ON OZAKI'S THEOREM REALIZING PRESCRIBED p-GROUPS AS p-CLASS TOWER GROUPS

by

Farshid Hajir, Christian Maire, Ravi Ramakrishna

Abstract. — We give a streamlined and effective proof of Ozaki's theorem that any finite p-group Γ 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 $[\mathrm{F} : \mathrm{k}_0]$ and the number of ramified primes of F/k_0 in terms of $\#\Gamma$.

1. Introduction

For a number field k, define $\mathrm{L}_p(\mathrm{k})$ to be the compositum of all finite unramified Galois p-extensions of k. The extension $\mathrm{L}_p(\mathrm{k})/\mathrm{k}$ is called the p-Hilbert class field tower of k, and its Galois group $\mathrm{Gal}(\mathrm{L}_p(\mathrm{k})/\mathrm{k})$ is its p-class tower group. In [**8**], Ozaki proved that every finite p-group Γ occurs as $\mathrm{Gal}(\mathrm{L}_p(\mathrm{F})/\mathrm{F})$ 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

$$1 \to \mathbb{Z}/p \to \mathrm{G}' \to \mathrm{G} \to 1 \qquad (1)$$

where $\mathrm{G} := \mathrm{Gal}(\mathrm{L}_p(\mathrm{k})/\mathrm{k})$, one can realize G' as $\mathrm{Gal}(\mathrm{L}_p(\mathrm{k}')/\mathrm{k}')$ 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:

2000 ***Mathematics Subject Classification.*** — 11R29.
Key words and phrases. — Hilbert class field tower, p-group.

The second author was partially supported by the ANR project FLAIR (ANR-17-CE40-0012) and by the EIPHI Graduate School (ANR-17-EURE-0002). The third author was partially supported by Simons Collaboration grant #524863. He also thanks FEMTO-ST for its hospitality and wonderful research environment during his visit there in the spring of 2022. 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.

- 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 Γ as its Galois group, while we start with a number field k_0 of arbitrary signature whose class number is prime to p.
- 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 [**8**].

We prove:

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

As any (topologically) countably generated pro-p group Γ is the inverse limit of finite p-groups, Ozaki shows any such Γ 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* Γ*, including p-adic analytic* Γ*, can be realized as* $\mathrm{Gal}(L_p(F)/F)$ *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 2.8.

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).

Arranging this and its split analog are the main technical difficulties. One then chooses a second prime v_2 that also solves the embedding problem as above and remains prime in $\mathrm{L}_p(\mathrm{k})_{\{v_1\}}/\mathrm{L}_p(\mathrm{k})$. The existence of v_1 and v_2 will follow from Chebotarev's Theorem. The compositum of these two solutions, after a $\mathbb{Z}/p$-base change k'/k ramified at both v_1 and v_2 (which exists!), gives the unramified solution to the embedding problem (1) which we show is $\mathrm{L}_p(\mathrm{k}')$. This is done in the proof of Theorem 2.

Our ability to choose primes v_i as above depends upon the existence of *Minkowski units* in the tower $\mathrm{L}_p(\mathrm{k})/\mathrm{k}$, namely on the condition that $\mathscr{O}^{\times}_{\mathrm{L}_p(\mathrm{k})} \otimes \mathbb{F}_p \simeq \mathbb{F}_p[\mathrm{G}]^{\lambda} \oplus N$ where N is an $\mathbb{F}_p[\mathrm{G}]$-torsion module and λ is a large enough integer. In some situations, Minkowski units are rare - see §5.3 of [**4**]. By contrast, both for Ozaki's proof (implicitly) and ours (explicitly), much of the work involves seeking fields for which they exist in abundance.

If $\mu_p \subset \mathrm{k}$, we may not be able to make our choices of v_i as above to both split completely in $\mathrm{L}_p(\mathrm{k})/\mathrm{k}$ and solve the nonsplit embedding problem (1). In this case we need to perform an extra base change $\tilde{\mathrm{k}}/\mathrm{k}$ to shift the obstruction to the embedding problem so that we can proceed as above. The base change $\tilde{\mathrm{k}}/\mathrm{k}$ must preserve the tower, that is $\mathrm{L}_p(\tilde{\mathrm{k}}) = \mathrm{L}_p(\mathrm{k})\tilde{\mathrm{k}}$. Theorem 1 provides such a $\tilde{\mathrm{k}}$.

Finally we check that the condition 'λ is large enough' persists, that is there are enough Minkowski units to keep the induction going. Proposition 2.7 guarantees this. To sum up, the key ingredients of the proof of the above Theorem and Corollary are Theorems 1 and 2 and Proposition 2.7.

We now explain in some detail Ozaki's approach and our simplifications.

- Using a result of Horie, [**5**], 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 $\mathrm{k}' \supset \mathrm{k}$ whose p-Hilbert class field tower has Galois group G'. For the induction to go forward, Ozaki needs $r_2(\mathrm{k}) \geqslant B_p(\mathrm{k})$ (implicit in this inequality is the existence of enough Minkowski units) where $B_p(\mathrm{k})$ is a certain explicit quantity depending on k, G and the p-part of the class group of $\mathrm{K} := \mathrm{L}_p(\mathrm{k})(\mu_p)$. This involves delicate estimates in §4 of [**8**]. We replace $r_2(\mathrm{k}) \geqslant B_p(\mathrm{k})$ with $f(\mathrm{k}) \geqslant 2h^1(\mathrm{G}) + 3$ where $h^i(\mathrm{G}) := \dim H^i(\mathrm{G}, \mathbb{Z}/p)$ and $f(\mathrm{k})$, which is a lower bound for the number of Minkowski units in $\mathrm{L}_p(\mathrm{k})/\mathrm{k}$, depends only on $h^1(\mathrm{G})$, $h^2(\mathrm{G})$ and the signature of k. We neither consider K nor invoke the estimates of §4 of [**8**].
- In §6 of [**8**], Ozaki proves his base change Proposition 1, namely he shows there exists a ramified $\mathbb{Z}/p$-extension $\tilde{\mathrm{k}}/\mathrm{k}$ such that $\mathrm{Gal}(\mathrm{L}_p(\tilde{\mathrm{k}})/\tilde{\mathrm{k}}) \simeq \mathrm{Gal}(\mathrm{L}_p(\mathrm{k})/\mathrm{k})$. He uses this repeatedly when solving each embedding problem (1). Several tame primes are ramified in $\tilde{\mathrm{k}}/\mathrm{k}$ and he also needs that K and $\mathrm{K}\tilde{\mathrm{k}}$ have the same p-class group. This makes the proof significantly more involved. Theorem 1 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 1 when $\mu_p \subset \mathrm{k}$. In particular, for p odd, our Corollary above makes no use of Theorem 1.
- 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 $\mathrm{L}/\mathrm{L}_p(\mathrm{k})$ 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

$\mathrm{Gal}(\mathrm{L}_p(\mathrm{k}')/\mathrm{k}') = \mathrm{G}'$. *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, $\mathscr{O}_{\mathrm{L}}$ its ring of integers, $\mathscr{O}_{\mathrm{L}}^{\times}$ its units and Cl_{L} and $\mathrm{Cl}_{\mathrm{L}}[p^\infty]$ are, respectively, the class group of L and its p-Sylow subgroup.

• For a finite set S of primes of L, set

$$V_{\mathrm{L},S} = \{x \in \mathrm{L}^\times, (x) = \mathscr{I}^p, x \in (\mathrm{L}_v^\times)^p \ \forall v \in S\}.$$

In particular, one has the exact sequence:

$$1 \longrightarrow \mathscr{O}_{\mathrm{L}}^{\times} \otimes \mathbb{F}_p \longrightarrow V_{\mathrm{L},\varnothing}/(\mathrm{L}^\times)^p \longrightarrow \mathrm{Cl}_{\mathrm{L}}[p] \longrightarrow 1.$$

• The superscript ^ indicates the Kummer dual of an object Z defined over a number field L, though we never work with the $\mathrm{Gal}(\mathrm{L}(\mu_p)/\mathrm{L})$ action on $Z^\wedge$.

• L_S is the maximal pro-p-extension of L unramified outside S, $G_S := \mathrm{Gal}(\mathrm{L}_S/\mathrm{L})$ and $\mathrm{L}_p(\mathrm{L}) := \mathrm{L}_\varnothing$, the maximal unramified pro-p-extension of L, as it will ease notation at various points.

