On Ozaki’s theorem realizing prescribed $p$-groups as $p$-class tower groups

Farshid Hajir, Christian Maire and Ravi Ramakrishna
On Ozaki’s theorem realizing prescribed $p$-groups as $p$-class tower groups

Farshid Hajir, Christian Maire and Ravi Ramakrishna

We give a streamlined and effective proof of Ozaki’s theorem that any finite $p$-group $\Gamma$ is the Galois group of the $p$-Hilbert class field tower of some number field $F$. Our work is inspired by Ozaki’s and applies in broader circumstances. While his theorem is in the totally complex setting, we obtain the result in any mixed signature setting for which there exists a number field $k_0$ with class number prime to $p$. We construct $F/k_0$ by a sequence of $\mathbb{Z}/p$-extensions ramified only at finite tame primes and also give explicit bounds on $[F:k_0]$ and the number of ramified primes of $F/k_0$ in terms of $\#\Gamma$.

1. Introduction

For a number field $k$, define $L_p(k)$ to be the compositum of all finite unramified Galois $p$-extensions of $k$. The extension $L_p(k)/k$ is called the $p$-Hilbert class field tower of $k$, and its Galois group $\text{Gal}(L_p(k)/k)$ is its $p$-class tower group. Ozaki [2011] proved that every finite $p$-group $\Gamma$ occurs as $\text{Gal}(L_p(F)/F)$ for some totally complex number field $F$. His strategy is as follows.

As finite $p$-groups are solvable, it is natural to proceed by induction. After establishing the base case (realizing $\mathbb{Z}/p$ as a $p$-class tower group), it remains to show that given any short exact sequence of finite $p$-groups

$$1 \to \mathbb{Z}/p \to G' \to G \to 1$$

where $G := \text{Gal}(L_p(k)/k)$, one can realize $G'$ as $\text{Gal}(L_p(k')/k')$ for some number field $k'$. Ozaki constructs such a $k'/k$ via a sequence of carefully chosen $\mathbb{Z}/p$-extensions.

In this paper, we provide a streamlined and effective proof of Ozaki’s theorem. Some differences between our work and Ozaki’s are:

- He must start with a totally complex $k_0$ and then construct a field $F/k_0$ whose $p$-Hilbert class field tower has the given $\Gamma$ as its Galois group, while we start with a number field $k_0$ of arbitrary signature whose class number is prime to $p$.  

Maire was partially supported by the ANR project FLAIR (ANR-17-CE40-0012) and by the EIPHI Graduate School (ANR-17-EURE-0002). Ramakrishna was partially supported by Simons Collaboration grant #524863. He also thanks FEMTO-ST for its hospitality and wonderful research environment during his visit there in the spring of 2022. All three authors were supported for a Collaborate@ICERM visit in January, 2022. We express our gratitude to the referees for carefully reading the manuscript and providing many helpful suggestions for improvement.

MSC2020: 11R29.

Keywords: Class group, Hilbert class field tower, Minkowski unit, $p$-groups.

© 2024 MSP (Mathematical Sciences Publishers). Distributed under the Creative Commons Attribution License 4.0 (CC BY). Open Access made possible by subscribing institutions via Subscribe to Open.
Our result is effective and we are able to obtain explicit upper bounds on \([F : k_0]\) and the number of ramified primes in \(F/k_0\), all of which are tame and finite.

Moreover, we bypass some of the most delicate and involved arguments of [Ozaki 2011].

We prove:

**Theorem.** Let \(\Gamma\) be a finite \(p\)-group and \(k_0\) a number field with \((\# \text{Cl}_{k_0}, p) = 1\). There exist infinitely many number fields \(F/k_0\) such that \(\text{Gal}(L_p(F)/F) \simeq \Gamma\) and

- if \(\mu_p \not\subset k_0\) then \(F/k_0\) is of degree at most \(p^2 \cdot \#\Gamma\) and is ramified at at most \(2 + 2 \log_p(\#\Gamma)\) finite tame primes,
- if \(\mu_p \subset k_0\) then \(F/k_0\) is of degree at most \(p \cdot (\#\Gamma)^2\) and is ramified at at most \(1 + 3 \log_p(\#\Gamma)\) finite tame primes.

**Remark.** If our starting field \(k_0\) has infinite \(p\)-Hilbert class field tower, there is no hope of solving the problem with a finite extension of \(k_0\). If on the other hand the tower is finite, one can simply pass to the number field \(L_p(k_0)\), which has the same signature ratio as \(k_0\), and use that as the starting point to realize \(\Gamma\).

As any (topologically) countably generated pro-\(p\) group \(\Gamma\) is the inverse limit of finite \(p\)-groups, Ozaki shows any such \(\Gamma\) is the Galois group of the maximal unramified \(p\)-extension of some infinite extension of \(\mathbb{Q}\). The corresponding corollary of our theorem is:

**Corollary.** Any (topologically) countably generated pro-\(p\) group \(\Gamma\), including \(p\)-adic analytic \(\Gamma\), can be realized as \(\text{Gal}(L_p(F)/F)\) for a totally real tamely ramified infinite extension \(F/\mathbb{Q}\).

We now give details about the structure of our proof and the difference between our methods and Ozaki’s, though we were very much inspired by Ozaki’s beautiful theorem and techniques.

We start the base case of the inductive process with any number field \(k_0\), of any signature, whose class number is prime to \(p\). Referring to the group extension (1) with \(G\) being trivial, one has to find an extension \(k'/k_0\) such that \(k'\) has \(p\)-class group tower exactly \(\mathbb{Z}/p\), which is equivalent to the \(p\)-class group being \(\mathbb{Z}/p\). This is a standard argument and is part of Proposition 2.15.

The base case being done, we proceed to the inductive step (with our base field relabeled \(k\)). There are two cases, depending on whether (1) splits or not. For the sake of brevity, we only outline the nonsplit case in this introduction; the split case is handled similarly. For a set of places of \(k\), we say that an extension \(k'/k\) is exactly ramified at \(S\) if it is ramified at all the places in \(S\) and nowhere else.

We need to find a suitable tame prime \(v_1\) of \(k\) such that:

- \(v_1\) splits completely in \(L_p(k)/k\).
- There is no \(\mathbb{Z}/p\)-extension of \(k\) exactly ramified at \(v_1\).
- The maximal \(p\)-extension \(L_p(k)_{v_1}/L_p(k)\) exactly ramified at the primes of \(L_p(k)\) above \(v_1\) is of degree \(p\) and solves the embedding problem (1).
We replace Theorem 3.2 when version of his Proposition 1, has only one tame prime of ramification and $K$ plays no role. We only invoke embedding problem (1). Several tame primes are ramified in $\tilde{\mathcal{O}}_{L}$ to a solution ramified at one tame prime. He then proceeds as in the description of this work using two wildly ramified $\mathbb{Z}$.

Ozaki [2011, Section 6] proves his base change Proposition 1, namely he shows there exists a ramified $\bullet$ signature of $k$. We neither consider $K$ nor invoke the estimates of Section 4 of [loc. cit.].

For the induction to go forward, Ozaki needs enough Minkowski units to keep the induction going. Proposition 2.14 guarantees this. To sum up, the key ingredients of the proof of the above theorem and corollary are Theorems 3.2 and 3.3 and Proposition 2.14.

We now explain in some detail Ozaki’s approach and our simplifications:

- Using a result of Horie [1987], Ozaki starts with a quadratic imaginary field with class number prime to $p$ in which $p$ is inert. He then chooses a suitable layer $k$ in the cyclotomic $\mathbb{Z}/p$-extension as the starting point of his induction. Assuming the problem solved for $G$ in (1) and relabelling $k$ as his base field, he proceeds inductively with the goal to find a $k$ such that $\text{Gal}(L_p(k)/k) \simeq \text{Gal}(L_p(k)/k)$. Theorem 3.2 provides such a $k$.

