ON S-SPLIT p-HILBERT CLASS FIELD TOWERS WITH PRESCRIBED GALOIS GROUPS

Christian Maire, Karim Sankara

ON S-SPLIT p-HILBERT CLASS FIELD TOWERS WITH PRESCRIBED GALOIS GROUPS

by

Christian Maire & Karim Sankara

Abstract. — In this work, we show that given a finite p-group G, a number field K having a trivial p-class group Cl_K, and a finite set of primes S of K, there exists a finite extension F/K such that the S-split p-Hilbert class field tower $L_p^S(F)$ of F has G as its Galois group. This extends results by Ozaki and Hajir-Maire-Ramakrishna.

Introduction

Let p be a prime number and K be a number field. Denote by $L_p(K)$ the top of the p-Hilbert class field tower of K, which is the maximal unramified p-extension of K. The extension $L_p(K)/K$ can also be constructed by iteratively stacking the p-Hilbert class fields $K^{(i)}$: here, $K^{(0)} = K$, and $K^{(i+1)}$ is the p-Hilbert class field of $K^{(i)}$, *i.e.*, the maximal unramified abelian p-extension of $K^{(i)}$. Recall that the Artin map provides an isomorphism between the p-Sylow subgroup $Cl_{K^{(i)}}$ of the class group of $K^{(i)}$ and $Gal(K^{(i+1)}/K^{(i)})$. Let $G_K := Gal(L_p(K)/K)$.
Observe that $L_p(K) = K$ if and only if the p-part Cl_K of the class group of K is trivial (which is the case, for example, when $K = \mathbb{Q}$). On the other hand, the Golod–Shafarevich criterion shows that the p-extension $L_p(K)/K$ can be infinite (see **[1]**, **[4]**, §7.7 or **[10]**). To the best of our knowledge, using this criterion is the only method available to identify infinite p-towers. This naturally leads to the following question:
Does every finite p-group G arise as the Galois group of the p-Hilbert class field tower of some number field K?
This question can be viewed as an inverse Galois problem for the p-Hilbert tower.
Ozaki answered this question affirmatively in **[9]**. This result was revisited and further extended in **[3]**. It is this version that forms the basis of our approach.

Here, we focus on the inverse Galois problem for the p-Hilbert class field towers with decomposition. Let us clarify the context.

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

The authors are very grateful to Ravi Ramakrishna for his interest in our work and helpful comments. They also thank the International Mathematical Union, Commission for Developing Countries (IMU CDC) and the GRAID program for their support. This work has been supported by the EIPHI Graduate School (contract "ANR-17-EURE-0002") and by the Bourgogne-Franche-Comté Region.

Let S be a set of primes of K. Denote by $L_p^S(K)$ the p-extension of K that is unramified everywhere, totally decomposed at the places in S, and maximal with these properties. Let $G_K^S := Gal(L_p^S(K)/K)$. The extension $L_p^S(K)/K$ is also the largest normal subextension of $L_p(K)/K$ fixed by the decomposition groups of the primes above S, and G_K^S is a quotient of G_K.
The groups G_K^S have been the subject of extensive study; see, for example, [**4**, Chapter 11], [**2**, Chapter III], [**8**, Chapter X], [**7**], etc.

Before stating the main result of this note, let us introduce some notations.

For a finite p-group G, let $h_G^i = \dim H^i(G, \mathbb{Z}/p)$, and let p^{e_G} denote the exponent of G.
For a number field K, denote its signature by $(r_{K,1}, r_{K,2})$.
Theorem A. — *Let K be a number field with a finite p-Hilbert tower $L_p(K)/K$; set $G := G_K = Gal(L_p(K)/K)$. Assume that $r_{K,1} + r_{K,2} \geq h_G^1 + h_G^2$.*
Let S be a finite set of primes of K.
Then there exists a tamely ramified extension F/K of degree p^m such that
(i) $L_p(F) = L_p^S(F)$;
(ii) the Galois group $Gal(L_p^S(F)/F)$ is isomorphic to G;
(iii) the extension F/K is ramified at m primes;
(iv) $m \leq e_G$.
Here, we make a slight abuse of notation by still denoting by S the set S_F of primes of F lying above the primes in the original set S.
In Theorem A, the proof shows that $\#S_F = \#S$.
Remark 1. — *The choice of F depends on S. However, we can observe that the estimates on the degree of F/K and on the number of primes ramified in F/K do not depend on S.*
When $\zeta_p \notin K$, the condition on the signature of K can be refined (see Theorem 2.1), as it ensures the presence of a sufficient number of Minkowski units associated with K (see §1.3 for the definition). This condition is satisfied in the main result of [**3**], allowing us to deduce the following corollary.
Corollary B. — *Let K be a number field with a trivial p-class group Cl_K, and let S be a finite set of primes of K. Let G be a finite p-group. Then there exists an extension F/K, tamely ramified and unramified at infinity, such that the Galois group $Gal(L_p^S(F)/F)$ is isomorphic to G.*
Remark 2. — *The previous results establish the existence of an extension F/K with very specific properties. This extension is constructed by successively applying Chebotarev's theorem, which in fact ensures the existence of infinitely many extensions satisfying the mentioned properties.*
The proof of the main result relies critically on the presence of Minkowski units along the p-Hilbert tower $L_p(K)/K$. We then need to *eliminate* the residue degree at S within a given p-tower. This is achieved by forming the compositum with extensions $\tilde{F}/\tilde{K}$ that are inert at S, while maintaining the stability of the p-tower, a point where we use a result found in [**3**]. The existence of the extensions $\tilde{F}/\tilde{K}$ is ensured by carefully selecting Frobenius elements in appropriate governing fields.

Our work is organized into three parts. In §1, we recall the necessary tools. In §2, we prove Theorem A. Finally, in §3, we conclude with three remarks: one concerns a certain condition $\mathcal{C}_S$, another concerns the degrees of the fields encountered, and the third

addresses the same problem in the context of p-Hilbert towers with tame ramification and decomposition.

Preliminaries

We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Let p be a prime number. The element $\zeta_p \in \overline{\mathbb{Q}}$ denotes a primitive pth root of unity.