• $h^i(H) := \dim H^i(H, \mathbb{Z}/p)$.

• $\mathrm{Gov}(\mathrm{L}) := \mathrm{L}(\mu_p)(\sqrt[p]{V_{\mathrm{L},\varnothing}})$: the governing field of L. The span of $\{\mathrm{Fr}_v\}_{v\in S}$ in $M(\mathrm{L}) := \mathrm{Gal}(\mathrm{Gov}(\mathrm{L})/\mathrm{L}(\mu_p))$ 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 $r_i(\mathrm{L}') = p \cdot r_i(\mathrm{L})$ and $\mu_p \subset \mathrm{L}' \iff \mu_p \subset \mathrm{L}$.
– 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, $\tilde{\mathrm{k}}/\mathrm{k}$ is an extension having p-class tower group G, the same as for k.

2. Tools for the proof

2.1. $\mathbb{F}_p[\mathrm{G}]$**-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 $\mathbb{F}_p[\mathrm{G}]$-modules M. See [**1**], §62.

Fact 1. — *Any finitely generated* $\mathbb{F}_p[\mathrm{G}]$*-module* M *is isomorphic to* $\mathbb{F}_p[\mathrm{G}]^\lambda \oplus N$ *where* N *is a torsion* $\mathbb{F}_p[\mathrm{G}]$*-module (every* $n \in N$ *is a torsion element) and where* λ *depends only on* M.

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

Set $T_{\mathrm{G}} := \sum_{g\in \mathrm{G}} g$. Denote by I_{G} the augmentation ideal of $\mathbb{F}_p[\mathrm{G}]$. For $x \in M$ set $\mathrm{Ann}_{\mathrm{G}}(x) := \{\alpha \in \mathbb{F}_p[\mathrm{G}] \mid \alpha \cdot x = 0\}$. Let $\{s_1, \cdots, s_{h^1(\mathrm{G})}\}$ be a system of minimal generators of G. By Nakayama's lemma and the fact that $I_{\mathrm{G}}/I_{\mathrm{G}}^2 \simeq \mathrm{G}/\mathrm{G}^p[\mathrm{G},\mathrm{G}]$, I_{G} can be generated, as G-(right or left)-module, by the elements $x_i := s_i - 1$.

Proposition 2.1. — *With the x_i as above, let $M = \mathbb{F}_p[\mathrm{G}]^{h^1(\mathrm{G})}$ and $x = (x_1, x_2, \cdots, x_{h^1(\mathrm{G})}) \in M$. Then $\mathrm{Ann}_{\mathrm{G}}(x) = \mathbb{F}_p T_{\mathrm{G}}$.*

Proof. — $\mathrm{Ann}_{\mathrm{G}}(x) = \bigcap_i \mathrm{Ann}_{\mathrm{G}}(x_i) = \mathrm{Ann}_{\mathrm{G}}(\langle x_i\rangle_{i=1}^{h^1(\mathrm{G})}) = \mathrm{Ann}_{\mathrm{G}}(I_{\mathrm{G}}) = \mathbb{F}_p T_{\mathrm{G}}$. □

Proposition 2.2. — *Let $M = \mathbb{F}_p[\mathrm{G}]^\lambda \oplus N$ be a finitely generated $\mathbb{F}_p[\mathrm{G}]$-module where N is torsion. Then $T_{\mathrm{G}}(M) \simeq \mathbb{F}_p^\lambda$.*

Proof. — It is clear that $T_{\mathrm{G}}(\mathbb{F}_p[\mathrm{G}]^\lambda) \simeq \mathbb{F}_p^\lambda$. We now show $T_{\mathrm{G}}(N) = 0$.
Let $n \in N$ so $\mathrm{Ann}_{\mathrm{G}}(n) \neq 0$. Note that $\mathrm{Ann}_{\mathrm{G}}(n) \subset \mathbb{F}_p[\mathrm{G}]$ 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 $\mathbb{F}_p[\mathrm{G}]$ are multiples of T_{G} so $T_{\mathrm{G}} \in \mathrm{Ann}_{\mathrm{G}}(n)$ as desired. □

Definition 1. — *We say the tower $\mathrm{L}_p(\mathrm{k})/\mathrm{k}$ with Galois group G has λ Minkowski units if, as $\mathbb{F}_p[\mathrm{G}]$-modules, $V_{\mathrm{L}_p(\mathrm{k}),\varnothing}/\mathrm{L}_p(\mathrm{k})^{\times p} = \mathscr{O}_{\mathrm{L}_p(\mathrm{k})}^\times \otimes \mathbb{F}_p \simeq \mathbb{F}_p[\mathrm{G}]^\lambda \oplus N$ where N is an $\mathbb{F}_p[\mathrm{G}]$-torsion module.*

2.2. 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 §11.3 of [**6**] for a proof. Recall that for a field L, $\delta(\mathrm{L}) = \begin{cases} 0 & \mu_p \not\subset \mathrm{L} \\ 1 & \mu_p \subset \mathrm{L} \end{cases}$.

Proposition 2.3. — *Let L be a number field, p a prime number and X a set of tame primes of L prime to p. Then*

(2) $$\dim H^1(\mathrm{G}_{\mathrm{L},X}, \mathbb{Z}/p) = \dim(V_{\mathrm{L},X}/\mathrm{L}^{\times p}) - r_1(\mathrm{L}) - r_2(\mathrm{L}) - \delta(\mathrm{L}) + 1 + \sum_{v\in X} \delta(\mathrm{L}_v).$$

Our $v \in X$ are always finite and have norm congruent to 1 mod p so $\delta(\mathrm{L}_v) = 1$.

Fact 2. — *Let S be a set of tame primes of L as above. For each $v \in S$ let $\mathrm{Fr}_v \in M(\mathrm{L}) := \mathrm{Gal}(\mathrm{Gov}(\mathrm{L})/\mathrm{L}(\mu_p))$. If the set $\{\mathrm{Fr}_v, v \in S\}$ spans an $(\#S - d)$-dimensional subspace of $M(\mathrm{L})$, then*

$$\dim H^1(\mathrm{G}_{\mathrm{L},S}, \mathbb{Z}/p) = d + \dim H^1(\mathrm{G}_{\mathrm{L},\varnothing}, \mathbb{Z}/p).$$

When $\mu_p \not\subset \mathrm{L}$, Fr_v is only well-defined up to nonzero scalar multiplication.

Proof. — In (2), as we vary X from $\varnothing$ to S, we are adding $\sum_{v\in S} \delta(\mathrm{L}_v) = \#S$ to the right side, but also subtracting $\dim(V_{\mathrm{L},\varnothing}/\mathrm{L}^{\times p}) - \dim(V_{\mathrm{L},X}/\mathrm{L}^{\times p})$ from the right side. This last quantity is $\#S - d$. □

Fact 3. — *Let L be a number field such that $(\#\mathrm{Cl}_{\mathrm{L}}, p) = 1$. Let L'/L be a $\mathbb{Z}/p$-extension exactly ramified at $S = \{v_1, \cdots, v_r\}$ where the v_i are finite and tame. Then $(\#\mathrm{Cl}_{\mathrm{L}'}, p) = 1$ 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, $(\#\mathrm{Cl}_{\mathrm{L}'}, p) \neq 1$ if and only if there exists an unramified $\mathbb{Z}/p$-extension H/L' such that H/L is Galois (use the fact the 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 $\mathrm{Gal}(H/\mathrm{L})$ have order p and they would thus fix an unramified extension of L, a contradiction. So $\mathrm{Gal}(H/\mathrm{L}) \simeq \mathbb{Z}/p \times \mathbb{Z}/p$, and L has at least two disjoints $\mathbb{Z}/p$-extension unramified outside S, also a contradiction. □

Set $Б_{\mathrm{L},S} = (V_{\mathrm{L},S}/\mathrm{L}^{\times p})^\wedge$. Recall $Ш^2_{\mathrm{L},S} := \mathrm{Ker}\,(H^2(G_S, \mathbb{Z}/p) \to \oplus_{v\in S} H^2(G_v, \mathbb{Z}/p))$. Fact 4 below is well-known. See Theorem 11.3 of [**6**].

Fact 4. — $Ш^2_{\mathrm{L},S} \hookrightarrow Б_{\mathrm{L},S}$.

Let λ_{L} be the number of Minkowski units in $\mathrm{L}_p(\mathrm{L})/\mathrm{L}$.