- Ozaki [2011, Section 6] proves his base change Proposition 1, namely he shows there exists a ramified $\mathbb{Z}/p$-extension $\tilde{k}/k$ such that $\text{Gal}(L_p(\tilde{k})/\tilde{k}) \simeq \text{Gal}(L_p(k)/k)$. He uses this repeatedly when solving each embedding problem (1). Several tame primes are ramified in $\tilde{k}/k$ and he also needs that $K$ and $Kk$ have the same $p$-class group. This makes the proof significantly more involved. Theorem 3.2 of this paper, our version of his Proposition 1, has only one tame prime of ramification and $K$ plays no role. We only invoke Theorem 3.2 when $\mu_p \subseteq k$. In particular, for $p$ odd, our Corollary above makes no use of Theorem 3.2.

- To solve the embedding problem (1), Ozaki base changes several times (to a field relabeled $k$) and then uses a wildly ramified $\mathbb{Z}/p$-extension $L/L_p(k)$ to solve (1). After more base changes this is switched to a solution ramified at one tame prime. He then proceeds as in the description of this work using two
such solutions and a base change that absorbs the ramification at both tame primes to find a $k'$ such that $\text{Gal}(L_p(k'/k')) = G'$. We go directly to this last step and require at most two $\mathbb{Z}/p$-base changes to solve the embedding problem. This allows us to quantify explicitly both the degree and number of ramified primes of $F/k_0$.

**Notations.** Let $p$ be a prime number:

- $L$ is a number field, $\mathcal{O}_L$ its ring of integers, $\mathcal{O}_L^\times$ its units and $\text{Cl}_L$ and $\text{Cl}_L[p^\infty]$ are, respectively, the class group of $L$ and its $p$-Sylow subgroup.
- For a finite set $S$ of primes of $L$, set $V_{L,S} = \{x \in L^\times, (x) = I^p, x \in (L^\times_v)^p\forall v \in S\}$.

In particular, one has the exact sequence

$$1 \to \mathcal{O}_L^\times \otimes_{\mathbb{F}_p} V_{L,\emptyset} \to (L^\times)^p \to \text{Cl}_L[p] \to 1.$$ 

- The superscript $^\wedge$ indicates the Kummer dual of an object $Z$ defined over a number field $L$, though we never work with the $\text{Gal}(L(\mu_p)/L)$ action on $Z^\wedge$.
- $L_S$ is the maximal pro-$p$-extension of $L$ unramified outside $S$, $G_S := \text{Gal}(L_S/L)$ and $L_p(L) := L_\emptyset$, the maximal unramified pro-$p$-extension of $L$, as it will ease notation at various points.
- $h^i(H) := \dim H^i(H, \mathbb{Z}/p)$.
- $\text{Gov}(L) := L(\mu_p)(\sqrt[p]{V_{L,\emptyset}})$, the governing field of $L$. The span of $\{\text{Fr}_v\}_{v \in S}$ in $M(L) := \text{Gal}(\text{Gov}(L)/L(\mu_p))$ controls $\dim H^1(G_S)$.

The following may be helpful in orienting the reader:

- We frequently use finite tame primes with desired splitting properties in number field extensions. We always use Chebotarev’s theorem for the existence of such primes.
- Our $\mathbb{Z}/p$-extensions $L'/L$ of number fields are only ramified at (one or two) finite tame primes so $r_i(L') = p \cdot r_i(L)$ and $\mu_p \subset L' \iff \mu_p \subset L$.
- Note that $k_0$ is our given base field, whereas $k$ is a field used in the inductive process with $p$-class tower group $G$ from (1). Our task is to construct $k'$ with $p$-class tower group $G'$. Finally, $\tilde{k}/k$ is an extension having $p$-class tower group $G$, the same as for $k$.

2. Tools for the proof

2A. $\mathbb{F}_p[G]$-modules and Minkowski units. Let $G$ be a finite group, a $p$-group in our situation. We record a few basic facts about finitely generated $\mathbb{F}_p[G]$-modules $M$; see [Curtis and Reiner 1962, Section 62].

**Fact 2.1.** Any finitely generated $\mathbb{F}_p[G]$-module $M$ is isomorphic to $\mathbb{F}_p[G] \lambda \oplus N$ where $N$ is a torsion $\mathbb{F}_p[G]$-module (every $n \in N$ is a torsion element) and where $\lambda$ depends only on $M$. 

Proof. As free modules are clearly projective, Theorem 62.3 of [Curtis and Reiner 1962] implies they are injective. It follows immediately that if \( \mathbb{F}_p[G] \) is a submodule of an \( \mathbb{F}_p[G] \)-module \( M \), we have the \( \mathbb{F}_p[G] \)-module decomposition \( M = \mathbb{F}_p[G] \oplus M^{(1)} \). Apply the same argument to \( M^{(1)} \) and iterate until, at the \( \lambda \)-th stage there are no copies of \( \mathbb{F}_p[G] \) in \( M^{(\lambda)} \). Thus for every \( m_0 \in M^{(\lambda)} \) we have \( \mathbb{F}_p[G] \cdot m_0 \neq \mathbb{F}_p[G] \) and thus \( m_0 \) has nontrivial annihilator. The result is established. \( \square \)

Set \( T_G := \sum_{g \in G} g \). Denote by \( I_G \) the augmentation ideal of \( \mathbb{F}_p[G] \). For \( x \in M \) set \( \text{Ann}_G(x) := \{ \alpha \in \mathbb{F}_p[G] \mid \alpha \cdot x = 0 \} \). Let \( \{s_1, \ldots, s_{h^1(G)}\} \) be a system of minimal generators of \( G \). By Nakayama’s lemma and the fact that \( I_G/I_G^2 \cong G/G^p[G, G] \), \( I_G \) can be generated, as \( G \)-module, by the elements \( x_i := s_i - 1 \).

**Proposition 2.2.** With the \( x_i \) as above, let \( M = \mathbb{F}_p[G]^{h^1(G)} \) and \( x = (x_1, x_2, \ldots, x_{h^1(G)}) \in M \). Then \( \text{Ann}_G(x) = \mathbb{F}_p T_G \).

**Proof.** \( \text{Ann}_G(x) = \bigcap_i \text{Ann}_G(x_i) = \text{Ann}_G((x_i)_{i=1}^{h^1(G)}) = \text{Ann}_G(I_G) = \mathbb{F}_p T_G. \) \( \square \)

**Proposition 2.3.** Let \( M = \mathbb{F}_p[G]^{\lambda} \oplus N \) be a finitely generated \( \mathbb{F}_p[G] \)-module where \( N \) is torsion. Then \( T_G(M) \cong \mathbb{F}_p^\lambda \).

**Proof.** It is clear that \( T_G(\mathbb{F}_p[G]^{\lambda}) \cong \mathbb{F}_p^\lambda \). We now show \( T_G(N) = 0 \).

Let \( n \in N \) so \( \text{Ann}_G(n) \neq 0 \). Note that \( \text{Ann}_G(n) \subset \mathbb{F}_p[G] \) is a \( p \)-group stable under the action of the \( p \)-group \( G \) and thus has a fixed point. But it is easy to see the only fixed points of \( \mathbb{F}_p[G] \) are multiples of \( T_G \) so \( T_G \in \text{Ann}_G(n) \) as desired. \( \square \)

**Definition 2.4.** We say the tower \( L_p(k)/k \) with Galois group \( G \) has \( \lambda \) Minkowski units if, as \( \mathbb{F}_p[G] \)-modules, \( V_{L_p(k),C}/L_p(k)^{\times p} = \mathcal{O}_{L_p(k)}^\times \otimes \mathbb{F}_p \cong \mathbb{F}_p[G]^{\lambda} \oplus N \) where \( N \) is an \( \mathbb{F}_p[G] \)-torsion module.