- Let K be a number field.
  - A prime $\mathfrak{q}$ of the ring of integers $\mathcal{O}_K$ of K is called *tame* if $\#\mathcal{O}_K/\mathfrak{q} \equiv 1 \ (mod\ p)$.
  - A $\mathbb{Z}/p$-extension F/K refers to a cyclic extension of degree p.
  - The field $K(\zeta_p)$ is denoted by K'.
- Let $S = \{\mathfrak{l}_1, ..., \mathfrak{l}_s\}$ be a finite set of primes of K.
  - $\mathcal{O}_K^S = \{\alpha \in K \mid v_\mathfrak{p}(\alpha) \geq 0,\ \forall \mathfrak{p} \notin S\}$ is the ring of S-integers of K, where $v_\mathfrak{p}$ is the $\mathfrak{p}$-valuation (normalized) associated to the prime $\mathfrak{p}$ of K.
  - The group $E^S := E_K^S$ of S-units of K is the group of invertible elements of $\mathcal{O}_K^S$.
  - We recall that E^S is isomorphic to $W_K \times \mathbb{Z}^r$, where W_K is the cyclic group of the roots of unity in K, and $r = r_{K,1} + r_{K,2} - 1 + s$.
- The p-Sylow subgroup of the S-class group of K denoted by Cl_K^S is defined by

$$Cl_K^S := \mathbb{Z}_p \otimes (I_K/\mathcal{P}_K\langle S\rangle)\,,$$

where I_K is the group of fractional ideals of $K^\times$, $\mathcal{P}_K$ is the subgroup of principal fractional ideals, and $\langle S\rangle$ is the subgroup of I_K constructed from the primes in S. Set $Cl_K^S[p] := \{h \in Cl_K^S, h^p = 1\}$. Recall that, by class field theory, the group Cl_K^S is isomorphic to the Galois group of the abelian p-extension $K^{S,(1)}/K$, which is unramified everywhere, totally decomposed at all the primes of S, and maximal for these properties ("real archimedean places stay real").

- For a prime $\mathfrak{p}$ of K, let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$, and $U_\mathfrak{p}$ be the subgroup of units of $K_\mathfrak{p}^\times$. Let $\mathcal{J} := \mathcal{J}_K$ be the group of the idèles of K; set $U_\infty = \prod_{v|\infty} K_v^\times$, where the products is taken over archimedean places v of K; set $\mathcal{U} := \mathcal{U}_K = U_\infty \prod_\mathfrak{p} U_\mathfrak{p}$.
Observe that $Cl_K \simeq \mathbb{Z}_p \otimes (\mathcal{J}/K^\times\mathcal{U})$, and $Cl_K^S \simeq \mathbb{Z}_p \otimes \left(\mathcal{J}/K^\times\mathcal{U}\prod_{\mathfrak{l}\in S} K_\mathfrak{l}^\times\right)$.
- More generally, let S and T be two finite and disjoint sets of primes of K. We assume that the primes in T are tame. Let $L_{p,T}^S$ be the pro-p extension of K, unramified outside T, totally splitting at S, and maximal for these properties. Observe that $L_{p,\emptyset}^S = L_p^S$ and $L_{p,\emptyset}^\emptyset = L_p(K)$. Set $G_{K,T}^S := Gal(L_{p,T}^S/K)$.
- If G is a p-group, we denote by $\Phi(G) := G^p[G,G]$ its Frattini subgroup. All cohomology groups have coefficients $\mathbb{Z}/p$ (with trivial action) so we write $H^i(G)$ for $H^i(G, \mathbb{Z}/p)$. We denote by h_G^i the dimension over $\mathbb{F}_p$ of $H^i(G)$. Recall that h_G^1 is the minimal number of generators of G, and h_G^2 is the minimal number of relations.
- For $p = 2$, the set of extensions considered in this paper are unramified at infinity.

1. Tools for the proof

1.1. Governing field. —

1.1.1. *Definition.* — Given a finite set S of primes of K, we define the multiplicative subgroup V_K^S of $K^\times$ as

$$V_K^S = \{x \in K^\times, (x) \in (I_K)^p \langle S \rangle\}.$$

When $S = \emptyset$, we denote $V_K := V_K^\emptyset$.

Lemma 1.1. — *The following exact sequence holds:*

$$1 \longrightarrow E_K^S/(E_K^S)^p \longrightarrow V_K^S/(K^\times)^p \longrightarrow Cl_K^S[p] \longrightarrow 1$$

Proof. — The map $f : V_K^S/(K^\times)^p \to Cl_K^S[p]$ is defined as follows. Take $x \in V_K^S$: there exists $\mathfrak{a} \in I_K$ and $\mathfrak{b} \in \langle S \rangle$ such that $(x) = \mathfrak{a}^p\mathfrak{b}$. Then, $f(x)$ is the class of $\mathfrak{a}$ in Cl_K^S. The map f is surjective, and the kernel is exactly $E_K^S/(E_K^S)^p$. □

Definition 1.2. — *The governing field relatively to K and S is the number field $Gov_K^S := K'(\sqrt[p]{V_K^S})$. When $S = \emptyset$, we denote $Gov_K := Gov_K^\emptyset$.*

The extension Gov_K^S/K is Galois. Set $M_K^S = Gal(Gov_K^S/K')$: it is an elementary abelian p-group of p-rank which can be deduced from Lemma 1.1. Again, when $S = \emptyset$, we denote $M_K := M_K^\emptyset$.

For the groups M_K^S, we will use additive notation.

1.1.2. *Governing field and idèles.* — Let $S = \{\mathfrak{l}_1, \cdots, \mathfrak{l}_s\}$ and $T = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_t\}$ be two finite and disjoint sets of primes of K. We assume that the primes $\mathfrak{q}_i$ in T are tame.
Set

- $\mathcal{U}_T^S := U_\infty \prod_{\mathfrak{l} \in S} K_\mathfrak{l}^\times \prod_{\mathfrak{p} \notin S \cup T} U_\mathfrak{p}$, $\mathcal{U}^S := \mathcal{U}_\emptyset^S$, $\mathcal{U}_T := \mathcal{U}_T^\emptyset$,
- $V_T^S := V_{K,T}^S = \{x \in K^\times \mid x \in U_\mathfrak{p},\ \forall \mathfrak{p} \notin S \cup T; x \in (K_\mathfrak{q}^\times)^p,\ \forall \mathfrak{q} \in T\}$.