Fact 5. — *If* $\mu_p \not\subset \mathrm{L}$ *then* $\lambda_{\mathrm{L}} = r_1(\mathrm{L}) + r_2(\mathrm{L}) - 1 + h^1(\mathrm{G}) - h^2(\mathrm{G})$.
If $\mu_p \subset \mathrm{L}$ *then* $\lambda_{\mathrm{L}} \geqslant r_1(\mathrm{L}) + r_2(\mathrm{L}) - h^2(\mathrm{G})$.

This result is Theorem 2.9 of [**4**], but we sketch the proof for the sake of keeping this paper self-contained.

Proof. — Set $\mathrm{G} = \mathrm{Gal}(\mathrm{L}_p(\mathrm{L})/\mathrm{L})$. We consider two "norm maps" induced by the norm map on units: $\mathscr{O}^\times_{\mathrm{L}_p(\mathrm{L})} \to \mathscr{O}^\times_{\mathrm{L}}$.

- N_{G} sending $\mathscr{O}^\times_{\mathrm{L}_p(\mathrm{L})} \otimes \mathbb{F}_p$ to $\dfrac{\mathscr{O}^\times_{\mathrm{L}}}{\mathscr{O}^\times_{\mathrm{L}} \cap (\mathscr{O}^\times_{\mathrm{L}_p(\mathrm{L})})^p} \subset \mathscr{O}^\times_{\mathrm{L}_p(\mathrm{L})} \otimes \mathbb{F}_p$;
- $N'_{\mathrm{G}} : \mathscr{O}^\times_{\mathrm{L}_p(\mathrm{L})} \otimes \mathbb{F}_p \to \mathscr{O}^\times_{\mathrm{L}} \otimes \mathbb{F}_p$.

One easily sees $N'_{\mathrm{G}}(\mathscr{O}^\times_{\mathrm{L}_p(\mathrm{L})} \otimes \mathbb{F}_p) \twoheadrightarrow N_{\mathrm{G}}(\mathscr{O}^\times_{\mathrm{L}_p(\mathrm{L})} \otimes \mathbb{F}_p)$ and this is an isomorphism provided $\mathscr{O}^\times_{\mathrm{L}} \cap (\mathscr{O}^\times_{\mathrm{L}_p(\mathrm{L})})^p = (\mathscr{O}^\times_{\mathrm{L}})^p$: in particular this is the case when $\mu_p \not\subset \mathrm{L}$, see Proposition 2.8 of [**4**].
Write $\mathscr{O}^\times_{\mathrm{L}_p(\mathrm{L})} \otimes \mathbb{F}_p \simeq \mathbb{F}_p[\mathrm{G}]^{\lambda_{\mathrm{L}}} \oplus N$, where N is an $\mathbb{F}_p[\mathrm{G}]$-torsion module. By Proposition 2.2 one has $N_{\mathrm{G}}(\mathscr{O}^\times_{\mathrm{L}_p(\mathrm{L})} \otimes \mathbb{F}_p) \simeq \mathbb{F}_p^{\lambda_{\mathrm{L}}}$. Hence, when $\mu_p \not\subset \mathrm{L}$

$$\dim\left(\frac{\mathscr{O}^\times_{\mathrm{L}} \otimes \mathbb{F}_p}{N'_{\mathrm{G}}(\mathscr{O}^\times_{\mathrm{L}_p(\mathrm{L})} \otimes \mathbb{F}_p)}\right) = \dim(\mathscr{O}^\times_{\mathrm{L}} \otimes \mathbb{F}_p) - \lambda_{\mathrm{L}}.$$

When $\mu_p \subset \mathrm{L}$, note that the 'difference' between the images of N_{G} and N'_{G} has p-rank at most $\dim\left(\frac{\mathscr{O}^\times_{\mathrm{L}} \cap \mathscr{O}^{\times p}_{\mathrm{L}_p(\mathrm{L})}}{(\mathscr{O}^\times_{\mathrm{L}})^p}\right) \leqslant h^1(\mathrm{G})$, so

$$\dim\left(\frac{\mathscr{O}^\times_{\mathrm{L}} \otimes \mathbb{F}_p}{N'_{\mathrm{G}}(\mathscr{O}^\times_{\mathrm{L}_p(\mathrm{L})} \otimes \mathbb{F}_p)}\right) \geqslant \dim(\mathscr{O}^\times_{\mathrm{L}} \otimes \mathbb{F}_p) - \lambda_{\mathrm{L}} - h^1(\mathrm{G}).$$

To conclude, we use the well-known equality (see [**9**, Lemma 9]):

$$h^2(\mathrm{G}) - h^1(\mathrm{G}) = \dim\left(\frac{\mathscr{O}^\times_{\mathrm{L}} \otimes \mathbb{F}_p}{N'_{\mathrm{G}}(\mathscr{O}^\times_{\mathrm{L}_p(\mathrm{L})} \otimes \mathbb{F}_p)}\right).$$

□

2.3. Solving the ramified embedding problem with one tame prime. — We start with our nonsplit exact sequence:

$$1 \longrightarrow \mathbb{Z}/p \longrightarrow \mathrm{G}' \longrightarrow \mathrm{G} \longrightarrow 1. \tag{3}$$

given by the element $0 \neq \varepsilon \in H^2(\mathrm{G}, \mathbb{Z}/p)$.
We assume that $\mathrm{G} = \mathrm{Gal}(\mathrm{L}_p(\mathrm{k})/\mathrm{k})$.

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 $Ш^2_{\mathrm{k},S} \hookrightarrow Б_{\mathrm{k},S}$ by Fact 4. Here $Ш^2_{\mathrm{k},\varnothing} \simeq H^2(\mathrm{G}_{\mathrm{k},\varnothing}, \mathbb{Z}/p) \simeq H^2(\mathrm{G}, \mathbb{Z}/p)$. Let $Inf_S : H^2(\mathrm{G}_{\mathrm{k},\varnothing}, \mathbb{Z}/p) \to H^2(\mathrm{G}_{\mathrm{k},S}, \mathbb{Z}/p)$ be the inflation map. We have the commutative diagram:

$$\begin{array}{ccccc} & & Ш^2_{\mathrm{k},\varnothing} & \xrightarrow{Inf_S} & Ш^2_{\mathrm{k},S} \\ & & \Big\downarrow h & & \Big\downarrow g \\ \left(\mathrm{k}_v^\times \otimes \mathbb{F}_p\right)^\wedge & \longrightarrow & Б_{\mathrm{k},\varnothing} & \xrightarrow{f_S} & Б_{\mathrm{k},S} \end{array}$$

By Hoeschmann's criteria (see [**7**, Chapter 3, §5]), the embedding problem has a solution in k_S if and only if $Inf_S(\varepsilon) = 0$. As $\mathrm{L}_p(\mathrm{k})/\mathrm{k}$ is unramified, $Inf_S(\varepsilon) \in Ш^2_{\mathrm{k},S}$ and as $g(Inf_S(\varepsilon)) = f_S(h(\varepsilon)) \in Б_{\mathrm{k},S}$, the embedding problem has a solution if and only if $h(\varepsilon) \in \mathrm{Ker}(f_S)$.
Set $\mathrm{Gov}_S(\mathrm{k}) := \mathrm{k}(\mu_p)(\sqrt[p]{V_{\mathrm{k},S}})$. In the governing extensions $\mathrm{k}(\mu_p) \subset \mathrm{Gov}_S(\mathrm{k}) \subset \mathrm{Gov}(\mathrm{k})$, one sees that the kernel of the map $f_S : Б_{\mathrm{k},\varnothing} \twoheadrightarrow Б_{\mathrm{k},S}$ is exactly the (unramified) decomposition group D_v of the prime v. As noted in Fact 2, if $w_1, w_2 | v$ are two primes of $\mathrm{k}(\mu_p)$, their Frobenius elements in $\mathrm{Gal}(\mathrm{Gov}(\mathrm{k})/\mathrm{k}(\mu_p))$ differ by a nonzero scalar multiple.
We have proved

Lemma 2.4. — *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* $\langle \mathrm{Fr}_v \rangle = \langle h(\varepsilon) \rangle$ *in* $M(\mathrm{k})$, *that is the lines spanned by these elements in* $M(k)$ *are equal. This is always possible by Chebotarev's Theorem.*

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

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

of finite p-groups where $\mathrm{G} = \mathrm{Gal}(\mathrm{L}_p(\mathrm{k})/\mathrm{k})$, there exists a finite tamely ramified extension k'/k with $\mathrm{G}' = \mathrm{Gal}(\mathrm{L}_p(\mathrm{k}')/\mathrm{k}')$. To solve this embedding problem using Theorem 2, the tower $\mathrm{L}_p(\mathrm{k})/\mathrm{k}$ must have $2h^1(\mathrm{G})$ Minkowski units. Proposition 2.7 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 2.6, which is only needed in the case when $\mu_p \subset \mathrm{k}$, shows that given at least $h^1(\mathrm{G})$ Minkowski units, we can perform a base change that preserves the tower and the number of Minkowski units increases. Proposition 2.5 is a basic group theory result bounding $h^1(\mathrm{G}')$ and $h^2(\mathrm{G}')$ in terms of $h^1(\mathrm{G})$ and $h^2(\mathrm{G})$. Furata proves a similar result in Lemma 2 of [**3**].

