all $\mathfrak{p}$), $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)^{\perp}$ is the trivial subgroup of $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')$ for each $\mathfrak{p} \in P \smallsetminus S$, and $H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)^{\perp} = H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')$, if $\mathfrak{p} \in \mathbb{P}_{\mathrm{nonarch}}(K_0) \smallsetminus P$ [NSW00, p. 333, Thm. 7.2.15]. Hence,

$$W^{\perp} = \prod_{\mathfrak{p} \in S} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A') \times \prod_{\mathfrak{p} \in P \smallsetminus S} \mathbf{1}'_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin P} H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')$$

(where, $\mathbf{1}'_{\mathfrak{p}}$ is the trivial subgroup of $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')$) is a subgroup of X' and $X'/W^{\perp}$ is equal to the right-hand side of (9). Therefore, the map $Y' \to X'/W^{\perp}$ defined by $y' \mapsto y'W^{\perp}$ is injective. It follows that

(13) $Y' \cap W^{\perp} = \mathbf{1}_{X'}$.

Part E: *We prove that $Y \cdot W$ is a closed subgroup of X.* Indeed, by the definition of the restricted topology, the open subgroups of X have the form $\prod_{\mathfrak{p} \in T} V_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin T} H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$, where T is a finite subset of $\mathbb{P}(K_0)$ and $V_{\mathfrak{p}}$ is a subgroup of $H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ for each $\mathfrak{p} \notin T$. By (12), W hence also $Y \cdot W$ contains such a subgroup. Therefore, $Y \cdot W$ is an open subgroup of X. It follows that $Y \cdot W$ is a closed subgroup of X.

Part F: *Conclusion of the proof.* By Remark 15.1, Part C, and (13), $(Y \cdot W)^{\perp} = Y^{\perp} \cap W^{\perp} = Y' \cap W^{\perp} = \mathbf{1}_{X'}$. By Part E, $Y \cdot W$ is closed. Hence, by Remark 15.1, $Y \cdot W = (Y \cdot W)^{\perp\perp} = \mathbf{1}_{X'}^{\perp} = X$. Thus, Y is mapped onto X/W under the quotient map $X \to X/W$. By (10) and (12),

(14) $X/W = \prod_{\mathfrak{p} \in S} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A) \times \prod_{\mathfrak{p} \notin P} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)/H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$.

Since Y is the image of $H^1(\mathrm{Gal}(K_0), A)$ in X, there exists $z \in H^1(\mathrm{Gal}(K_0), A)$ such that $\mathrm{res}_{\mathfrak{p}}(z) = y_{\mathfrak{p}}$ for each $\mathfrak{p} \in S$ and $\mathrm{res}_{\mathfrak{p}}(z) \in H^1_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ for each $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus P$, in particular $\mathrm{res}_{\mathfrak{p}}(z)$ is unramified. Therefore, if $\mathfrak{p} \in \mathbb{P}(K_0) \smallsetminus S$ and $\mathrm{res}_{\mathfrak{p}}(z)$ is ramified, we have $\mathfrak{p} \in P \smallsetminus S$, so $\mathfrak{p} \in \mathrm{Splt}(K(\zeta_l)/K_0)$, which means that $\mathfrak{p}$ totally splits in $K(\zeta_l)$, as claimed. ■

Definition 15.6: For a $\mathrm{Gal}(K_0)$-module A we denote the restricted product of the groups RESP input, 570
$H^2(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ with respect to the subgroups $H^2_{\mathrm{ur}}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ by $\prod'_{\mathfrak{p}} H^2(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$.■
■

Lemma 15.7: *In the notation of Remark 15.2 the homomorphism* APNe input, 580

$$\prod\nolimits_{\mathfrak{p}} \mathrm{res}_{\mathfrak{p}} \colon H^2(\mathrm{Gal}(K_0), A) \to \prod\nolimits'_{\mathfrak{p}} H^2(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A) \tag{15}$$

defined as the product of the restriction maps is injective.

Proof: First note that the image of the left-hand side of (15) does indeed lie in $\prod'_{\mathfrak{p}} H^2(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A)$ [NSW00, p. 417, Prop. 8.6.1]. Now let $\mathbf{Sh}^2(\mathrm{Gal}(K_0), A)$ be the kernel of the map (15) and let

$$\mathbf{Sh}^1(\mathrm{Gal}(K_0), A')$$

be the kernel of the map $H^1(\mathrm{Gal}(K_0), A') \to \prod'_{\mathfrak{p}} H^1(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), A')$. The Poitou-Tate duality theorem supplies a perfect pairing $\mathbf{Sh}^2(\mathrm{Gal}(K_0), A) \times \mathbf{Sh}^1(\mathrm{Gal}(K_0), A') \to \mu_l$ (by [NSW00, p. 422, Thm. 8.6.8], taking into account that the exponents of the cohomology groups are l).