One can express the sets V_T^S in terms of idèles:

$$V_T^S = K^\times \cap \mathcal{J}^p\mathcal{U}_T^S.$$

In particular, $V^S = K^\times \cap \mathcal{J}^p\mathcal{U}^S$ and $V_T = K^\times \cap \mathcal{J}^p\mathcal{U}_T$.

1.1.3. *Governing field anf Frobenius.* — Let us choose a tame prime $\mathfrak{q}$ of K, not in S. Since $\#\mathcal{O}_K/\mathfrak{q} \equiv 1$ modulo p, the prime $\mathfrak{q}$ splits completely in K'/K. Let $\mathfrak{Q}$ be a prime ideal of K' above $\mathfrak{q}$. Denot by $\sigma_\mathfrak{Q}$ the Frobenius of $\mathfrak{Q}$ in $Gal(Gov_K^S/K')$. For convenience, we will write $\sigma_\mathfrak{q} := \sigma_\mathfrak{Q}$ for some specific $\mathfrak{Q}|\mathfrak{q}$. Note that if $\mathfrak{Q}'$ is another prime of K' above $\mathfrak{q}$, then $\sigma_\mathfrak{Q} = a\sigma_{\mathfrak{Q}'}$ for some $a \in \mathbb{F}_p^\times$. It follows that any property involving $\sigma_\mathfrak{q}$ will not depend on the choice of $\mathfrak{Q}|\mathfrak{q}$.

Let S and T be as before. Set $Gov_{K,T}^S := K'(\sqrt[p]{V_{K,T}^S})$, and $M_{K,T}^S = Gal(Gov_{K,T}^S/K')$.

Lemma 1.3. — *The Galois group $Gal(Gov_K^S/Gov_{K,T}^S)$ is generated by the Frobenius elements $\sigma_\mathfrak{q}$ at $\mathfrak{q} \in T$.*

Proof. — First observe that primes $\mathfrak{q} \in T$ are unramified in Gov_K^S/K'.
Take $x \in V_{K,T}^S$, and $\mathfrak{q} \in T$. Then $x \in (K_\mathfrak{q}^\times)^p$, $(Gov_{K,T}^S)_\mathfrak{q} = K_\mathfrak{q}$, and consequently $Gov_{K,T}^S$ is fixed by $\sigma_\mathfrak{q} \in M_K^S$.
Reciprocally. Take $x \in V_K^S$ such that for all $\mathfrak{q} \in T$, $\sigma_\mathfrak{q} \in Gal(Gov_K^S/K'(\sqrt[p]{x}))$. Then $x \in (K_\mathfrak{q}^\times)^p$ (recall that $\zeta_p \in K_\mathfrak{q}$). Hence, $x \in V_{K,T}^S$. □

Remark 1.4. — *Observe that if a prime $\mathfrak{p}$ of K, coprime to p and S, has a non-trivial Frobenius in M_K^S then $\mathfrak{p}$ is tame.*

1.1.4. *Governing field and $\mathbb{Z}/p$-extensions with prescribed ramification.* — Let us state the following theorem due to Gras (see [**2**, Chapter V, Corollary 2.4.2]), which is not a priori useful in the proof of our result but which we will use in a remark in §3.1.
Let S and T be as before.
***Theorem 1.5* (Gras).** — *There exists a $\mathbb{Z}/p$-extension F/K that is exactly ramified at $T = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_t\}$ and totally decomposed at S if and only if, for $i = 1, ..., t$, there exists $a_i \in \mathbb{F}_p^\times$ such that:*

$$\sum_{i=1}^{t} a_i \sigma_{\mathfrak{q}_i} = 0 \in M_K^S.$$

Here "exactly ramified" at T means that F/K is unramified outside T and every prime in T is ramified in F/K.

We will use the following corollary.
Corollary 1.6. — *Assume $S = \{\mathfrak{l}\}$ and let $\mathfrak{q}$ be a tame prime of K, $\mathfrak{q} \neq \mathfrak{l}$, such that $\sigma_\mathfrak{q} \neq 0$ in M_K^S. If there exists a $\mathbb{Z}/p$-extension F/K that is exactly ramified at $\mathfrak{q}$, then $\mathfrak{l}$ is inert in F/K.*

1.2. Governing fields in the p-Hilbert tower. — Our main result relies on the choice of Frobenius elements in $M_{L_p(K)}$ while considering the action of G_K. To do this, we will need the following properties of linear disjunction.
Lemma 1.7. — *Let L/K' be an unramified extension. Then*

$$L \cap K'(\sqrt[p]{V_K^S}) = L \cap K'(\sqrt[p]{V_K})$$

and

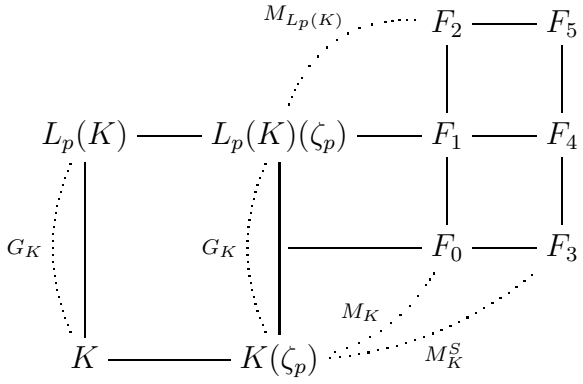
$$L(\sqrt[p]{V_L}) \cap L(\sqrt[p]{V_K^S}) = L(\sqrt[p]{V_K}).$$