Set $H^2(\mathrm{G}',\mathbb{Z}/p)_1 := \mathrm{Ker}\left(H^2(\mathrm{G}',\mathbb{Z}/p) \stackrel{Res}{\to} H^2(\mathbb{Z}/p,\mathbb{Z}/p)\right)$ and $h^2(\mathrm{G}')_1 := \dim H^2(\mathrm{G}',\mathbb{Z}/p)_1$. Note $h^2(\mathbb{Z}/p) = 1$ so $h^2(\mathrm{G}')_1$ is either $h^2(\mathrm{G}')$ or $h^2(\mathrm{G}') - 1$ and in either case $h^2(\mathrm{G}')_1 \geqslant h^2(\mathrm{G}') - 1$.

Proposition 2.5. — *Let*

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

be a short exact sequence of finite p-groups. Then $h^1(\mathrm{G}') \leqslant h^1(\mathrm{G}) + 1$ *and* $h^2(\mathrm{G}') \leqslant h^1(\mathrm{G}) + h^2(\mathrm{G}) + 1$.

Proof. — The h^1 result is clear. For the h^2 statement we have the long exact sequence (see for instance [**2**])

$$\begin{aligned} 0 \to H^1(\mathrm{G},\mathbb{Z}/p) \to H^1(\mathrm{G}',\mathbb{Z}/p) \to H^1(\mathbb{Z}/p,\mathbb{Z}/p)^G \\ \to H^2(\mathrm{G},\mathbb{Z}/p) \to H^2(\mathrm{G}',\mathbb{Z}/p)_1 \to H^1(\mathrm{G},H^1(\mathbb{Z}/p,\mathbb{Z}/p)). \end{aligned}$$

If $\mathrm{G}' \to \mathrm{G}$ splits, we have

$$0 \to H^2(\mathrm{G},\mathbb{Z}/p) \to H^2(\mathrm{G}',\mathbb{Z}/p)_1 \to H^1(\mathrm{G},H^1(\mathbb{Z}/p,\mathbb{Z}/p))$$

so $h^2(\mathrm{G}')_1 \leqslant h^2(\mathrm{G}) + h^1(\mathrm{G})$ and since $h^2(\mathrm{G}')_1 \geqslant h^2(\mathrm{G}') - 1$ the result follows.
In the nonsplit case we have

$$0 \to H^1(\mathbb{Z}/p,\mathbb{Z}/p)^{\mathrm{G}} \to H^2(\mathrm{G},\mathbb{Z}/p) \to H^2(\mathrm{G}',\mathbb{Z}/p)_1 \to H^1(\mathrm{G},H^1(\mathbb{Z}/p,\mathbb{Z}/p))$$

so $h^2(\mathrm{G}')_1 \leqslant h^2(\mathrm{G}) - 1 + h^1(\mathrm{G})$ so $h^2(\mathrm{G}') \leqslant h^1(\mathrm{G}) + h^2(\mathrm{G})$. □

Definition 2. — *For a number field* L *set* $\mathrm{G} = \mathrm{Gal}(\mathrm{L}_p(\mathrm{L})/\mathrm{L})$. *Define* f *as follows:*

$$f(\mathrm{L}) = \begin{cases} r_1(\mathrm{L}) + r_2(\mathrm{L}) - h^2(\mathrm{G}) + h^1(\mathrm{G}) - 1 & \mu_p \not\subset \mathrm{L} \\ r_1(\mathrm{L}) + r_2(\mathrm{L}) - h^2(\mathrm{G}) & \mu_p \subset \mathrm{L} \end{cases}.$$

Fact 5 implies $f(\mathrm{L})$ *is a lower bound on the number of Minkowski units of* $\mathrm{L}_p(\mathrm{L})/\mathrm{L}$.

Proposition 2.6. — *Let* $\tilde{\mathrm{k}}/\mathrm{k}$ *be a* $\mathbb{Z}/p$*-extension ramified at finite tame primes such that* $\mathrm{G} = \mathrm{Gal}(\mathrm{L}_p(\mathrm{k})/\mathrm{k}) = \mathrm{Gal}(\mathrm{L}_p(\tilde{\mathrm{k}})/\tilde{\mathrm{k}})$. *Then* $f(\tilde{\mathrm{k}}) = f(\mathrm{k}) + (p-1)(r_1(\mathrm{k}) + r_2(\mathrm{k}))$.

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

Proposition 2.7. — *Let* k'/k *be a tamely ramified* $\mathbb{Z}/p$*-extension such that* $\mathrm{G} = \mathrm{Gal}(\mathrm{L}_p(\mathrm{k})/\mathrm{k})$ *and* $\mathrm{G}' = \mathrm{Gal}(\mathrm{L}_p(\mathrm{k}')/\mathrm{k}')$ *where*

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

Let $f(\mathrm{k})$ *be as in Definition 2. Then*

$$f(\mathrm{k}) \geqslant 2h^1(\mathrm{G}) + 3 \implies f(\mathrm{k}') \geqslant 2h^1(\mathrm{G}') + 3.$$

Proof. — We do the case $\mu_p \not\subset \mathrm{k}$ first. We need to prove

$$\begin{aligned} r_1(\mathrm{k}) + r_2(\mathrm{k}) - h^2(\mathrm{G}) + h^1(\mathrm{G}) - 1 \geqslant 2h^1(\mathrm{G}) + 3 \\ \implies r_1(\mathrm{k}') + r_2(\mathrm{k}') - h^2(\mathrm{G}') + h^1(\mathrm{G}') - 1 \geqslant 2h^1(\mathrm{G}') + 3, \end{aligned}$$

that is

$$r_1(\mathrm{k}') + r_2(\mathrm{k}') \stackrel{?}{\geqslant} h^1(\mathrm{G}') + h^2(\mathrm{G}') + 4.$$

Clearly

$$r_1(\mathrm{k}') + r_2(\mathrm{k}') = p(r_1(\mathrm{k}) + r_2(\mathrm{k})) \geqslant p(h^1(\mathrm{G}) + h^2(\mathrm{G}) + 4)$$

and by Proposition 2.5 we have

$$h^2(\mathrm{G}') + h^1(\mathrm{G}') + 4 \leqslant (h^1(\mathrm{G}) + h^2(\mathrm{G}) + 1) + (h^1(\mathrm{G}) + 1) + 4 = 2h^1(\mathrm{G}) + h^2(\mathrm{G}) + 6$$

so it suffices to show

$$(p-1)h^2(\mathrm{G}) + (p-2)h^1(\mathrm{G}) + 4p \overset{\checkmark}{\geqslant} 6.$$

This holds for all p.

When $\mu_p \subset \mathrm{k}$. We need to prove

$$r_1(\mathrm{k}) + r_2(\mathrm{k}) - h^2(\mathrm{G}) \geqslant 2h^1(\mathrm{G}) + 3 \implies r_1(\mathrm{k}') + r_2(\mathrm{k}') - h^2(\mathrm{G}') \geqslant 2h^1(\mathrm{G}') + 3,$$

that is

$$r_1(\mathrm{k}') + r_2(\mathrm{k}') \overset{?}{\geqslant} 2h^1(\mathrm{G}') + h^2(\mathrm{G}') + 3.$$

Again using Proposition 2.5 and that $r_i(\mathrm{k}') = p \cdot r_i(\mathrm{k})$ it suffices to show

$$(p-1)h^2(\mathrm{G}) + (2p-3)h^1(\mathrm{G}) + 3p \overset{\checkmark}{\geqslant} 6$$

which holds for all p. □

Proposition 2.8 below provides the base case of the induction.