**2B. Extensions ramified at a tame set of primes.** We recall a standard formula on the number of \( \mathbb{Z}/p \)-extensions of a number field with given tame ramification; see Section 11.3 of [Koch 2002] for a proof. Recall that for a field \( L \),

\[
\delta(L) = \begin{cases} 
0, & \mu_p \nsubseteq L, \\
1, & \mu_p \subseteq L.
\end{cases}
\]

**Proposition 2.5.** Let \( L \) be a number field, \( p \) a prime number and \( X \) a set of tame primes of \( L \) prime to \( p \). Then

\[
\dim H^1(G_{L,X}, \mathbb{Z}/p) = \dim(V_{L,X}/L^{\times p}) - r_1(L) - r_2(L) - \delta(L) + 1 + \sum_{v \in X} \delta(L_v).
\]

Our \( v \in X \) are always finite and have norm congruent to 1 mod \( p \) so \( \delta(L_v) = 1 \).

**Fact 2.6.** Let \( S \) be a set of tame primes of \( L \) as above. For each \( v \in S \) let \( F_v \in M(L) := \text{Gal}(\text{Gov}(L)/L(\mu_p)) \). If the set \( \{F_v, v \in S\} \) spans an \((#S - d)\)-dimensional subspace of \( M(L) \), then

\[
\dim H^1(G_{L,S}, \mathbb{Z}/p) = d + \dim H^1(G_{L,\emptyset}, \mathbb{Z}/p).
\]

When \( \mu_p \nsubseteq L \), \( F_v \) is only well-defined up to nonzero scalar multiplication.
Proof. In (2), as we vary \( X \) from \( \emptyset \) to \( S \), we are adding \( \sum_{v \in S} \delta(L_v) = \#S \) to the right side, but also subtracting \( \dim(V_{L,\emptyset}/L\times p) - \dim(V_{L,X}/L\times p) \) from the right side. This last quantity is \( \#S - d \). \( \square \)

**Fact 2.7.** Let \( L \) be a number field such that \( (\# \text{Cl}_L, p) = 1 \). Let \( L'/L \) be a \( \mathbb{Z}/p \)-extension exactly ramified at \( S = \{v_1, \ldots, v_r\} \) where the \( v_i \) are finite and tame. Then \( (\# \text{Cl}_{L'}, p) = 1 \) if and only if \( L'/L \) is the unique \( \mathbb{Z}/p \)-extension of \( L \) unramified outside \( S \). In particular, that is the case when \( |S| = 1 \).

**Proof.** Indeed, \( (\# \text{Cl}_{L'}, p) \neq 1 \) if and only if there exists an unramified \( \mathbb{Z}/p \)-extension \( H/L' \) such that \( H/L \) is Galois (use the fact the action of a \( p \)-group on a \( p \)-group always has fixed points). Observe that \( H/L \) cannot be cyclic of degree \( p^2 \) as all inertial elements of \( \text{Gal}(H/L) \) have order \( p \) and they would thus fix an unramified extension of \( L \), a contradiction. So \( \text{Gal}(H/L) \simeq \mathbb{Z}/p \times \mathbb{Z}/p \), and \( L \) has at least two disjoints \( \mathbb{Z}/p \)-extension unramified outside \( S \), also a contradiction. \( \square \)

Set \( \mathcal{B}_{L,S} = (V_{L,S}/L\times p)^\wedge \). Recall \( \mathcal{I}^2_{L,S} \) : \( \text{Ker}(H^2(G_S, \mathbb{Z}/p) \to \bigoplus_{v \in S} H^2(G_v, \mathbb{Z}/p)) \). **Fact 2.8** below is well-known; see Theorem 11.3 of [Koch 2002].

**Fact 2.8.** \( \mathcal{I}^2_{L,S} \to \mathcal{B}_{L,S} \).

Let \( \lambda_L \) be the number of Minkowski units in \( L_p(L)/L \).

**Fact 2.9.** If \( \mu_p \not\subset L \) then \( \lambda_L = r_1(L) + r_2(L) - 1 + h^1(G) - h^2(G) \). If \( \mu_p \subset L \) then \( \lambda_L \geq r_1(L) + r_2(L) - h^2(G) \).

This result is Theorem 2.9 of [Hajir et al. 2021], but we sketch the proof for the sake of keeping this paper self-contained.

**Proof.** Set \( G = \text{Gal}(L_p(L)/L) \). We consider two “norm maps” induced by the norm map on units \( \mathcal{O}^\times_{L_p(L)} \to \mathcal{O}^\times_L \):

- \( N_G \) sending \( \mathcal{O}^\times_{L_p(L)} \otimes \mathbb{F}_p \) to \( \mathcal{O}^\times_L/(\mathcal{O}^\times_L \cap (\mathcal{O}^\times_{L_p(L)})^p) \subset \mathcal{O}^\times_{L_p(L)} \otimes \mathbb{F}_p \).

- \( N'_G : \mathcal{O}^\times_{L_p(L)} \otimes \mathbb{F}_p \to \mathcal{O}^\times_L \otimes \mathbb{F}_p \).

One easily sees \( N'_G(\mathcal{O}^\times_{L_p(L)} \otimes \mathbb{F}_p) \to N_G(\mathcal{O}^\times_{L_p(L)} \otimes \mathbb{F}_p) \) and this is an isomorphism provided \( \mathcal{O}^\times_L \cap (\mathcal{O}^\times_{L_p(L)})^p = (\mathcal{O}^\times_L)^p \); in particular this is the case when \( \mu_p \not\subset L \); see Proposition 2.8 of [Hajir et al. 2021].

Write \( \mathcal{O}^\times_{L_p(L)} \otimes \mathbb{F}_p \simeq \mathbb{F}_p[G]^\times \oplus N \), where \( N \) is an \( \mathbb{F}_p[G] \)-torsion module. By Proposition 2.3 one has \( N_G(\mathcal{O}^\times_{L_p(L)} \otimes \mathbb{F}_p) \simeq \mathbb{F}_p[G]^\times \). Hence, when \( \mu_p \not\subset L \)

\[
\dim\left( \frac{\mathcal{O}^\times_L \otimes \mathbb{F}_p}{N'_G(\mathcal{O}^\times_{L_p(L)} \otimes \mathbb{F}_p)} \right) = \dim(\mathcal{O}^\times_L \otimes \mathbb{F}_p) - \lambda_L.
\]

When \( \mu_p \subset L \), note that the “difference” between the images of \( N_G \) and \( N'_G \) has \( p \)-rank at most \( \dim(\mathcal{O}^\times_L \cap \mathcal{O}^\times_{L_p(L)}^p)/\mathcal{O}^\times_L^p \) \( \leq h^1(G) \), so

\[
\dim\left( \frac{\mathcal{O}^\times_L \otimes \mathbb{F}_p}{N_G(\mathcal{O}^\times_{L_p(L)} \otimes \mathbb{F}_p)} \right) \geq \dim(\mathcal{O}^\times_L \otimes \mathbb{F}_p) - \lambda_L - h^1(G).
\]
To conclude, we use the well-known equality (see [Roquette 1967, Lemma 9])

\[ h^2(G) - h^1(G) = \dim \left( \frac{C^\times_k \otimes \mathbb{F}_p}{N^G_G(\mathcal{O}_{L_p(L)}^\times \otimes \mathbb{F}_p)} \right). \]

\[ \square \]

2C. **Solving the ramified embedding problem with one tame prime.** We start with our nonsplit exact sequence

\[ 1 \to \mathbb{Z}/p \to G' \to G \to 1. \] (3)

given by the element \( 0 \neq \varepsilon \in H^2(G, \mathbb{Z}/p) \).