Proof. — For the first point, obviously $L \cap K'(\sqrt[p]{V_K}) \subset L \cap K'(\sqrt[p]{V_K^S})$. Now, let $x \in V_K^S$ such that $K'(\sqrt[p]{x})/K'$ is unramified. This implies that $x\mathcal{O}_{K'} \in \mathcal{I}_{K'}^p$, and we will see that $x \in V_K$. Indeed, it is sufficient to take the norm in K'/K and then observe that $([K' : K], p) = 1$. Hence, the first point is proved.
Now let $x \in V_K^S$ such that $L(\sqrt[p]{x}) \subset L(\sqrt[p]{V_L})$. By Kummer theory, there exists $z \in V_L$ such that $zx^{-1} \in (L^\times)^p$. Therefore, $x\mathcal{O}_L \in \mathcal{I}_L^p$. On the other hand, in K, we have $(x) = \mathfrak{a}^p\mathfrak{b}$, with $\mathfrak{b} \in \langle S \rangle$. Since the extension L/K' is unramified at S (and $[K' : K]$ is prime to p), we deduce that $\mathfrak{b} \in \mathcal{I}_K^p$, which implies $x \in V_K$. Thus, we have

$$L(\sqrt[p]{V_L}) \cap L(\sqrt[p]{V_K^S}) = L(\sqrt[p]{V_L}) \cap L(\sqrt[p]{V_K}) = L(\sqrt[p]{V_K}),$$

since $V_K \subset V_L$. □

Consider now the following extensions.



where $F_0 := K'(\sqrt[p]{V_K}) = Gov_K$, $F_1 := L_p(K)F_0$, $F_2 := L_p(K)\left(\zeta_p, \sqrt[p]{E_{L_p(K)}}\right) = Gov_{L_p(K)}$, $F_3 := K'\left(\sqrt[p]{V_K^S}\right) = Gov_K^S$, $F_4 = F_3F_1 = L_p(K)F_3$, and $F_5 = F_3F_2$.
Observe that $V_L = E_{L_p(K)}$.

Since $L_p(K)(\zeta_p)/K'$ is unramified, by Lemma 1.7, we have $F_1 \cap F_3 = F_0$ and $F_2 \cap F_4 = F_1$. Therefore, $F_2 \cap F_3 = F_2 \cap F_4 \cap F_3 = F_1 \cap F_3 = F_0$.

In conclusion, the extensions F_2/F_0 and F_3/F_0 are linearly disjoint over F_0, and we thus have

$$(1) \qquad Gal(F_5/F_0) = Gal(F_5/F_2) \times Gal(F_5/F_3) \simeq Gal(F_3/F_0) \times Gal(F_2/F_0).$$

1.3. Minkowski units. —

1.3.1. *Structure.* — First, let us recall a well-known result.
Proposition 1.8. — *Let G be a p-group, and let M be a finitely generated $\mathbb{F}_p[G]$-module. Then every free submodule of M is a direct summand of M. In particular, there exists a well-defined integer $\lambda \geq 0$ such that $M \simeq \mathbb{F}_p[G]^\lambda \oplus N$, where N is a torsion $\mathbb{F}_p[G]$-module.*
Proof. — This result follows from the fact that $\mathbb{F}_p[G]$ is a Frobenius algebra (see [**5**, §1, (3.15.E)], and from the Krull-Schmidt theorem). See also [**9**, §4]. □

We apply this result to the following context: $G_K = Gal(L_p(K)/K)$ is finite, and $M = E_{L_p(K)}/(E_{L_p(K)})^p$. We then denote $\lambda_K := \lambda$.
Definition 1.9. — *When $\lambda_K > 0$, we say that the p-tower $L_p(K)/K$ contains λ_K Minkowski units.*
Remark 1.10. — *We actually use the Kummer dual of $V_{L_p(K)}/(K^\times)^p$, which is itself equal to the Kummer dual of $E_{L_p(K)}/(E_{L_p(K)})^p$, as p does not divide the order of the class group of $L_p(K)$. Minkowski units of $L_p(K)/K$ provide a free part of the same rank for this dual, i.e., for the group $M_{L_p(K)}$ viewed as an $\mathbb{F}_p[G_K]$-module.*
Remark 1.11. — *Supppose that $\zeta_p \in K$. Let $\mathfrak{q}$ be a tame prime of K that splits completely in $L_p(K)/K$. There are exactly $\#G_K$ primes $\mathfrak{Q}_i$ of $L_p(K)$ above $\mathfrak{q}$, on which the group G_K acts transitively. Consider such a prime $\mathfrak{Q}$, and let $\sigma_\mathfrak{Q}$ be its Frobenius element in the Galois group $M_{L_p(K)}$ of the governing field $Gov_{L_p(K)}$. By the property of the Artin symbol, G_K acts transitively on the $\sigma_\mathfrak{Q}$. When $\zeta_p \notin K$, G_K acts transitively on the lines spanned by the Frobenius elements $\sigma_\mathfrak{Q} \in M_{L_p(L)}$ (see also the observation made in §1.1.3).*

1.3.2. *Growth of the number of Minkowski units.* — We fix a number field K such that G_K is finite. Let us begin with a definition:

Definition 1.12. — *Set*

$$A_K = \begin{cases} r_{K,1} + r_{K,2} - h^2_{G_K} + h^1_{G_K} - 1 & \text{if} \quad \zeta_p \notin K \\ r_{K,1} + r_{K,2} - h^2_{G_K} & \text{if} \quad \zeta_p \in K. \end{cases}$$

The presence of Minkowski units is central to our study, and the phenomenon of growth due to a base change becomes highly significant. This was observed by Ozaki in [**9**] and quantified in [**3**] through the following two propositions:

Proposition 1.13. — *Let F/K be a $\mathbb{Z}/p$-extension unramified at infinity and such that $L_p(F) = FL_p(K)$. Then, $A_F = A_K + (p-1)(r_{K,1} + r_{K,2})$.*

Proof. — See [**3**, Proposition 2.6]. □

Proposition 1.14. — *Let K be a number field. Then, $\lambda_K \geq A_K$.*

Proof. — See [**3**, §2, Fact 5]. □

1.4. Stability of the p-Hilbert class field tower. — We begin with a number field K such that G_K is finite.

Let $\{g_1, ..., g_d\}$ be a minimal system of generators of $G_K = Gal(L_p(K)/K)$, where $d = h^1_{G_K}$. The augmentation ideal I_{G_K} of $\mathbb{F}_p[G]$ is generated as a G-module by the elements $x_i := g_i - 1$, for $i = 1, ..., d$.