Proposition 2.8. — *Recall* $(\#\mathrm{Cl}_{\mathrm{k}_0}, p) = 1$. *There exists a tamely ramified extension* k'/k_0 *such that*

- *the p-part of the class group of* k' *is* $\mathbb{Z}/p$,
- $[\mathrm{k}' : \mathrm{k}_0] = p^3$,
- *and* $f(\mathrm{k}') > 2h^1(\mathbb{Z}/p) + 3 = 5$.

Proof. — Since $\mathrm{L}_p(\mathrm{k}_0) = \mathrm{k}_0$, we see $\mathrm{G} = \{e\}$. Choose a tame prime v of k whose Frobenius is trivial in the governing Galois group $M(\mathrm{k})$. By Fact 2 there is a unique $\mathbb{Z}/p$-extension $\mathrm{k}_1/\mathrm{k}_0$ unramified outside v. That $(\#\mathrm{Cl}_{\mathrm{k}_1}, p) = 1$ follows from Fact 3. Repeat this process with k_1 to get a field k_2 with $(\#\mathrm{Cl}_{\mathrm{k}_2}, p) = 1$.

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 2, but we include a short proof here.

Choose v_1 a finite tame prime of k_2 with trivial Frobenius in $M(\mathrm{k}_2)$ so that by Fact 2 there exists a unique D_1/k_2 ramified at v_1. As $D_1 \cap \mathrm{Gov}(\mathrm{k}_2) = \mathrm{k}_2$, we may choose v_2 a finite tame prime of k_2 with trivial Frobenius in $\mathrm{Gov}(\mathrm{k}_2)$ such that v_2 remains prime in D_1/k_2. Again by Fact 2 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_1D_2/D is everywhere unramified. We claim $D_1D_2 = \mathrm{L}_p(D)$. Indeed, by Fact 3 applied to D_1/k_2 we see $(\#\mathrm{Cl}_{D_1}, p) = 1$. As v_2 is inert in D_1/k_2, the extension D_2D_1/D_1 is ramified only at v_2 and Fact 3 applied to D_2D_1/D_1 implies $(\#\mathrm{Cl}_{D_1D_2}, p) = 1$. Whether or not $\mu_p \subset \mathrm{k}_0$, we have $\mathrm{k}' := D$, $\mathrm{Cl}_{\mathrm{k}'}[p^\infty] = \mathbb{Z}/p$ and

$$f(\mathrm{k}') \geqslant r_1(\mathrm{k}') + r_2(\mathrm{k}') - h^2(\mathbb{Z}/p) = p^3 r_1(\mathrm{k}_0) + p^3 r_2(\mathrm{k}_0) - 1 > 5 = 2h^1(\mathbb{Z}/p) + 3.$$

□

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 2, the main

Inductive Step. — *Let*

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

be exact and let k *be a number field with* $\mathrm{Gal}(\mathrm{L}_p(\mathrm{k})/\mathrm{k}) = \mathrm{G}$ *and* $f(\mathrm{k}) \geqslant 2h^1(\mathrm{G})+3$. *Then there exists a number field* k'/k *with* $\mathrm{Gal}(\mathrm{L}_p(\mathrm{k}')/\mathrm{k}') = \mathrm{G}'$ *and* $f(\mathrm{k}') \geqslant 2h^1(\mathrm{G}') + 3$.

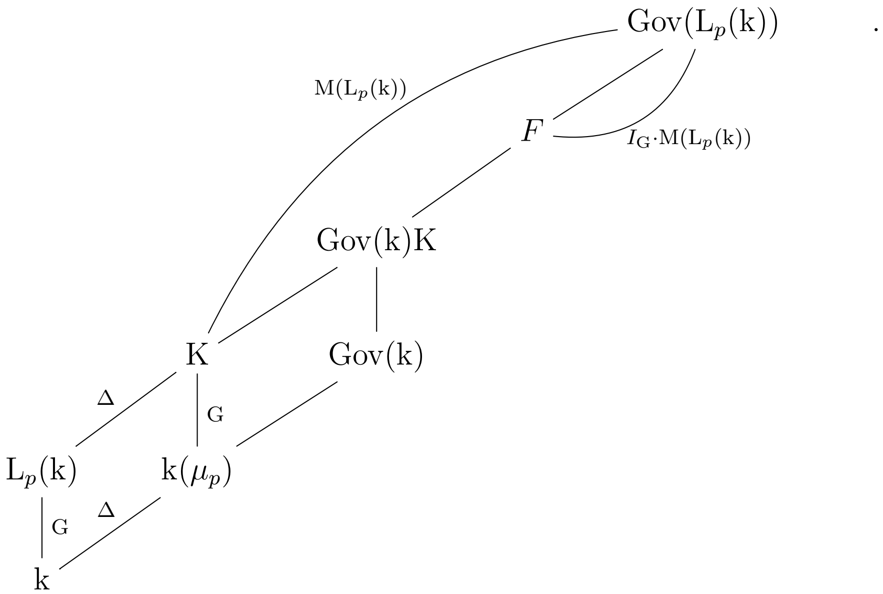
Theorem 1 below is only necessary for the key inductive step, Theorem 2, when $\mu_p \subset \mathrm{k}$. Set $\mathrm{K} := \mathrm{L}_p(\mathrm{k})(\mu_p)$. We only consider finite tame primes v of k that split completely in K/k. When $\mu_p \not\subset \mathrm{k}$, our Frobenius elements in governing fields (or their subfields) are only defined up to scalar multiples. We write $\langle \mathrm{Fr}_v \rangle_{\mathrm{Gov(k)/k}(\mu_p)}$ for the well-defined line spanned by Frobenius at v in $\mathrm{Gal}(\mathrm{Gov(k)/k}(\mu_p))$. When the Frobenius is trivial there is no ambiguity so we write $\langle \mathrm{Fr}_v \rangle_{\mathrm{Gov(k)/k}(\mu_p)} = 0$.

We need primes v of k that let us control $h^1(\mathrm{Gal}(\mathrm{k}_{\{v\}}/\mathrm{k}))$ and $h^1(\mathrm{Gal}(\mathrm{L}_p(\mathrm{k})_{\{v\}}/\mathrm{L}_p(\mathrm{k})))$ simultaneously via Fact 2. Recall $M(\mathrm{L}_p(\mathrm{k})) := \mathrm{Gal}(\mathrm{Gov}(\mathrm{L}_p(\mathrm{k}))/\mathrm{L}_p(\mathrm{k})(\mu_p)) \simeq \mathbb{F}_p[\mathrm{G}]^{\lambda_\mathrm{k}} \oplus N$ where N is a torsion module over $\mathbb{F}_p[\mathrm{G}]$. We have no knowledge of N and must work with the free part to control things over $\mathrm{L}_p(\mathrm{k})$. We then use Proposition 3.1 to control things over k.

3.1. The Stability Theorem. —

Proposition 3.1. — *Let* $F \subset \mathrm{Gov}(\mathrm{L}_p(\mathrm{k}))$ *be the field fixed by* $I_\mathrm{G} \cdot M(\mathrm{L}_p(\mathrm{k}))$. *For* v *of* k *splitting completely in* K *and* $w|v$ *in* K, *the lines* $\langle \mathrm{Fr}_w \rangle_{F/\mathrm{K}}$ *do not depend on* w *so we may write* $\langle \mathrm{Fr}_v \rangle_{F/\mathrm{K}}$. *Then* $\langle \mathrm{Fr}_{v_1} \rangle_{F/\mathrm{K}} = \langle \mathrm{Fr}_{v_2} \rangle_{F/\mathrm{K}}$ *implies* $\langle \mathrm{Fr}_{v_1} \rangle_{\mathrm{Gov(k)/k}(\mu_p)} = \langle \mathrm{Fr}_{v_2} \rangle_{\mathrm{Gov(k)/k}(\mu_p)}$. *If* $\langle \mathrm{Fr}_{v_1} \rangle_{F/\mathrm{K}} = 0$ *then* $\langle \mathrm{Fr}_{v_1} \rangle_{\mathrm{Gov(k)/k}(\mu_p)} = 0$.

Proof. — This diagram is useful in Theorems 1 and 2 as well.