We assume that \( G = \text{Gal}(L_p(k)/k) \).

Set \( S = \{v\} \) where \( v \) is a finite tame prime of \( k \). We first show the existence of a lift of \( G \) to \( G' \) in some \( k_S/k \) for certain \( v \) of \( k \). We call this solving the embedding problem (3) in \( k_S \).

Recall that \( \Pi^2_{k,S} \leftarrow \Gamma_{k,S} \) by Fact 2.8. Here \( \Pi^2_{k,\varnothing} \simeq H^2(G_{k,\varnothing}, \mathbb{Z}/p) \simeq H^2(G, \mathbb{Z}/p) \). Let \( \text{Inf}_S : H^2(G_{k,\varnothing}, \mathbb{Z}/p) \to H^2(G_{k,S}, \mathbb{Z}/p) \) be the inflation map. We have the commutative diagram:

\[
\begin{array}{ccc}
\Pi^2_{k,\varnothing} & \xrightarrow{\text{Inf}_S} & \Pi^2_{k,S} \\
\downarrow^{h} & & \downarrow^{g} \\
(k_v^\times \otimes \mathbb{F}_p)^\wedge & \xrightarrow{f_S} & \Gamma_{k,\varnothing} \\
\end{array}
\]

By Hoeschmann’s criteria (see [Neukirch et al. 2008, Chapter 3, Section 5]), the embedding problem has a solution in \( k_S \) if and only if \( \text{Inf}_S(\varepsilon) = 0 \). As \( L_p(k)/k \) is unramified, \( \text{Inf}_S(\varepsilon) \in \Pi^2_{k,S} \) and as \( g(\text{Inf}_S(\varepsilon)) = f_S(h(\varepsilon)) \in \Gamma_{k,S}, \) the embedding problem has a solution if and only if \( h(\varepsilon) \in \text{Ker}(f_S) \).

Set \( \text{Gov}_S(k) := k(\mu_p)(\sqrt[3]{k,S}) \). In the governing extensions \( k(\mu_p) \subset \text{Gov}_S(k) \subset \text{Gov}(k) \), one sees that the kernel of the map \( f_S : \Gamma_{k,\varnothing} \to \Gamma_{k,S} \) is exactly the (unramified) decomposition group \( D_v \) of the prime \( v \). As noted in Fact 2.6, if \( w_1, w_2 \mid v \) are two primes of \( k(\mu_p) \), their Frobenius elements in \( \text{Gal}(\text{Gov}(k)/k(\mu_p)) \) differ by a nonzero scalar multiple.

We have proved:

**Lemma 2.10.** The embedding problem (3) has a solution in \( k_S/k \) if and only if \( h(\varepsilon) \in D_v \). Thus it has a solution in \( k_S/k \) if we choose the prime \( v \) such that \( (\text{Fr}_v) = (h(\varepsilon)) \) in \( M(k) \), that is the lines spanned by these elements in \( M(k) \) are equal. This is always possible by Chebotarev’s theorem.

2D. **Cohomological facts implying the persistence of Minkowski units.** Our main aim in this paper is to show that given a short exact sequence

\[ 1 \to \mathbb{Z}/p \to G' \to G \to 1 \]

of finite \( p \)-groups where \( G = \text{Gal}(L_p(k)/k) \), there exists a finite tamely ramified extension \( k'/k \) with \( G' = \text{Gal}(L_p(k')/k') \). To solve this embedding problem using Theorem 3.3, the tower \( L_p(k)/k \) must have \( 2h^1(G) \) Minkowski units. Proposition 2.14 below shows that if we start with enough Minkowski units, after a base change that realizes \( G' \), we will be able to continue the induction. Proposition 2.13, which is
only needed in the case when \( \mu_p \subset k \), shows that given at least \( h^1(G) \) Minkowski units, we can perform a base change that preserves the tower and the number of Minkowski units increases. Proposition 2.11 is a basic group theory result bounding \( h^1(G') \) and \( h^2(G') \) in terms of \( h^1(G) \) and \( h^2(G) \). Furuta proves a similar result in Lemma 2 of [Furuta 1972].

Set \( H^2(G', \mathbb{Z}/p)_1 := \ker(H^2(G', \mathbb{Z}/p) \xrightarrow{\text{Res}} H^2(\mathbb{Z}/p, \mathbb{Z}/p)) \) and \( h^2(G')_1 := \dim H^2(G', \mathbb{Z}/p)_1 \). Note \( h^2(\mathbb{Z}/p) = 1 \) so \( h^2(G')_1 \) is either \( h^2(G') \) or \( h^2(G') - 1 \) and in either case \( h^2(G')_1 \geq h^2(G') - 1 \).

**Proposition 2.11.** Let
\[
1 \to \mathbb{Z}/p \to G' \to G \to 1
\]
be a short exact sequence of finite \( p \)-groups. Then \( h^1(G') \leq h^1(G) + 1 \) and \( h^2(G') \leq h^1(G) + h^2(G) + 1 \).

**Proof.** The \( h^1 \) result is clear. For the \( h^2 \) statement we have the long exact sequence (see for instance [Dekimpe et al. 2012])
\[
0 \to H^1(G, \mathbb{Z}/p) \to H^1(G', \mathbb{Z}/p) \to H^1(\mathbb{Z}/p, \mathbb{Z}/p)^G
\to H^2(G, \mathbb{Z}/p) \to H^2(G', \mathbb{Z}/p)_1 \to H^1(G, H^1(\mathbb{Z}/p, \mathbb{Z}/p)).
\]
If \( G' \to G \) splits, we have
\[
0 \to H^2(G, \mathbb{Z}/p) \to H^2(G', \mathbb{Z}/p)_1 \to H^1(G, H^1(\mathbb{Z}/p, \mathbb{Z}/p))
\]
so \( h^2(G')_1 \leq h^2(G) + h^1(G) \) and since \( h^2(G')_1 \geq h^2(G') - 1 \) the result follows.

In the nonsplit case we have
\[
0 \to H^1(\mathbb{Z}/p, \mathbb{Z}/p)^G \to H^2(G, \mathbb{Z}/p) \to H^2(G', \mathbb{Z}/p)_1 \to H^1(G, H^1(\mathbb{Z}/p, \mathbb{Z}/p))
\]
so \( h^2(G')_1 \leq h^2(G) - 1 + h^1(G) \) so \( h^2(G') \leq h^1(G) + h^2(G) \).

**Definition 2.12.** For a number field \( L \) set \( G = \text{Gal}(L_p(L)/L) \). Define \( f \) as follows:
\[
f(L) = \begin{cases} r_1(L) + r_2(L) - h^2(G) + h^1(G) - 1, & \mu_p \not\subset L, \\
r_1(L) + r_2(L) - h^2(G), & \mu_p \subset L. \end{cases}
\]
Fact 2.9 implies \( f(L) \) is a lower bound on the number of Minkowski units of \( L_p(L)/L \).

**Proposition 2.13.** Let \( \tilde{k}/k \) be a \( \mathbb{Z}/p \)-extension ramified at finite tame primes such that \( G = \text{Gal}(L_p(k)/k) = \text{Gal}(L_p(\tilde{k})/\tilde{k}) \). Then \( f(\tilde{k}) = f(k) + (p - 1)(r_1(k) + r_2(k)) \).