Suppose $\lambda_K \geq d$, and write $M_{L_p(K)} := Gal(Gov_{L_p(K)}/L_p(K)(\zeta_p)) \simeq \mathbb{F}_p[G_K]^d \oplus M_0$.
In this notation, set

$$z = ((x_1, ..., x_d), 0) \in M_{L_p(K)}.$$

Observe that $z \in I_{G_K}\left(M_{L_p(K)}\right)$. In particular, $z \in Gal\left(Gov_{L_p(K)}/L_p(K)Gov_K\right)$. Indeed, $M_{L_p(K)}/I_{G_K}\left(M_{L_p(K)}\right)$ is the maximal extension of $L_p(K)$ on which G_K acts trivially, and G_K obviously acts trivially on $Gal(L_p(K)Gov_K/L_p(K))$.

The result concerning the stability of the p-tower is as follows.

Theorem 1.15. — *Suppose that $\lambda_K \geq d$. Let $\mathfrak{q}$ be a tame prime of K such that $\sigma_{\mathfrak{q}} = z \in M_{L_p(K)} \subset Gal(Gov(L_p(K))/K)$. Then, there exists a $\mathbb{Z}/p$-extension F/K exactly ramified at $\mathfrak{q}$ and such that $L_p(F) = FL_p(K)$. Moreover $A_F > A_K$.*

Proof. — See [**3**, Theorem 1]. □

2. Main result

Let us recall the main result of our work (Theorem A).

Theorem 2.1. — *Let K be a number field with a finite p-Hilbert tower $L_p(K)/K$; set $G := G_K = Gal(L_p(K)/K)$. Assume that $A_K \geq h^1_G$.*
Let S be a finite set of primes of K.
Then there exists a tamely ramified extension F/K of degree p^m such that

- *(i) $L_p(F) = L_p^S(F)$;*
- *(ii) the Galois group $Gal(L_p^S(F)/F)$ is isomorphic to G;*
- *(iii) the extension F/K is ramified at m primes;*
- *(iv) $m \leq e_G$.*

Observe that when $G = \{e\}$, the result is immediate. Suppose now G to be nontrivial. In this case, the condition $r_{K,1} + r_{2,K} \geq h^1_G + h^2_G$ from Theorem A implies that $A_K \geq h^1_G$.

2.1. Proof of Theorem 2.1. — Let $\Sigma = \{\mathfrak{l}_1, \cdots\}$ and $T = \{\mathfrak{q}_1, \cdots\}$ be two finite and disjoint sets of primes of K. We assume that the primes $\mathfrak{q}_i \in T$ are tame. We use the notation from §1.1.2.

Lemma 2.2. — *We have the exact sequence:*

$$V_T/(K^\times)^p \hookrightarrow V_T^\Sigma/(K^\times)^p \longrightarrow \prod_{\mathfrak{l}\in\Sigma} K_\mathfrak{l}^\times/(K_\mathfrak{l}^\times)^p U_\mathfrak{l} \longrightarrow \mathcal{J}/\mathcal{J}^p K^\times \mathcal{U}_T \twoheadrightarrow \mathcal{J}/\mathcal{J}^p K^\times \mathcal{U}_T^\Sigma.$$

Proof. — Let us first describe $\alpha : V_T^\Sigma/(K^\times)^p \to \prod_{\mathfrak{l}\in\Sigma} K_\mathfrak{l}^\times/(K_\mathfrak{l}^\times)^p U_\mathfrak{l}$. Take $x \in V_T^\Sigma$. Then $x \in \mathcal{J}^p\mathcal{U}_T^\Sigma$, and $\alpha(x)$ is simply the projection to the Σ-coordinates. Thus, $ker(\alpha) = \mathcal{J}^p\mathcal{U}_T$ modulo $(K^\times)^p$ that is $V_T/(K^\times)^p$.
The map $\beta : \prod_{\mathfrak{l}\in\Sigma} K_\mathfrak{l}^\times/(K_\mathfrak{l}^\times)^p \to \mathcal{J}/\mathcal{J}^p K^\times\mathcal{U}_T$ is the inclusion followed by the restriction modulo $\mathcal{J}^p K^\times \mathcal{U}_T$. Obviously, $\beta \circ \alpha = 0$, then $Im(\alpha) \subset ker(\beta)$. Let us study the reverse inclusion. Let $z := (z_\mathfrak{l}) \in \prod_{\mathfrak{l}\in\Sigma} K_\mathfrak{l}^\times$ be such that $z \in \mathcal{J}^p K^\times \mathcal{U}_T$ (in other words, $z \in ker(\beta)$). Then there exists $x \in K^\times$ such that $z = j^p \cdot x \cdot u$, where $j \in \mathcal{J}$ and $u \in \mathcal{U}_T$. Then $x \in K^\times \cap \mathcal{J}^p\mathcal{U}_T^\Sigma = V_T^\Sigma$, and $\alpha(x) = z$.
The other maps are obvious. □

Given a prime $\mathfrak{p}$ of K, let $K_\mathfrak{p}^{ur}$ be the maximal unramified extension of $K_\mathfrak{p}$; set $G_\mathfrak{p}^{ur} := Gal(K_\mathfrak{p}^{ur}/K_\mathfrak{p})$.
The exact sequence of Lemma 2.2 allows us to obtain the following proposition:

Proposition 2.3. — *One has the exact sequence*

$$H^1(G_T^\Sigma) \hookrightarrow H^1(G_T) \longrightarrow \bigoplus_{\mathfrak{l}\in\Sigma} H^1(G_\mathfrak{l}^{ur}) \longrightarrow M_{K,T}^\Sigma \twoheadrightarrow M_{K,T},$$

where the map $H^1(G_\mathfrak{l}^{ur}) \longrightarrow M_{K,T}^\Sigma$ relies on the Artin map and Kummer duality.
Proof. — By the Artin maps, $\mathcal{J}/\mathcal{J}^p K^\times \mathcal{U}_T^\Sigma \simeq G_T^\Sigma/\Phi(G_T^\Sigma)$, and $K_\mathfrak{l}^\times/(K_\mathfrak{l}^\times)^p U_\mathfrak{l} \simeq G_\mathfrak{l}^{ur}/(G_\mathfrak{l}^{ur})^p$. Then the exact sequence of Lemma 2.2 becomes

$$V_T/(K^\times)^p \hookrightarrow V_T^\Sigma/(K^\times)^p \longrightarrow \prod_{\mathfrak{l}\in\Sigma} G_\mathfrak{l}^{ur}/(G_\mathfrak{l}^{ur})^p \longrightarrow G_T/\Phi(G_T) \twoheadrightarrow G_\Sigma/\Phi(G_T^\Sigma).$$