Let $\Delta = \mathrm{Gal}(\mathrm{k}(\mu_p)/\mathrm{k}) = \mathrm{Gal}(\mathrm{K}/\mathrm{L}_p(\mathrm{k}))$. As $\mathrm{Gal}(F/\mathrm{K}) := M(\mathrm{L}_p(\mathrm{k}))/I_\mathrm{G} \cdot M(\mathrm{L}_p(\mathrm{k}))$ is the maximal quotient of $M(\mathrm{L}_p(\mathrm{k}))$ on which G acts trivially, and Δ acts on $\mathrm{Gal}(F/\mathrm{K})$ by scalars, the line $\langle \mathrm{Fr}_w \rangle_{F/\mathrm{K}}$ is invariant under the action of $\mathrm{Gal}(\mathrm{K}/\mathrm{k}) = \mathrm{G} \times \Delta$. Since the

$w|v$ form an orbit under this action of Gal(K/k), this line is independent of the choice of $w|v$ as desired.

As Gov(k)K/K ascends from Gov(k)/k(μ_p), we see G acts trivially on Gal(Gov(k)K/K) so Gov(k)K $\subset F$. Below, we implicitly use that our primes of k split completely in K. If $\langle \mathrm{Fr}_{v_1} \rangle_{F/\mathrm{K}} = \langle \mathrm{Fr}_{v_2} \rangle_{F/\mathrm{K}}$, these lines are equal when projected to Gal(Gov(k)K/K) $\subset$ Gal(Gov(k)K/k(μ_p)) and they are again equal in Gal(Gov(k)/k(μ_p)) so $\langle \mathrm{Fr}_{v_1} \rangle_{\mathrm{Gov(k)/k}(\mu_p)} = \langle \mathrm{Fr}_{v_2} \rangle_{\mathrm{Gov(k)/k}(\mu_p)}$. The last statement is clear. □

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

$$\mathrm{Fr}_w = ((x_1, x_2, \cdots, x_{h^1(\mathrm{G})}, 0, \cdots, 0), 0) \in M(\mathrm{L}_p(\mathrm{k})) \simeq \mathbb{F}_p[\mathrm{G}]^{\lambda_\mathrm{k}} \oplus N.$$

Then for v *of* k *below* w, $\langle \mathrm{Fr}_v \rangle_{\mathrm{Gov(k)/k}(\mu_p)} = 0$ *so there exists a* $\mathbb{Z}/p$*-extension* $\tilde{\mathrm{k}}/\mathrm{k}$ *ramified at only* v. *Furthermore,* $\mathrm{L}_p(\tilde{\mathrm{k}}) = \mathrm{L}_p(\mathrm{k})\tilde{\mathrm{k}}$ *and* $f(\tilde{\mathrm{k}}) > f(\mathrm{k})$.

Proof. — As Fr_w projects to 0 in the $\mathbb{F}_p$-vector space Gal(F/K), Proposition 3.1 implies $\langle \mathrm{Fr}_v \rangle_{\mathrm{Gov(k)/k}(\mu_p)} = 0$ so $\tilde{k}$ exists by Fact 2. We show the $\mathbb{F}_p$[G]-span of $(x_1, \cdots, x_{h^1(\mathrm{G})}) \in \mathbb{F}_p[\mathrm{G}]^{h^1(\mathrm{G})}$ has dimension $\#\mathrm{G} - 1$ by computing the dimension of $\cap_{i=1}^{h^1(\mathrm{G})} \mathrm{Ann}(x_i)$. This intersection is the annihilator of I_G which by Proposition 2.1 is just $\mathbb{F}_p T_\mathrm{G}$, establishing our dimension result. By Fact 2 there is a unique extension over $\mathrm{L}_p(\mathrm{k})$ ramified at v and thus it must be $\mathrm{L}_p(\mathrm{k})\tilde{\mathrm{k}}$. Fact 3 applied to $\mathrm{L}_p(\mathrm{k})\tilde{\mathrm{k}}/\mathrm{L}_p(\mathrm{k})$ implies $(\#\mathrm{Cl}_{\mathrm{L}_p(\mathrm{k})\tilde{\mathrm{k}}}, p) = 1$ so $\mathrm{L}_p(\tilde{\mathrm{k}}) = \mathrm{L}_p(\mathrm{k})\tilde{\mathrm{k}}$. Proposition 2.6 gives $f(\tilde{\mathrm{k}}) > f(\mathrm{k})$. □

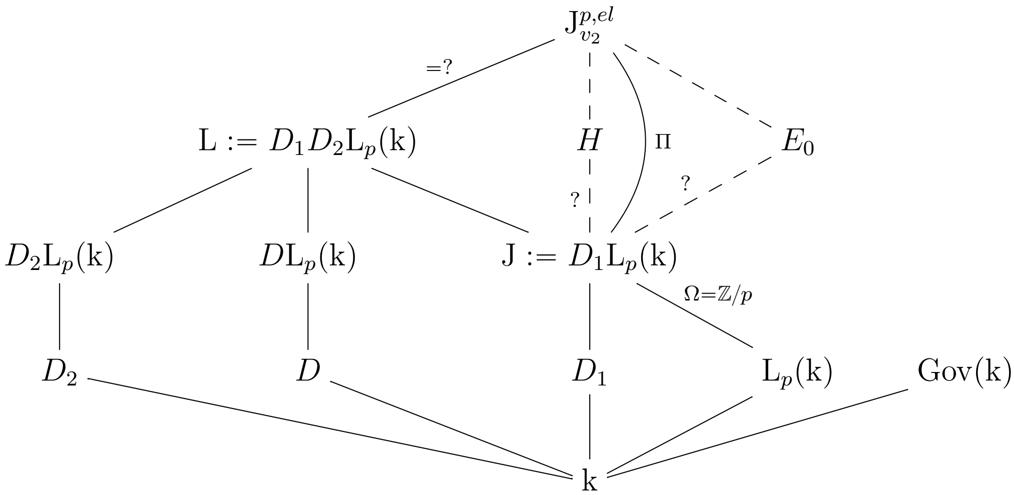
3.2. The inductive step. —

Theorem 2. — *Assume that* $\mathrm{L}_p(\mathrm{k})/\mathrm{k}$ *has* $\lambda_\mathrm{k} \geqslant 2h^1(\mathrm{G}) + 3$ *Minkowski units. Let* $1 \to \mathbb{Z}/p \to \mathrm{G}' \to \mathrm{G} \to 1$. *If the extension splits or* $\mu_p \not\subset \mathrm{k}$, *there exists a* $\mathbb{Z}/p$*-extension* k'/k *such that* $\mathrm{Gal}(\mathrm{L}_p(\mathrm{k}')/\mathrm{k}') \simeq \mathrm{G}'$ *and* $\mathrm{L}_p(\mathrm{k}')/\mathrm{k}'$ *has at least* $2h^1(\mathrm{G}') + 3$ *Minkowski units. If* $\mu_p \subset \mathrm{k}$ *and the extension is non-split,* k' *can be realized as a compositum of two successive* $\mathbb{Z}/p$*-extensions and* $\mathrm{L}_p(\mathrm{k}')/\mathrm{k}'$ *has at least* $2h^1(\mathrm{G}') + 3$ *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 $\mu_p \subset \mathrm{k}$.
Split case. Choose tame degree one primes w_1 and w_2 of Gov(k)K such that