By Lemma 15.3, $\mathbf{Sh}^1(\mathrm{Gal}(K_0), A') = \mathbf{1}$. Hence, by the perfect pairing, also $\mathbf{Sh}^2(\mathrm{Gal}(K_0), A) = \mathbf{1}$. It follows that map (15) is injective. ■

The following lemma appears as Lemma 4 of [Neu79] for number fields and as Lemma 9.5.6 on page 565 of [NSW15] for global fields.

Lemma 15.8: *In the notation of Remark 15.2 and Subsection 7.3 we have* APNf input, 617

$$\mathcal{H}\mathrm{om}_{\Gamma,\rho,\alpha}(\mathrm{Gal}(K_0), G) \neq \emptyset \iff \prod \mathcal{H}\mathrm{om}_{\Gamma,\rho_{\mathfrak{p}},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}), G) \neq \emptyset. \tag{16}$$

Proof: We have already noticed in Subsection 7.3 that the restrictions to the local groups $\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})$ give the implication "$\Longrightarrow$" of (16). The proof of the reverse implication "$\Longleftarrow$" of (16) breaks up into three parts.

Part A: *Global short exact sequences.* We consider the commutative diagram

(17)
$$\begin{tikzcd}
\mathbf{1} \arrow[r] & A \arrow[r] \arrow[d, equal] & \hat{G} \arrow[r, "\hat{\alpha}"] \arrow[d] & \mathrm{Gal}(K_0) \arrow[r] \arrow[d, "\rho"] & \mathbf{1} \\
\mathbf{1} \arrow[r] & A \arrow[r] & G \arrow[r, "\alpha"] & \Gamma \arrow[r] & \mathbf{1},
\end{tikzcd}$$

where the right square is cartesian (with the fiber product $\hat{G} = G \times_A \mathrm{Gal}(K_0)$) [FrJ08, p. 500, Def. 22.2.2]. By the basic property of cartesian squares, the upper row of (17) splits if and only if there exists a homomorphism ψ: $\mathrm{Gal}(K_0) \to G$ such that $\alpha \circ \psi = \rho$. Thus, $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\alpha}(\mathrm{Gal}(K_0), G) \neq \emptyset$ if and only if the upper row of (17) splits.

By a theorem of Schreier [NSW00, p. 7, Thm. 1.2.5], each element y of $H^2(\mathrm{Gal}(K_0), A)$ bijectively corresponds to a short exact sequence, as in the upper row of (17), modulo a natural "congruence relation". The unit element of $H^2(\mathrm{Gal}(K_0), A)$ corresponds to the class of the splitting short exact sequences.

Next consider the homomorphism ρ^*: $H^2(\Gamma, A) \to H^2(\mathrm{Gal}(K_0), A)$ that attaches the cohomology class of each inhomogeneous cocycle f: $\Gamma^2 \to A$ to the cohomology class of the inhomogeneous cocycle $f \circ \rho$: $\mathrm{Gal}(K_0)^2 \to A$. Thus, if x is the element of $H^2(\Gamma, A)$ that corresponds (under the theorem of Schreier) to the lower row of (17), then by the two preceding paragraphs, $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\alpha}(\mathrm{Gal}(K_0), G) \neq \emptyset$ if and only if $\rho^*(x) = 1$.

Part B: *Local short exact sequences.* Similarly, for each $\mathfrak{p} \in \mathbb{P}(K_0)$ we consider the local counterpart of Diagram (17):

(18)
$$\begin{tikzcd}
\mathbf{1} \arrow[r] & A \arrow[r] \arrow[d, equal] & \hat{G}_{\mathfrak{p}} \arrow[r, "\hat{\alpha}_{\mathfrak{p}}"] \arrow[d] & \mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}) \arrow[r] \arrow[d, "\rho_{\mathfrak{p}}"] & \mathbf{1} \\
\mathbf{1} \arrow[r] & A \arrow[r] & G \arrow[r, "\alpha"] & \Gamma \arrow[r] & \mathbf{1},
\end{tikzcd}$$

where, as in Subsection 7.3, $\rho_{\mathfrak{p}} = \rho|_{\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}})}$, and again the right square is cartesian. Then, $\mathrm{res}_{\mathfrak{p}}(x)$ is the element of $H^2(\Gamma_{\mathfrak{p}}, A)$ that corresponds to the lower short exact sequence in (18). As in Part A, $\mathcal{H}\mathrm{om}_{\Gamma,\rho_\mathfrak{p},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}),G) \neq \emptyset$ if and only if $\rho_\mathfrak{p}^*(x) = 1$, where $\rho_\mathfrak{p}^*\colon H^2(\Gamma_\mathfrak{p},A) \to H^2(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}),A)$ is the map associated with $\rho_\mathfrak{p}$.

Part C: *Conclusion of the proof.* Note that $\mathrm{res}_\mathfrak{p}(\rho^*(x)) = \rho_\mathfrak{p}^*(x)$. Thus, the diagram

(19)
$$\begin{tikzcd} & H^2(\Gamma,A) \arrow[dl, "\rho^*"'] \arrow[dr, "\prod \rho_\mathfrak{p}^*"] & \\ H^2(\mathrm{Gal}(K_0),A) \arrow[rr, "\prod_\mathfrak{p} \mathrm{res}_\mathfrak{p}"] & & \prod_\mathfrak{p}' H^2(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}),A) \end{tikzcd}$$

is commutative.