By taking the dual $\wedge$ we get

$$0 \longrightarrow H^1(G_T^\Sigma) \longrightarrow H^1(G_T) \longrightarrow \bigoplus_{\mathfrak{l}\in\Sigma} H^1(G_\mathfrak{l}^{ur}) \longrightarrow \left(V_{K,T}^\Sigma/(K^\times)^p\right)^\wedge \longrightarrow \left(V_{K,T}/(K^\times)^p\right)^\wedge \longrightarrow 0.$$

To conclude, observe that by Kummer duality

$$\left(V_{K,T}^\Sigma/(K^\times)^p\right)^\wedge \simeq M_{K,T}^\Sigma \text{ and, } \left(V_{K,T}/(K^\times)^p\right)^\wedge \simeq M_{K,T}.$$

□

Let $\mathfrak{q}$ be a tame prime of K. By applying Proposition 2.3 successively with $T = \emptyset$ and $T = \{\mathfrak{q}\}$, we get the following commutative diagram:

$$\begin{array}{ccccccc}
H^1(G_K) & \xrightarrow{\psi} & \bigoplus_{\mathfrak{l}\in\Sigma} H^1(G_\mathfrak{l}^{ur}) & \xrightarrow{\varphi} & M_K^\Sigma & \longrightarrow\!\!\!\!\rightarrow & M_K \\
\downarrow & & \| & & \downarrow{\scriptstyle \phi_\mathfrak{q}} & & \downarrow \\
H^1(G_{K,T}) & \xrightarrow{\psi'} & \bigoplus_{\mathfrak{l}\in\Sigma} H^1(G_\mathfrak{l}^{ur}) & \xrightarrow{\varphi'} & M_{K,T}^\Sigma & \longrightarrow\!\!\!\!\rightarrow & M_{K,T}
\end{array}$$

Recall that $\ker(\phi'')$ is generated by the Frobenius element $\sigma_{\mathfrak{q}} \in M_K^{\Sigma}$ (see Lemma 1.3).

Let us start with some local conditions $a := (a_{\mathfrak{l}})_{\mathfrak{l}\in S} \in \bigoplus_{\mathfrak{l}\in\Sigma} H^1(G_{\mathfrak{l}}^{ur})$. Then

$$a \in Im(\psi') \Longleftrightarrow a \in ker(\varphi') \Longleftrightarrow \varphi(a) \in ker(\phi_{\mathfrak{q}}) \Longleftrightarrow \langle\sigma_{\mathfrak{q}}\rangle = \langle\varphi(a)\rangle\cdot$$

Lemma 2.4. — *Suppose $a \notin Im(\psi)$. Let $\mathfrak{q}$ be a tame prime of K, not in Σ, such that in M_K^{Σ}, $\langle\sigma_{\mathfrak{q}}\rangle = \langle\varphi(a)\rangle$. Then there exists a $\mathbb{Z}/p$-extension N/K exactly ramified at $\mathfrak{q}$ that respects the $a_{\mathfrak{l}}$'s, $\mathfrak{l} \in \Sigma$. Moreover, the tame prime $\mathfrak{q}$ is such that $\sigma_{\mathfrak{q}} \in M_K^{\Sigma}$ restricts to M_K is trivial.*

Proof. — Let us choose a tame prime $\mathfrak{q} \notin S$ such that in M_K^{Σ}, $\langle\sigma_{\mathfrak{q}}\rangle = \langle\varphi(a)\rangle$. Then there exists a $\mathbb{Z}/p$-extension N/K unramified outside $\mathfrak{q}$ that respects the $a_{\mathfrak{l}}$, $\mathfrak{l} \in \Sigma$. Since $a \notin Im(\psi)$, the extension N/K is not unramified, and then N/K is exactly ramified at $\mathfrak{q}$. Moreover, the existence of such an extension implies that $\mathfrak{q}$ splits totally in M_K (see, for example, Theorem 1.5, or observe that $\sigma_{\mathfrak{q}} \in Im(\varphi)$). □

Remark 2.5. — *Observe now that a non-trivial $a_{\mathfrak{l}} \in H^1(G_{\mathfrak{l}}^{ur})$ indicates that $\mathfrak{l}$ is inert in N/K.*

We can prove the key proposition of our work.

Proposition 2.6. — *Suppose $\lambda_K \geq h^1_{G_K}$. Let $S = \{\mathfrak{l}_1, \cdots\}$ be a finite set of primes of K. Then there exists a $\mathbb{Z}/p$-extension N/K ramified at only one tame prime $\mathfrak{q}$ such that:*

(i) the extension N/K is inert at all places of S;

(ii) there is stability of the p-tower, i.e., $L_p(N) = NL_p(N)$.

Proof. — • For each $\mathfrak{l} \in S$, take the non-trivial element $a_{\mathfrak{l}} := 1 \in H^1(G_{\mathfrak{l}}^{ur})$.
Set $a' = (a_{\mathfrak{l}})_{\mathfrak{l}\in S)} \in \bigoplus_{\mathfrak{l}\in S} H^1(G_{\mathfrak{p}}^{ur})$.

– If $a' \notin Im(\psi)$, set $a = a'$ and $\Sigma = S$.

– If $a' \in Im(\psi)$, let us choose a prime $\mathfrak{l}_0$ that splits totally in the elementary abelian extension $(L_p^S)^{p,el}/K$ of L_p^S/K. Set $\Sigma = S \cup \{\mathfrak{l}_0\}$, and consider $a = (1)_{\mathfrak{l}\in\Sigma} \in \bigoplus_{\mathfrak{l}\in\Sigma} H^1(G_{\mathfrak{p}}^{ur})$. By the choice of $\mathfrak{l}_0$, $a \notin Im(\psi)$.