**Proof.** This follows immediately as we have the same group \( G \) for \( k \) and \( \tilde{k} \), \( \mu_p \subset \tilde{k} \iff \mu_p \subset k \) and \( r_i(\tilde{k}) = p \cdot r_i(k) \).

**Proposition 2.14.** Let \( k'/k \) be a tamely ramified \( \mathbb{Z}/p \)-extension such that \( G = \text{Gal}(L_p(k)/k) \) and \( G' = \text{Gal}(L_p(k')/k') \) where
\[
1 \to \mathbb{Z}/p \to G' \to G \to 1.
\]
Let \( f(k) \) be as in **Definition 2.12.** Then
\[
f(k) \geq 2h^1(G) + 3 \iff f(k') \geq 2h^1(G') + 3.
\]
Proof. We do the case $\mu_p \not\subset k$ first. We need to prove
\[ r_1(k) + r_2(k) - h^2(G) + h^1(G) - 1 \geq 2h^1(G) + 3 \implies r_1(k') + r_2(k') - h^2(G') + h^1(G') - 1 \geq 2h^1(G') + 3, \]
that is
\[ r_1(k') + r_2(k') \geq h^1(G') + h^2(G') + 4. \]
Clearly
\[ r_1(k') + r_2(k') = p(r_1(k) + r_2(k)) \geq p(h^1(G) + h^2(G) + 4) \]
and by Proposition 2.11 we have
\[ h^2(G') + h^1(G') + 4 \leq (h^1(G) + h^2(G) + 1) + (h^1(G) + 1) + 4 = 2h^1(G) + h^2(G) + 6 \]
so it suffices to show
\[ (p - 1)h^2(G) + (p - 2)h^1(G) + 4p \geq 6. \]
This holds for all $p$.
When $\mu_p \subset k$. We need to prove
\[ r_1(k) + r_2(k) - h^2(G) \geq 2h^1(G) + 3 \implies r_1(k') + r_2(k') - h^2(G') \geq 2h^1(G') + 3, \]
that is
\[ r_1(k') + r_2(k') \geq 2h^1(G') + h^2(G') + 3. \]
Again using Proposition 2.11 and that $r_i(k') = p \cdot r_i(k)$ it suffices to show
\[ (p - 1)h^2(G) + (2p - 3)h^1(G) + 3p \geq 6 \]
which holds for all $p$. \qed

Proposition 2.15 below provides the base case of the induction.

Proposition 2.15. Recall $(\# \text{Cl}_{k_0}, p) = 1$. There exists a tamely ramified extension $k'/k_0$ such that

- the $p$-part of the class group of $k'$ is $\mathbb{Z}/p$,
- $[k' : k_0] = p^3$,
- and $f(k') > 2h^1(\mathbb{Z}/p) + 3 = 5$.

Proof. Since $L_p(k_0) = k_0$, we see $G = \{e\}$. Choose a tame prime $v$ of $k$ whose Frobenius is trivial in the governing Galois group $M(k)$. By Fact 2.6 there is a unique $\mathbb{Z}/p$-extension $k_1/k_0$ unramified outside $v$. That $(\# \text{Cl}_{k_1}, p) = 1$ follows from Fact 2.7. Repeat this process with $k_1$ to get a field $k_2$ with $(\# \text{Cl}_{k_2}, p) = 1$.

We do one more base change to find a field $k'$ with class group $\mathbb{Z}/p$. This is proved more generally as part of Theorem 3.3, but we include a short proof here.

Choose $v_1$ a finite tame prime of $k_2$ with trivial Frobenius in $M(k_2)$ so that by Fact 2.6 there exists a unique $D_1/k_2$ ramified at $v_1$. As $D_1 \cap \text{Gov}(k_2) = k_2$, we may choose $v_2$ a finite tame prime of $k_2$ with
trivial Frobenius in \( \text{Gov}(k_2) \) such that \( v_2 \) remains prime in \( D_1/k_2 \). Again by Fact 2.6 there exists a unique \( D_2/k_2 \) ramified at \( v_2 \).

Let \( D/k_2 \) be any of the \( p - 1 \) “diagonal” \( \mathbb{Z}/p \)-extensions of \( k_2 \) between \( D_1 \) and \( D_2 \) so \( D_1 D_2/D \) is everywhere unramified. We claim \( D_1 D_2 = L_p(D) \). Indeed, by Fact 2.7 applied to \( D_1/k_2 \) we see \((#\text{Cl}_{D_1}, p) = 1 \). As \( v_2 \) is inert in \( D_1/k_2 \), the extension \( D_2 D_1/D_1 \) is ramified only at \( v_2 \) and Fact 2.7 applied to \( D_2 D_1/D_1 \) implies \((#\text{Cl}_{D_1 D_2}, p) = 1 \). Whether or not \( \mu_p \subset k_0 \), we have \( k' := D_1 \text{Cl}_k[p^\infty] = \mathbb{Z}/p \) and

\[
 f(k') \geq r_1(k') + r_2(k') - h^2(\mathbb{Z}/p) = p^3 r_1(k_0) + p^3 r_2(k_0) - 1 > 5 = 2h^1(\mathbb{Z}/p) + 3.
\]

\( \square \)

Depending on \( p \) and the signature of \( k_0 \) one can decrease the number of base changes, but this analysis complicates the statement of the main theorem without significant gain.

3. Solving the embedding problem

Having established the base case of our induction, we now prove Theorem 3.3.

**Inductive Step.** Let

\[
 1 \to \mathbb{Z}/p \to G' \to G \to 1
\]

be exact and let \( k \) be a number field with \( \text{Gal}(L_p(k)/k) = G \) and \( f(k) \geq 2h^1(G) + 3 \). Then there exists a number field \( k'/k \) with \( \text{Gal}(L_p(k'/k') = G' \) and \( f(k') \geq 2h^1(G') + 3 \).

Theorem 3.2 below is only necessary for the key inductive step, Theorem 3.3, when \( \mu_p \subset k \).

Set \( K := L_p(k)(\mu_p) \). We only consider finite tame primes \( v \) of \( k \) that split completely in \( K/k \). When \( \mu_p \not\subset k \), our Frobenius elements in governing fields (or their subfields) are only defined up to scalar multiples. We write \( \langle \text{Fr}_v \rangle_{\text{Gov}(k)/k(\mu_p)} \) for the well-defined line spanned by Frobenius at \( v \) in \( \text{Gal}(\text{Gov}(k)/k(\mu_p)) \). When the Frobenius is trivial there is no ambiguity so we write \( \langle \text{Fr}_v \rangle_{\text{Gov}(k)/k(\mu_p)} = 0 \).

We need primes \( v \) of \( k \) that let us control \( h^1(\text{Gal}(k_v/k)) \) and \( h^1(\text{Gal}(L_p(k_v)/L_p(k)(\mu_p))) \) simultaneously via Fact 2.6. Recall \( M(\text{L}_p(k)) := \text{Gal}(\text{Gov}(L_p(k)/L_p(k)(\mu_p))) \cong \mathbb{F}_p[G]^{\pm 1} \oplus N \) where \( N \) is a torsion module over \( \mathbb{F}_p[G] \). We have no knowledge of \( N \) and must work with the free part to control things over \( L_p(k) \). We then use Proposition 3.1 to control things over \( k \).

3A. The stability theorem.