Now suppose that $\prod_\mathfrak{p} \mathcal{H}\mathrm{om}_{\Gamma,\rho_\mathfrak{p},\alpha}(\mathrm{Gal}(\hat{K}_{0,\mathfrak{p}}),G) \neq \emptyset$. Then, by Part B, $\prod_\mathfrak{p} \rho_\mathfrak{p}^*(x) = 1$. Since Triangle (19) is commutative and $\prod_\mathfrak{p} \mathrm{res}_\mathfrak{p}$ is injective (Lemma 15.7), we have $\rho^*(x) = 1$. Hence, by Part A, $\mathcal{H}\mathrm{om}_{\Gamma,\rho,\alpha}(\mathrm{Gal}(K_0),G) \neq \emptyset$, as claimed. ∎

References

[ArT52] E. Artin and J. Tate, *Class Field Theory,* Notes of a seminar given at Princeton University, Princeton, New Jersey, 1951-1952.

[Bir94] B. Birch, *Noncongruence subgroups, covers and drawings,* in: Leila Schneps (Ed.), The Grothendieck Theory of Dessins d'Enfant, Cambridge University Press 1994, pp. 25–46.

[CaF67] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory,* Academic Press, London, 1967.

[FeT63] W. Feit and J. G. Thompson, *Solvability of groups of odd order,* Pacific Journal of Mathematics **13** (1963), 775–1029.

[FrJ08] M. D. Fried and M. Jarden, *Field Arithmetic, third edition, revised by Moshe Jarden,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2008.

[GeJ98] W.-D. Geyer and M. Jarden, *Bounded realization of l-groups over global fields,* Nagoya Mathematical Journal **150** (1998), 13–62.

[HaW62] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers, fourth edition,* Oxford at the Clarendon Press, London, 1962.

[Jar11] M. Jarden, *Algebraic Patching,* Springer Monographs in Mathematics, Springer, 2011.

[Lan93] S. Lang, *Algebra, third edition,* Addison-Wesley, Reading, 1993.

[MaU11] N. Markin and S. V. Ullom, *Minimal ramification in nilpotent extensions,* Pacific Journal of Mathematics **253** (2011), 125–143.

[Neu79] J. Neukirch, *On solvable number fields,* Inventiones Mathematicae **53** (1979), 135–164.

[Neu99] J. Neukirch, *Algebraic Number Theory,* Grundlehren der mathematischen Wissenschaften **322**, Springer, 1999.

[NSW00] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields,* Grundlehren der mathematischen Wissenschaften **323**, Springer-Verlag, Heidelberg, 2000.

[NSW15] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields,* Grundlehren der mathematischen Wissenschaften **323**, Springer-Verlag, Heidelberg, Second Edition, corrected version 2.2, July 2015. Electronic Edition, www.mathi.uni-heidelberg.de\ ∼schmidt\NSW2e.

[Pon46] L. Pontrjagin, *Topological Groups,* Princeton University Press, 1946.

[Pop96] F. Pop, *Embedding problems over large fields,* Annals of Mathematics **144** (1996), 1–34.

[Ram13] N. C. Ramiharimanana, *Realization of finite groups as Galois groups over* $\mathbb{Q}$ *in* $\mathbb{Q}_{\mathrm{tot},p}$, Master Thesis, Stellenbosch University, 2013.

[Ram16] N. C. Ramiharimanana, *Solving embedding problems with bounded ramification,* PhD Thesis, Stellenbosch University, 2016.

[Rei37] H. Reichhardt, *Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung,* Journal für die reine und angewandte Mathematik **177** (1937), 1–6.

[Rib70] L. Ribes, *Introduction to Profinite Groups and Galois Cohomology,* Queen's papers in Pure and Applied Mathematics **24**, Queen's University, Kingston, 1970.

[Sch37] Arnold Scholz, *Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I,* Mathematische Zeitschrift **42** (1937), 161–188.

[Ser79] J.-P. Serre, *Local Fields,* Graduate Text in Mathematics **67**, Springer, New York, 1979.

[Ser92] J.-P. Serre, *Topics in Galois Theory,* Jones and Barlett, Boston 1992.

[Sha54A] I. R. Shafarevich, *Construction of fields of algebraic numbers with given solvable groups (Russian),* Izvestia Akademy Nauk. SSSR **18** (1954), 525-578. English translation in American Mathematical Society Translations **4** (1956), 185-237.

[Sha54B] I. R Shafarevich, *On the construction of fields with a given Galois group of order l^n,* Izvestia Akademy Nauk **18** (1954), 261–296. (Collected Mathematical Papers 69–97, Springer, Berlin, 1989.)

[Sha89] I. R. Shafarevich, *Factors of descending center series,* Mathematical Notes **45** (1989), pp. 262-264.