- $\mathrm{Fr}_{w_1} = ((x_1, x_2, \cdots, x_{h^1(\mathrm{G})}, 0, \cdots, 0), 0) \in \mathrm{Gal}(\mathrm{Gov}(\mathrm{L}_p(\mathrm{k}))/\mathrm{Gov(k)K}) \subset M(\mathrm{L}_p(\mathrm{k}))$. This is possible as the tuple lies in $I_\mathrm{G} \cdot M(\mathrm{L}_p(\mathrm{k}))$ 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 $\langle \mathrm{Fr}_{v_1} \rangle_{F/\mathrm{K}} = 0$ so by Proposition 3.1 $\langle \mathrm{Fr}_{v_1} \rangle_{\mathrm{Gov(k)/k}(\mu_p)} = 0$. By Fact 2 applied to k there is one $\mathbb{Z}/p$-extension D_1/k ramified at v_1. Fact 2 also gives (see the proof of Theorem 1 as well) a unique $\mathbb{Z}/p$-extension of $\mathrm{L}_p(\mathrm{k})$ ramified at v_1, namely $D_1\mathrm{L}_p(\mathrm{k})/\mathrm{L}_p(\mathrm{k})$.
- $\mathrm{Fr}_{w_2} = ((0, 0, \cdots, 0_{h^1(\mathrm{G})}, x_1, x_2, \cdots, x_{h^1(\mathrm{G})}, 0, 0, 0, \cdots, 0), 0)$ so for v_2 of k below w_2, $\langle \mathrm{Fr}_{v_2} \rangle_{F/\mathrm{K}} = 0$. 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 $\mathrm{L}_p(\mathrm{k})$ ramified at v_2, namely D_2/k and $D_2\mathrm{L}_p(\mathrm{k})/\mathrm{L}_p(\mathrm{k})$. 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 and our choices of the Frobenius elements of v_1 and v_2 imply $h^1\big(\mathrm{Gal}(\mathrm{L}_p(\mathrm{k})_{\{v_1,v_2\}}/\mathrm{L}_p(\mathrm{k}))\big) = 2$ using that the span of the Frobenius elements above them in $\mathrm{Gal}(\mathrm{Gov}(\mathrm{L}_p(\mathrm{k}))/\mathrm{Gov}(\mathrm{k})\mathrm{K}) \subset M(\mathrm{L}_p(\mathrm{k}))$ has dimension $2\#\mathrm{G}-2$ and Fact 2. (With only $h^1(\mathrm{G})$ Minkowski units, we would again have had $h^1\big(\mathrm{Gal}(\mathrm{L}_p(\mathrm{k})_{\{v_1\}}/\mathrm{L}_p(\mathrm{k}))\big) = h^1\big(\mathrm{Gal}(\mathrm{L}_p(\mathrm{k})_{\{v_2\}}/\mathrm{L}_p(\mathrm{k}))\big) = 1$. In this case the span of the Frobenius elements above $\{v_1, v_2\}$ in $\mathrm{Gal}(\mathrm{Gov}(\mathrm{L}_p(\mathrm{k}))/\mathrm{Gov}(\mathrm{k})\mathrm{K}) \subset M(\mathrm{L}_p(\mathrm{k}))$ would have been $\#\mathrm{G}-1$ so by Fact 2, $h^1\big(\mathrm{Gal}(\mathrm{L}_p(\mathrm{k})_{\{v_1,v_2\}}/\mathrm{L}_p(\mathrm{k}))\big)$ would have been $2\#\mathrm{G} - (\#\mathrm{G}-1) = \#\mathrm{G}+1$.)



Set $\mathrm{L} := D_1D_2\mathrm{L}_p(\mathrm{k})$, $\mathrm{J} := D_1\mathrm{L}_p(\mathrm{k})$ 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 $(\#\mathrm{Cl}_{D_1D_2\mathrm{L}_p(\mathrm{k})}, p) = 1$.

Since $(\#\mathrm{Cl}_{\mathrm{L}_p(\mathrm{k})}, p) = 1$ and our choice of v_1 is such that $h^1(\mathrm{Gal}(\mathrm{L}_p(\mathrm{k})_{\{v_1\}}/\mathrm{L}_p(\mathrm{k})) = 1$, Fact 3 applied to $\mathrm{J}/\mathrm{L}_p(k)$ implies $(\#\mathrm{Cl}_\mathrm{J}, p) = 1$.

We now prove that there exists a unique $\mathbb{Z}/p$-extension over J unramified outside v_2, namely L. Set $\Omega = \mathrm{Gal}(\mathrm{J}/\mathrm{L}_p(\mathrm{k}))$, $\mathrm{J}^{p,el}_{\{v_2\}}$ to be the maximal elementary p-abelian extension of J inside $\mathrm{J}_{\{v_2\}}$, and $\Pi = \mathrm{Gal}(\mathrm{J}^{p,el}_{\{v_2\}}/\mathrm{J})$. Then Ω acts on Π and trivially on $\mathrm{Gal}(\mathrm{L}/\mathrm{J})$. We claim this is the only $\mathbb{Z}/p$-extension of J in $\mathrm{J}^{p,el}_{\{v_2\}}/\mathrm{J}$ on which Ω acts trivially: If not, there exists another $\mathbb{Z}/p$-extension H/J unramified outside v_2 and Galois over $\mathrm{L}_p(\mathrm{k})$. Hence $\mathrm{Gal}(H/\mathrm{L}_p(\mathrm{k}))$ has order p^2 and is abelian. The extension $H/\mathrm{L}_p(\mathrm{k})$ cannot be cyclic because all inertia elements have order p and would then fix an everywhere unramified extension of $\mathrm{L}_p(\mathrm{k})$, a contradiction. Suppose now that $\mathrm{Gal}(H/\mathrm{L}_p(\mathrm{k})) \simeq \mathbb{Z}/p \times \mathbb{Z}/p$, with $H \neq \mathrm{J}D_2 = \mathrm{L}$. Then $\mathrm{Gal}(HD_2/\mathrm{L}_p(\mathrm{k})) \simeq (\mathbb{Z}/p)^3$: this contradicts the already established fact that $h^1(\mathrm{Gal}(\mathrm{L}_p(\mathrm{k})_{\{v_1,v_2\}}/\mathrm{L}_p(\mathrm{k})) = 2$.

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 Ω; let S_0 be the set of ramification of E_0/J. As primes above v_2 in $\mathrm{L}_p(\mathrm{k})$ are inert in $\mathrm{J}/\mathrm{L}_p(\mathrm{k})$, $\Omega(S_0) = S_0$: then Ω 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 $E_0' \neq \mathrm{L}$ 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 $(\#\mathrm{Cl}_\mathrm{J}, p) = 1$. Thus L/J is the unique $\mathbb{Z}/p$-extension unramified outside v_2. Fact 3 applied to L/J implies $(\#\mathrm{Cl}_L, p) = 1$.

We have solved the split embedding problem with $\mathrm{k}' = D$ and $\mathrm{Gal}(\mathrm{L}_p(\mathrm{k}')/\mathrm{k}') = \mathrm{G} \times \mathbb{Z}/p$. It required one base change ramified at two tame finite primes. Proposition 2.7 implies $f(\mathrm{k}') \geqslant 2h^1(\mathrm{G}') + 3$ so the induction can proceed.

For the nonsplit case we treat $\mu_p \not\subset \mathrm{k}$ and $\mu_p \subset \mathrm{k}$ separately. Theorem 1 is only used in the nonsplit case when $\mu_p \subset \mathrm{k}$.

The nonsplit case, $\mu_p \not\subset \mathrm{k}$. By Lemma 2.4 we may use one tame prime v of k to find a *ramified* solution to the embedding problem. As $\mu_p \not\subset \mathrm{k}$ implies $\mathrm{Gov}(\mathrm{k}) \cap \mathrm{L}_p(\mathrm{k}) = \mathrm{k}$, we can assume v splits completely in K/k. Choosing any $w|v$ of K we set $\mathrm{Fr}_w = ((z_1, z_2, \cdots, z_{\lambda_\mathrm{k}}), n_0) \in M(\mathrm{L}_p(\mathrm{k}))$ where we claim $n_0 \notin I_\mathrm{G} \cdot N$ and $z_i \in I_\mathrm{G} \subset \mathbb{F}_p[\mathrm{G}]$. Indeed, if any $z_i \notin I_\mathrm{G}$, its $\mathbb{F}_p[\mathrm{G}]$-span is all of $\mathbb{F}_p[\mathrm{G}]$ and by Fact 2 there is no $\mathbb{Z}/p$-extension of $\mathrm{L}_p(\mathrm{k})$ ramified at the $w|v$, contradicting that we are solving an embedding problem with v. If $n_0 \in I_\mathrm{G} \cdot N$, then the projection of Fr_w to $\mathrm{Gal}(F/\mathrm{K})$ is trivial so Proposition 3.1 implies $\langle \mathrm{Fr}_v \rangle_{\mathrm{Gov}(\mathrm{k})/\mathrm{k}(\mu_p)} = 0$ and the embedding problem we are solving is split, also a contradiction.