• Let us consider the extensions of §1.2 by replacing S by Σ.

Recall the isomorphism (1):

$$Gal(F_5/F_0) = Gal(F_5/F_2) \times Gal(F_5/F_3),$$

with $Gal(F_5/F_2) \simeq Gal(F_3/F_0)$.

Let $z_0 \in Gal(F_5/F_2)$ such that its projection onto $Gal(F_3/F_0)$ coincides with a.

Let $d = h^1_{G_K}$, and let $z = ((x_1, ..., x_d), 0) \in M_{L_p(K)}$ as in Theorem 1.15. In fact, $z \in I_{G_K}(M_{L_p(K)})$, which indicates that $z \in Gal(F_2/F_1)$ (see §1.4). We then choose $z_1 \in Gal(F_5/F_4)$ such that its projection onto $Gal(F_2/F_1)$ coincides with z.

By the Chebotarev density theorem, we now choose a tame prime $\mathfrak{q}$ of K not belonging in Σ, such that

$$\sigma_{\mathfrak{q}} = (z_0, z_1) \in Gal(F_5/F_2) \times Gal(F_5/F_4) \subset Gal(F_5/K)\cdot$$

• Let's look at the implications of this choice.

First, by restriction to F_3, $\sigma_{\mathfrak{q}} = a \in Gal(F_3/F_0) \subset M_K^{\Sigma} = Gal(F_3/K')$, which, by Lemma 2.4 indicates the existence of a $\mathbb{Z}/p$-extension N/K ramified only at $\mathfrak{q}$, such that every prime $\mathfrak{l}$ of Σ is inert.

Then, $\sigma_{\mathfrak{q}}$ restricted to F_2 coincides with z, which, by Theorem 1.15, implies the stability of the p-tower, *i.e.*, $L_p(N) = NL_p(N)$. Hence, the result. □

We now have all the elements to prove the main result of our work.
First, by assumption $\lambda_K \geq h_G^1$: this is a consequence of Proposition 1.14.
By Proposition 2.6, there exists a $\mathbb{Z}/p$-extension N/K ramified at some prime $\mathfrak{q}$, inert at each prime $\mathfrak{p} \in S$, and such that $L_p(N) = NL_p(N)$.
Let $\mathfrak{l} \in S$ such that $\mathfrak{l}$ is not totally splitting in $L_p(K)/K$. Recall that $\mathfrak{l}$ is inert in N/K. Noting that the decomposition group of $\mathfrak{l}$ in $Gal(L_p(N)/N)$ is cyclic (defined up to conjugacy), it is then a small exercise to observe that the residual degree of $\mathfrak{l}$ in $L_p(N)/N$ strictly decreases: it is divisible by p. This is therefore true for any such prime $\mathfrak{l} \in S$.
If $\mathfrak{l} \in S$ splits totally in $L_p(K)/K$, then it also splits totally in $L_p(N)/N$.
By iterating this process m times, we obtain a p-extension F/K such that every prime $\mathfrak{l} \in S$ splits totally in $L_p(F)/F$. Thus, we have $L_p^S(F) = L_p(F)$.
To conclude, we need to estimate p^m. A coarse upper bound is $\#G_K$. We can go a bit further by bounding p^m by the exponent of G_K.
Remark 2.7. — *Observe also that each place $\mathfrak{l} \in S$ is "inert" in the successive steps. In particular, in Theorem A, $\#S_F = \#S$.*

2.2. Proof of Corollary B. — Let us conclude with a word on the proof of Corollary B. Let G be a p-group and let K be a number field such that $Cl_K = 1$. By the main theorem of **[3]**, there exists an extension $\tilde{K}/K$ such that $Gal(L_p(\tilde{K})/\tilde{K}) \simeq G$. Furthermore, the proof of this result shows that for the field $\tilde{K}$ in question, we have $A_{\tilde{K}} \geq h_G^1$, which implies $\lambda_{\tilde{K}} \geq h_G^1$. We can then apply Theorem A.

3. Remarks

3.1. The condition $\mathcal{C}_S$. — Let $S = \{\mathfrak{l}_1, \mathfrak{l}_2, ..., \mathfrak{l}_s\}$ be a set of primes of K. We denote by $\mathcal{C}_S$ the following condition.

($\mathcal{C}_S$): Every prime $\mathfrak{l} \in S$ splits totally in the elementary abelian extension $(L_p)^{p,el}/K$ of $L_p(K)/K$.

The condition $\mathcal{C}_S$ is therefore equivalent to the isomorphism between $Cl_K/(Cl_K)^p$ and $Cl_K^S/(Cl_K^S)^p$.

Observe that the condition $\mathcal{C}_S$ is satisfied after a first application of Proposition 2.6. The goal here is to revisit the element a and the choice of $\mathfrak{q}$ in §2.1.
Lemma 3.1. — *The condition $\mathcal{C}_S$ is equivalent to $\#Cl_K^S[p] = \#Cl_K[p]$.*
Proof. — This simply follows from the fact that for a finite abelian group A we have $\#A[p] = \#A/A^p$, an equality derived from the exact sequence:

$$1 \longrightarrow A[p] \longrightarrow A \stackrel{a \mapsto a^p}{\longrightarrow} A \longrightarrow A/A^p \longrightarrow 1.$$

□

Lemma 3.1 allows us to prove the following lemma.
Lemma 3.2. — *Suppose $\mathcal{C}_S$. Then for every subset $X \subset S$, we have the exact sequence:*

$$1 \longrightarrow V_K/(K^\times)^p \longrightarrow V_K^X/(K^\times)^p \longrightarrow (\mathbb{Z}/p)^{\#X} \longrightarrow 1.$$

Proof. — Let's start with the following commutative diagram:

$$(2)\qquad \begin{array}{ccccccccc} 1 & \longrightarrow & E_K/E_K^p & \longrightarrow & V_K/K^{\times p} & \longrightarrow & Cl_K[p] & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & E_K^X/(E_K^X)^p & \longrightarrow & V_K^X/K^{\times p} & \longrightarrow & Cl_K^X[p] & \longrightarrow & 1 \end{array}$$