**Proposition 3.1.** Let \( F \subset \text{Gov}(L_p(k)) \) be the field fixed by \( I_G \cdot M(L_p(k)) \). For \( v \) of \( k \) splitting completely in \( K \) and \( w \mid v \) in \( K \), the lines \( \langle \text{Fr}_w \rangle_F/K \) do not depend on \( w \) so we may write \( \langle \text{Fr}_v \rangle_F/K \). Then \( \langle \text{Fr}_v \rangle_F/K = \langle \text{Fr}_v \rangle_{\text{Gov}(k)/k(\mu_p)} \) implies \( \langle \text{Fr}_v \rangle_{\text{Gov}(k)/k(\mu_p)} = \langle \text{Fr}_v \rangle_{\text{Gov}(k)/k(\mu_p)} \). If \( \langle \text{Fr}_v \rangle_F/K = 0 \) then \( \langle \text{Fr}_v \rangle_{\text{Gov}(k)/k(\mu_p)} = 0 \).
Proof. This diagram is useful in Theorems 3.2 and 3.3 as well:

\[
\begin{array}{c}
\text{Gov}(L_p(k)) \\
M(L_p(k)) \ar{u} \\
F \ar{l} \\
I_G \cdot M(L_p(k)) \\
\text{Gov}(k) \ar{l} \\
\Delta \ar{l} \\
L_p(k) \ar{l} \\
\Delta \ar{u} \\
k(\mu_p) \ar{l} \\
k \ar{l} \\
\end{array}
\]

Let \( \Delta = \text{Gal}(k(\mu_p)/k) = \text{Gal}(K/L_p(k)) \). As \( \text{Gal}(F/K) := M(L_p(k))/I_G \cdot M(L_p(k)) \) is the maximal quotient of \( M(L_p(k)) \) on which \( G \) acts trivially, and \( \Delta \) acts on \( \text{Gal}(F/K) \) by scalars, the line \( (\text{Fr}_w)_{F/K} \) is invariant under the action of \( \text{Gal}(K/k) = G \times \Delta \). Since the \( w | v \) form an orbit under this action of \( \text{Gal}(K/k) \), this line is independent of the choice of \( w | v \) as desired.

As \( \text{Gov}(k)K/K \) ascends from \( \text{Gov}(k)/k(\mu_p) \), we see \( G \) acts trivially on \( \text{Gal}(\text{Gov}(k)K/K) \) so \( \text{Gov}(k)K \subset F \).

Below, we implicitly use that our primes of \( k \) split completely in \( K \). If \((\text{Fr}_{v_1})_{F/K} = (\text{Fr}_{v_2})_{F/K} \), these lines are equal when projected to \( \text{Gal}(\text{Gov}(k)K/K) \subset \text{Gal}(\text{Gov}(k)k(\mu_p)) \) and they are again equal in \( \text{Gal}(\text{Gov}(k)/k(\mu_p)) \) so \( (\text{Fr}_{v_1})_{\text{Gov}(k)/k(\mu_p)} = (\text{Fr}_{v_2})_{\text{Gov}(k)/k(\mu_p)} \). The last statement is clear. \( \square \)

Theorem 3.2. Recall \( \{x_i\}_{i=1}^{h^1(G)} \) is a minimal set of generators of \( I_G \). Assume that \( f(k) \geq h^1(G) \). Let \( w \) be a degree one prime of \( K \) such that

\[
\text{Fr}_w = ((x_1, x_2, \ldots, x_{h^1(G)}, 0, \ldots, 0), 0) \in M(L_p(k)) \simeq \mathbb{F}_p[G]^{h^1(G)} \oplus N.
\]

Then for \( v \) of \( k \) below \( w \),

\[
(\text{Fr}_v)_{\text{Gov}(k)/k(\mu_p)} = 0
\]

so there exists a \( \mathbb{Z}/p \)-extension \( \tilde{k}/k \) ramified at only \( v \). Furthermore,

\[
L_p(\tilde{k}) = L_p(k)\tilde{k} \quad \text{and} \quad f(\tilde{k}) > f(k).
\]

Proof: As \( \text{Fr}_w \) projects to 0 in the \( \mathbb{F}_p \)-vector space \( \text{Gal}(F/K) \), \text{Proposition 3.1} implies \( (\text{Fr}_v)_{\text{Gov}(k)/k(\mu_p)} = 0 \) so \( \tilde{k} \) exists by \text{Fact 2.6}. We show the \( \mathbb{F}_p[G] \)-span of \((x_1, \ldots, x_{h^1(G)}) \in \mathbb{F}_p[G]^{h^1(G)} \) has dimension \( \#G - 1 \).
by computing the dimension of $\bigcap_{i=1}^{h^1(G)} \Ann(x_i)$. This intersection is the annihilator of $I_G$ which by Proposition 2.2 is just $\mathbb{F}_p T_G$, establishing our dimension result. By Fact 2.6 there is a unique extension over $L_p(k)$ ramified at $v$ and thus it must be $L_p(k)\tilde{k}$. Fact 2.7 applied to $L_p(k)\tilde{k}/L_p(k)$ implies $(\#\Cl_{L_p(k)\tilde{k}}, p) = 1$ so

$$L_p(\tilde{k}) = L_p(k)\tilde{k}.$$  

Proposition 2.13 gives

$$f(\tilde{k}) > f(k).$$

3B. The inductive step.

**Theorem 3.3.** Assume that $L_p(k)/k$ has $\lambda_k \geq 2h^1(G) + 3$ Minkowski units. Let $1 \to \mathbb{Z}/p \to G' \to G \to 1$. If the extension splits or $\mu_p \not\subseteq k$, there exists a $\mathbb{Z}/p$-extension $k'/k$ such that $\Gal(L_p(k')/k') \simeq G'$ and $L_p(k')/k'$ has at least $2h^1(G') + 3$ Minkowski units. If $\mu_p \subseteq k$ and the extension is nonsplit, $k'$ can be realized as a compositum of two successive $\mathbb{Z}/p$-extensions and $L_p(k')/k'$ has at least $2h^1(G') + 3$ Minkowski units.

**Proof.** Recall that our finite tame primes split completely in $K/k$. We first treat the split case. This is independent of whether or not $\mu_p \subseteq k$.

**Split case.** Choose tame degree one primes $w_1$ and $w_2$ of $\Gov(k)K$ such that

- $\Fr_{w_1} = ((x_1, x_2, \ldots, x_{h^1(G)}, 0, \ldots, 0), 0) \in \Gal(\Gov(L_p(k))/\Gov(k)K) \subset M(L_p(k))$. This is possible as the tuple lies in $I_G \cdot M(L_p(k))$ and $\Gov(k)K \subset F$. As $\Fr_{w_1}$ projects to 0 in $\Gal(F/K)$, we see for $v_1$ of $k$ below $w_1$ that $\langle \Fr_{v_1} \rangle F/K \subseteq 0$ so by Proposition 3.1 $\langle \Fr_{v_1} \rangle \Gov(k)(k(\mu_p)) = 0$. By Fact 2.6 applied to $k$ there is one $\mathbb{Z}/p$-extension $D_1/k$ ramified at $v_1$. Fact 2.6 also gives (see the proof of Theorem 3.2 as well) a unique $\mathbb{Z}/p$-extension of $L_p(k)$ ramified at $v_1$, namely $D_1L_p(k)/L_p(k)$.

- $\Fr_{w_2} = ((0, 0, \ldots, 0, h^1(G), x_1, x_2, \ldots, x_{h^1(G)}, 0, 0, 0, \ldots, 0), 0)$ so for $v_2$ of $k$ below $w_2$, $\langle \Fr_{v_2} \rangle F/K = 0$. We also insist that $v_2$ remains prime in $D_1/k$. This last condition is linearly disjoint from the rest of the defining splitting conditions on $v_2$ and imposes no contradiction. Again, there are unique $\mathbb{Z}/p$-extensions of both $k$ and $L_p(k)$ ramified at $v_2$, namely $D_2/k$ and $D_2L_p(k)/L_p(k)$. Let $D/k$ be a “diagonal” extension between $D_1$ and $D_2$ ramified at both $v_1$ and $v_2$. There are $p - 1$ of these.