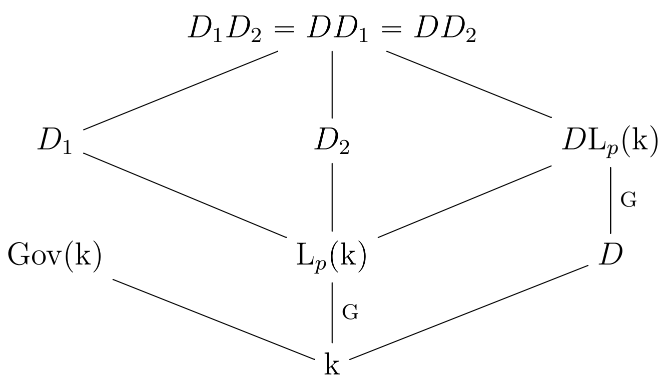
Choose a degree one w_1 of K with $\mathrm{Fr}_{w_1} = ((x_1, x_2, \cdots, x_{h^1(\mathrm{G})}, 0, 0, 0, \cdots, 0), n_0) \in M(\mathrm{L}_p(\mathrm{k}))$ where n_0 is as in the previous paragraph. Let v_1 be the prime of k below w_1. By Fact 2 (also see the proof of Theorem 1) there is one $\mathbb{Z}/p$-extension $D_1/\mathrm{L}_p(\mathrm{k})$ ramified at v_1.

Choose a degree one w_2 of K with $\mathrm{Fr}_{w_2} = ((0, 0, \cdots, 0, x_1, x_2, \cdots, x_{h^1(\mathrm{G})}, 0, 0, 0, \cdots, 0), n_0) \in M(\mathrm{L}_p(\mathrm{k}))$ and the primes of $\mathrm{L}_p(\mathrm{k})$ above v_2 remain prime in $D_1/\mathrm{L}_p(\mathrm{k})$. This last condition is linearly disjoint from the splitting conditions defining v_2 and imposes no contradiction. Again by Fact 2 there is one $\mathbb{Z}/p$-extension $D_2/\mathrm{L}_p(\mathrm{k})$ ramified at v_2.

As the free components of of Fr_w, Fr_{w_1} and Fr_{w_2} are all in $I_\mathrm{G}^{\lambda_\mathrm{k}}$, their projections to $\mathrm{Gal}(F/\mathrm{K})$ depend only on n_0 and Proposition 3.1 implies

$$0 \neq \langle \mathrm{Fr}_v \rangle_{\mathrm{Gov}(\mathrm{k})/\mathrm{k}(\mu_p)} = \langle \mathrm{Fr}_{v_1} \rangle_{\mathrm{Gov}(\mathrm{k})/\mathrm{k}(\mu_p)} = \langle \mathrm{Fr}_{v_2} \rangle_{\mathrm{Gov}(\mathrm{k})/\mathrm{k}(\mu_p)}.$$

Thus there is no extension of k ramified at either v_1 or v_2, but, by Fact 2, there is a $\mathbb{Z}/p$-extension of k ramified at $\{v_1, v_2\}$. Call it D. Note $\mathrm{G}' \simeq \mathrm{Gal}(D_1/\mathrm{k}) \simeq \mathrm{Gal}(D_2/\mathrm{k}) \simeq \mathrm{Gal}(D_1D_2/D)$.

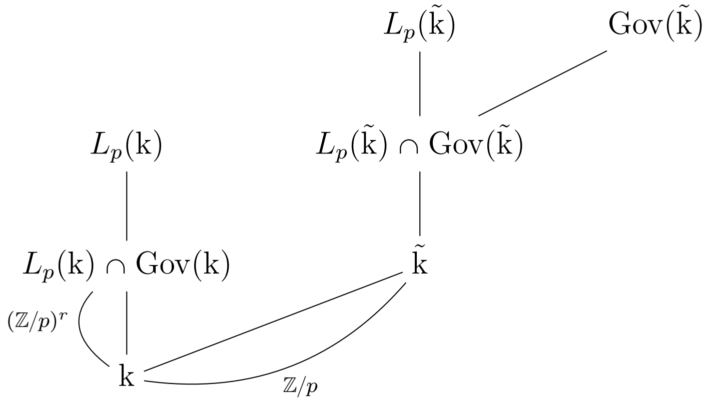


That D_1D_2 has trivial p-class group follows exactly as it did in the split case and we may set $\mathrm{k}' = D$ so $\mathrm{L}_p(\mathrm{k}') = D_1D_2$ and $\mathrm{Gal}(\mathrm{L}_p(\mathrm{k}')/\mathrm{k}') \simeq \mathrm{G}'$.

We have solved the embedding problem in the nonsplit case when $\mu_p \not\subset \mathrm{k}$. We performed one base change ramified at two tame finite primes and Proposition 2.7 implies $f(\mathrm{k}') \geqslant 2h^1(\mathrm{G}') + 3$ so the induction can proceed.

The nonsplit case, $\mu_p \subset \mathrm{k}$. We can no longer assume $\mathrm{L}_p(\mathrm{k}) \cap \mathrm{Gov}(\mathrm{k}) = \mathrm{k}$.
Let $0 \neq \varepsilon \in \text{Ш}^2_{\mathrm{k},\varnothing}$ be the obstruction to our embedding problem $\mathrm{G}' \twoheadrightarrow \mathrm{G}$. Using Lemma 2.4, let v of k be a tame prime annihilating ε. The difficulty is that in the diagram below we may have $\mathrm{L}_p(\mathrm{k}) \cap \mathrm{Gov}(\mathrm{k}) \supsetneq \mathrm{k}$ *and* that Fr_v, which is necessarily nonzero in $M(\mathrm{k})$, may also be nonzero in $\mathrm{Gal}((\mathrm{L}_p(\mathrm{k}) \cap \mathrm{Gov}(\mathrm{k}))/\mathrm{k})$. This prevents us from also choosing v to split completely in $\mathrm{L}_p(\mathrm{k})/\mathrm{k}$ and as we need in $\mathrm{Gov}(\mathrm{L}_p(\mathrm{k}))/\mathrm{L}_p(\mathrm{k})$ to ensure there is only one extension of $\mathrm{L}_p(\mathrm{k})$ ramified at the primes of $\mathrm{L}_p(\mathrm{k})$ above v. If we could choose v to annihilate ε such that $\mathrm{Fr}_v = 0 \in \mathrm{Gal}(\mathrm{L}_p(\mathrm{k})/\mathrm{k})$, 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, $\mathrm{Gal}(\mathrm{Gov}(\mathrm{L})/\mathrm{L}(\mu_p))$ is an elementary p-abelian group. Let $\tilde{\mathrm{k}}/\mathrm{k}$ be a tamely ramified $\mathbb{Z}/p$-extension as given by Theorem 1 so $\mathrm{Gal}(\mathrm{L}_p(\tilde{\mathrm{k}})/\tilde{\mathrm{k}}) = \mathrm{G}$. By Proposition 2.6 we have $\lambda_{\tilde{\mathrm{k}}} \geqslant 2h^1(\mathrm{G}) + 3$.



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

We now prove the Main Theorem of the Introduction:

Proof. — We have verified the base case of the induction in Proposition 2.8 and the inductive step with Theorem 2. It remains to count degrees and ramified primes. Proposition 2.8 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

- $\mu_p \not\subset \mathrm{k}_0$: At each of the $\log_p(\#\Gamma) - 1$ inductive stages we need one base change ramified at two primes for a total of $3 + \left(\log_p(\#\Gamma) - 1\right)$ base changes ramified at $4 + 2(\log_p(\#\Gamma) - 1)$ primes.

– $\mu_p \subset \mathrm{k}_0$: 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 $3 + 2\left(\log_p(\#\Gamma) - 1\right)$ base changes ramified at at most $4 + 3(\log_p(\#\Gamma) - 1)$ primes.

□

References

[1] C.W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, John Wiley and sons, coll. "Pure and Applied Mathematics", no 11, 1988.

[2] K. Dekimpe, M. Hartl, S. Wauters, *A seven-term exact sequence for the cohomology of a group extension*, J. Algebra 369 (2012), 70–95.

[3] Y. Furata, *On class field towers and the rank of ideal class groups*, Nagoya Math J. **48** (1972) 147-157.

[4] F. Hajir, C. Maire, R. Ramakrishna, *Deficiency of p-class tower groups and Minkowski units*, preprint 2021, arXiv:2103.09508.

[5] K. Horie, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields*, Invent. Math. **88** (1987) 31-38.

[6] H. Koch, Galois Theory of p-extensions (English translation by F. Lemmermeyer) Springer Monographs in Mathematics, Springer (2002).

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

[8] M. Ozaki, *Construction of maximal unramified p-extensions with prescribed Galois groups*, Invent. Math. **183** (2011), no. 3, 649–680.

[9] P. Roquette, *On class field towers*, In "J.-W.-S. Cassels and A. Fröhlich, Algebraic number theory", Academic Press London, 1967.

April 2, 2023

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