Fact 2.6 and our choices of the Frobenius elements of $v_1$ and $v_2$ imply

$$h^1(\Gal(L_p(k)_{v_1,v_2}/L_p(k))) = 2$$

using that the span of the Frobenius elements above them in $\Gal(\Gov(L_p(k))/\Gov(k)K) \subset M(L_p(k))$ has dimension $2\#G - 2$ and Fact 2.6. (With only $h^1(G)$ Minkowski units, we would again have had

$$h^1(\Gal(L_p(k)_{v_1}/L_p(k))) = h^1(\Gal(L_p(k)_{v_2}/L_p(k))) = 1.$$
In this case the span of the Frobenius elements above \{v_1, v_2\} in \text{Gal}(\text{Gov}(L_p(k)) / \text{Gov}(k) K) \subset M(L_p(k)) would have been \#G - 1 so by Fact 2.6, \(h^1(\text{Gal}(L_p(k)_{\{v_1,v_2\}}/L_p(k)))\) would have been \(2\#G - (\#G - 1) = \#G + 1\).

Set \(L := D_1D_2L_p(k), J := D_1L_p(k)\) and note \(L/D\) is unramified as \(D/k\) has absorbed all ramification at \(\{v_1, v_2\}\). We will solve the problem by showing \((\#\text{Cl}_{D_1D_2L_p(k)}, p) = 1\).

Since \((\#\text{Cl}_{L_p(k)}, p) = 1\) and our choice of \(v_1\) is such that

\[h^1(\text{Gal}(L_p(k)_{\{v_1\}}/L_p(k))) = 1,\]

Fact 2.7 applied to \(J/L_p(k)\) implies \((\#\text{Cl}_J, p) = 1\).

We now prove that there exists a unique \(\mathbb{Z}/p\)-extension over \(J\) unramified outside \(v_2\), namely \(L\). Set \(\Omega = \text{Gal}(J/L_p(k))\), \(J_{p,\text{el}}^{v_2}\) to be the maximal elementary \(p\)-abelian extension of \(J\) inside \(J_{\{v_2\}}\), and \(\Pi = \text{Gal}(J_{p,\text{el}}^{v_2}/J)\). Then \(\Omega\) acts on \(\Pi\) and trivially on \(\text{Gal}(L/J)\). We claim this is the only \(\mathbb{Z}/p\)-extension of \(J\) in \(J_{p,\text{el}}^{v_2}/J\) on which \(\Omega\) acts trivially: If not, there exists another \(\mathbb{Z}/p\)-extension \(H/J\) unramified outside \(v_2\) and Galois over \(L_p(k)\). Hence \(\text{Gal}(H/L_p(k))\) has order \(p^2\) and is abelian. The extension \(H/L_p(k)\) cannot be cyclic because all inertia elements have order \(p\) and would then fix an everywhere unramified extension of \(L_p(k)\), a contradiction. Suppose now that \(\text{Gal}(H/L_p(k)) \simeq \mathbb{Z}/p \times \mathbb{Z}/p\), with \(H \neq JD_2 = L\). Then \(\text{Gal}(HD_2/L_p(k)) \simeq (\mathbb{Z}/p)^3\): this contradicts the already established fact that \(h^1(\text{Gal}(L_p(k)_{\{v_1,v_2\}}/L_p(k))) = 2\).

The final possibility is that there exists a \(\mathbb{Z}/p\)-extension \(E_0/J\) unramified outside \(v_2\), different from \(L/J\) and not fixed by \(\Omega\); let \(S_0\) be the set of ramification of \(E_0/J\). As primes above \(v_2\) in \(L_p(k)\) are inert in \(J/L_p(k)\), \(\Omega(S_0) = S_0\): then \(\Omega\) takes \(E_0\) to another \(\mathbb{Z}/p\)-extension \(E_1/J\) exactly ramified at \(S_0\) and such that \(E_1 \neq E_0\). The compositum \(E_1E_0/J\) contains a \(\mathbb{Z}/p\)-extension \(E_0'/J\) exactly ramified at a set \(S'_0 \subsetneq S_0\). Observe that \(E_0' \neq L\) since \(L/J\) is totally ramified at every prime above \(v_2\). Continuing the process, we obtain an unramified \(\mathbb{Z}/p\)-extension \(H/J\), which is impossible since \((\#\text{Cl}_J, p) = 1\). Thus \(L/J\) is the unique \(\mathbb{Z}/p\)-extension unramified outside \(v_2\). Fact 2.7 applied to \(L/J\) implies \((\#\text{Cl}_L, p) = 1\).
We have solved the split embedding problem with \( k' = D \) and \( \text{Gal}(L_p(k')/k') = G \times \mathbb{Z}/p \). It required one base change ramified at two tame finite primes. \textbf{Proposition 2.14} implies \( f(k') \geq 2h^1(G') + 3 \) so the induction can proceed.

For the nonsplit case we treat \( \mu_p \not\subset k \) and \( \mu_p \subset k \) separately. \textbf{Theorem 3.2} is only used in the nonsplit case when \( \mu_p \subset k \).

The nonsplit case, \( \mu_p \not\subset k \). By \textbf{Lemma 2.10} we may use one tame prime \( v \) of \( k \) to find a \textit{ramified} solution to the embedding problem. As \( \mu_p \not\subset k \) implies \( \text{Gov}(k) \cap L_p(k) = k \), we can assume \( v \) splits completely in \( K/k \). Choosing any \( w \mid v \) of \( K \) we set \( \text{Fr}_w = ((z_1, z_2, \ldots, z_{\lambda_k}), n_0) \in M(L_p(k)) \) where we claim \( n_0 \notin I_G \cdot N \) and \( z_i \in I_G \subset \mathbb{F}_p[G] \). Indeed, if any \( z_i \notin I_G \), its \( \mathbb{F}_p[G] \)-span is all of \( \mathbb{F}_p[G] \) and by \textbf{Fact 2.6} there is no \( \mathbb{Z}/p \)-extension of \( L_p(k) \) ramified at the \( w \mid v \), contradicting that we are solving an embedding problem with \( v \). If \( n_0 \in I_G \cdot N \), then the projection of \( \text{Fr}_w \) to \( \text{Gal}(F/K) \) is trivial so \textbf{Proposition 3.1} implies 
\[
\langle \text{Fr}_v \rangle_{\text{Gov}(k)/k(\mu_p)} = 0
\]
and the embedding problem we are solving is split, also a contradiction.

Choose a degree one \( w_1 \) of \( K \) with \( \text{Fr}_{w_1} = ((x_1, x_2, \ldots, x_{h^1(G)}), 0, 0, 0, \ldots, 0), n_0) \in M(L_p(k)) \) where \( n_0 \) is as in the previous paragraph. Let \( v_1 \) be the prime of \( k \) below \( w_1 \). By \textbf{Fact 2.6} (also see the proof of \textbf{Theorem 3.2}) there is one \( \mathbb{Z}/p \)-extension \( D_1/L_p(k) \) ramified at \( v_1 \).

Choose a degree one \( w_2 \) of \( K \) with \( \text{Fr}_{w_2} = ((0, 0, \ldots, 0, x_1, x_2, \ldots, x_{h^1(G)}), 0, 0, 0, \ldots, 0), n_0) \in M(L_p(k)) \) and the primes of \( L_p(k) \) above \( v_2 \) remain prime in \( D_1/L_p(k) \). This last condition is linearly disjoint from the splitting conditions defining \( v_2 \) and imposes no contradiction. Again by \textbf{Fact 2.6} there is one \( \mathbb{Z}/p \)-extension \( D_2/L_p(k) \) ramified at \( v_2 \).

As the free components of \( \text{Fr}_w, \text{Fr}_{w_1} \) and \( \text{Fr}_{w_2} \) are all in \( I^k_G \), their projections to \( \text{Gal}(F/K) \) depend only on \( n_0 \) and \textbf{Proposition 3.1} implies
\[
0 \neq \langle \text{Fr}_v \rangle_{\text{Gov}(k)/k(\mu_p)} = \langle \text{Fr}_{v_1} \rangle_{\text{Gov}(k)/k(\mu_p)} = \langle \text{Fr}_{v_2} \rangle_{\text{Gov}(k)/k(\mu_p)}.
\]

Thus there is no extension of \( k \) ramified at either \( v_1 \) or \( v_2 \), but, by \textbf{Fact 2.6}, there is a \( \mathbb{Z}/p \)-extension of \( k \) ramified at \( \{v_1, v_2\} \). Call it \( D \). Note \( G' \cong \text{Gal}(D_1/k) \cong \text{Gal}(D_2/k) \cong \text{Gal}(D_1D_2/D) \):

That \( D_1D_2 \) has trivial \( p \)-class group follows exactly as it did in the split case and we may set \( k' = D \) so \( L_p(k') = D_1D_2 \) and \( \text{Gal}(L_p(k')/k') \cong G' \).
We have solved the embedding problem in the nonsplit case when \( \mu_p \not\subset k \). We performed one base change at two tame finite primes and Proposition 2.14 implies \( f(k') \geq 2 h^1(G') + 3 \) so the induction can proceed.

**The nonsplit case, \( \mu_p \subset k \).** We can no longer assume \( L_p(k) \cap \text{Gov}(k) = k \).

Let \( 0 \neq \varepsilon \in \mathbb{H}_k^2 \) be the obstruction to our embedding problem \( G' \hookrightarrow G \). Using Lemma 2.10, let \( v \) of \( k \) be a tame prime annihilating \( \varepsilon \). The difficulty is that in the diagram below we may have \( L_p(k) \cap \text{Gov}(k) \not\supset k \) and that \( \text{Fr}_v \), which is necessarily nonzero in \( M(k) \), may also be nonzero in \( \text{Gal}((L_p(k) \cap \text{Gov}(k))/k) \).

This prevents us from also choosing \( v \) to split completely in \( L_p(k)/k \) and as we need in \( \text{Gov}(L_p(k))/L_p(k) \) to ensure there is only one extension of \( L_p(k) \) ramified at the primes of \( L_p(k) \) above \( v \). If we could choose \( v \) to annihilate \( \varepsilon \) such that \( \text{Fr}_v = 0 \in \text{Gal}(L_p(k)/k) \), we would be able to proceed as in the \( \mu_p \not\subset k \) case. We get around this by a base change.

By Kummer theory and the definition of governing fields, \( \text{Gal}(\text{Gov}(L)/L(\mu_p)) \) is an elementary \( p \)-abelian group. Let \( \tilde{k}/k \) be a tamely ramified \( \mathbb{Z}/p \)-extension as given by Theorem 3.2 so \( \text{Gal}(L_p(\tilde{k})/\tilde{k}) = G \). By Proposition 2.13 we have \( \lambda_{\tilde{k}} \geq 2 h^1(G) + 3 \):

As \( \text{Gov}(k) \cap \tilde{k} = k \), we may choose a prime \( v \) to solve the embedding problem for \( k \) whose Frobenius is nontrivial in \( \text{Gal}(\tilde{k}/k) \), that is \( v \) remains prime in \( \tilde{k}/k \). As observed above, \( L_p(\tilde{k}) \cap \text{Gov}(\tilde{k})/k \) is a \((\mathbb{Z}/p)^r\)-extension for some \( r \) and, as \( \text{Gal}(L_p(k)/k) = \text{Gal}(L_p(\tilde{k})/\tilde{k}) = G \), it is the base change of such a subextension of \( L_p(k)/k \) from \( k \) so \( L_p(\tilde{k}) \cap \text{Gov}(\tilde{k})/k \) is a \((\mathbb{Z}/p)^{r+1}\)-extension. Since \( v \) remains prime in \( \tilde{k}/k \) and residue field extensions are cyclic, it splits completely in \( L_p(\tilde{k}) \cap \text{Gov}(\tilde{k})/\tilde{k} \). As the embedding problem is solvable over \( k \) by allowing ramification at \( v \), it is also solvable over \( \tilde{k} \) by allowing ramification at the unique prime of \( \tilde{k} \) above \( v \). Thus \( \varepsilon \in \mathbb{H}_k^2 \leftrightarrow \mathbb{D}_{\tilde{k},\emptyset} = M(\tilde{k}) \) actually lies in \( \text{Gal}(\text{Gov}(\tilde{k})/(L_p(\tilde{k}) \cap \text{Gov}(\tilde{k}))) \). The base change shifted the obstruction to outside of our \( p \)-Hilbert class field tower! The rest of the proof is identical to the \( \mu_p \not\subset k \) case.

We now prove the main theorem of the introduction.

**Proof:** We have verified the base case of the induction in Proposition 2.15 and the inductive step with Theorem 3.3. It remains to count degrees and ramified primes. Proposition 2.15 involved three \( \mathbb{Z}/p \)-base
changes, the first two ramified at one tame prime and the last at two tame primes. The inductive steps breaks into cases as follows:

- $\mu_p \not\subset k_0$: At each of the $\log_p(\#\Gamma) - 1$ inductive stages we need one base change ramified at two primes for a total of $3 + (\log_p(\#\Gamma) - 1)$ base changes ramified at $4 + 2(\log_p(\#\Gamma) - 1)$ primes.

- $\mu_p \subset k_0$: At each of the $\log_p(\#\Gamma) - 1$ inductive stages we need at most two base changes and at most three ramified tame primes so in total there are at most $3 + 2(\log_p(\#\Gamma) - 1)$ base changes ramified at most $4 + 3(\log_p(\#\Gamma) - 1)$ primes.

\[\square\]

References


Communicated by Melanie Matchett Wood
Received 2022-04-18 Revised 2023-04-03 Accepted 2023-05-29

Farshid Hajir, Christian Maire and Ravi Ramakrishna

Department of Mathematics and Statistics, University of Massachusetts, Amherst, MA, United States

FEMTO-ST Institute, Universite Bourgogne Franche-Comté, CNRS, Besançon, France

Department of Mathematics, Cornell University, Ithaca, NY, United States
See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2024 is US $525/year for the electronic version, and $770/year (+$65, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

© 2024 Mathematical Sciences Publishers
Fundamental exact sequence for the pro-étale fundamental group
Marcin Lara 631

Infinitesimal dilogarithm on curves over truncated polynomial rings
Sinan Ünver 685

Wide moments of L-functions I: Twists by class group characters of imaginary quadratic fields
Asbjørn Christian Nordentoft 735

On Ozaki’s theorem realizing prescribed p-groups as p-class tower groups
Farshid Hajir, Christian Maire and Ravi Ramakrishna 771

Supersolvable descent for rational points
Yonatan Harpaz and Olivier Wittenberg 787

On Kato and Kuzumaki’s properties for the Milnor K_2 of function fields of p-adic curves
Diego Izquierdo and Giancarlo Lucchini Arteche 815