Under the condition $\mathcal{C}_S$, by Lemma 3.1, we known that $ker(\gamma)$ and $coker(\gamma)$ have the same order. This implies that $coker(\alpha)$ and $coker(\beta)$ also have the same order by the Snake Lemma. Now, since $coker(\alpha) \simeq (\mathbb{Z}/p)^{\#X}$ by Dirichlet's theorem, we obtain the result. □

Lemma 3.3. — *Suppose $\mathcal{C}_S$. Let $X = \{\mathfrak{l}_{i_1}, \cdots, \mathfrak{l}_{i_x}\} \subset S$ be a subset of x primes of S. Then*

$$K'(\sqrt[p]{V_K^X}) = K'\left(\sqrt[p]{V_K^{\{\mathfrak{l}_{i_1}\}}}, \sqrt[p]{V_K^{\{\mathfrak{l}_{i_2}\}}}, \cdots, \sqrt[p]{V_K^{\{\mathfrak{l}_{i_x}\}}}\right),$$

and the Galois group of $K'(\sqrt[p]{V_K^X})/K'(\sqrt[p]{V_K})$ is isomorphic to $(\mathbb{Z}/p)^x$.
Proof. — For $\#X = 1$, this is the Lemma 3.2.

Suppose $X = \{\mathfrak{l}_1, \mathfrak{l}_2\} \subset S$. Obviously $V_K^{\{\mathfrak{l}_1\}} V_K^{\{\mathfrak{l}_2\}} \subset V_K^X$, and $V_K^{\{\mathfrak{l}_1\}} \cap V_K^{\{\mathfrak{l}_2\}} (K'^{\times})^p = V_K$. By Lemma 3.2, $Gal(K'(\sqrt[p]{V_K^{\{\mathfrak{l}_i\}}})/K'(\sqrt[p]{V_K})) \simeq \mathbb{Z}/p$, and $Gal(K'(\sqrt[p]{V_K^X}/K'(\sqrt[p]{V_K}) \simeq (\mathbb{Z}/p)^2$, which proves the result.

Continue the process. □

We then obtain the following proposition.
Proposition 3.4. — *Suppose $\mathcal{C}_S$. Then*

$$Gal\left(K'(\sqrt[p]{V_K^S})/K'(\sqrt[p]{V_K})\right) \simeq \prod_{i=1}^{s} Gal\left(K'(\sqrt[p]{V_K^{\{\mathfrak{l}_i\}}})/K'(\sqrt[p]{V_K})\right) \simeq (\mathbb{Z}/p)^s.$$

Proof. — It is an immediate consequence of Lemma 3.3. □

We arrive at the following remark. Recall the isomorphism (1): $Gal(F_5/F_0) \simeq Gal(F_5/F_2) \times Gal(F_5/F_3)$ used in the proof of our main result (see §2.1). We have choosen a tame prime $\mathfrak{q}$ of K and an element $z_0 \in Gal(F_5/F_0)$ such that $\sigma_\mathfrak{q} = z_0$ in $Gal(F_3/K')$.
Under $\mathcal{C}_S$, the element z_0 can be chosen as $(1, 1, ..., 1) \in Gal(F_5/F_2)$ according to the isomorphism:

$$Gal(F_5/F_2) \simeq Gal(F_3/F_0) \simeq \prod_{i=1}^{s} Gal\left(K'(\sqrt[p]{V_K^{\{\mathfrak{l}_i\}}})/K'(\sqrt[p]{V_K})\right) \simeq (\mathbb{Z}/p)^s.$$

By the Chebotarev density theorem, choose a tame prime $\mathfrak{q}$ of K not belonging in S, such that $\sigma_\mathfrak{q} = z_0 \in Gal(F_5/F_2)$. Since $\sigma_\mathfrak{q} = 0$ in M_K, by Theorem 1.5, there exists a $\mathbb{Z}/p$-extension N/K ramified only at $\mathfrak{q}$,

Let $\mathfrak{l} \in S$. The restriction of $\sigma_\mathfrak{q}$ to $Gal\left(K'(\sqrt[p]{V_K^{\{\mathfrak{l}\}}})/K'(\sqrt[p]{V_K})\right)$ is non-trivial by the choice of z_0, which, by Corollary1.6, implies that $\mathfrak{l}$ is inert in N/K.

3.2. On the degree. — Let G be a pro-p group. Let $d = h^1_G$ and $r = h^2_G$. Recall the Golod-Shafarevich criterion (see [**1**], [**4**, §7.7] or [**10**]): If G is finite, then $r > d^2/4$.

On the other hand, when $G = Gal(L^S_p(K)/K)$, according to Shafarevich and Koch, we know that $0 \leq r-d \leq r_{K,1}+r_{K,2}+\#S$ (see for example [**8**, Chapter X, Theorem 10.7.12]). Therefore, if $L^S_p(K)/K$ is finite then $r_{K,1} + r_{K,2} + \#S > d^2/4 - d$.
Thus, when $\#S$ is bounded, the degree $[K : \mathbb{Q}]$ grows according to the p-rank of G.

3.3. On T-ramified and S-split p-Hilbert ray class field towers. — Let p be a prime number. Let K be a number field, and let S and T be two finite and disjoint sets of primes of K. We assume that the primes in T are tame. Let $L^S_{p,T}(K)$ be the pro-p extension of K, unramified outside T, totally splitting at S, and maximal for these properties. Set $G^S_{K,T} := Gal(K^S_T/K)$.

Recall that if $\#T$ is large compared to the degree of $K/\mathbb{Q}$ and $\#S$ is fixed, then G^S_T is infinite. This can be seen, for example, through genus theory (see the main theorem of [**6**]) associated with the Golod-Shafarevich theorem. See also, for example, [**7**].

Here, we make the following observation.

Theorem 3.5. — *Let K be a number field such that $Cl_K = 1$, and let S be a finite set of primes of K. Let G be a p-group and let $n \geq 0$. Then there exists an extension F/K and a set T of tame primes of F such that:*

(i) $\#T = n$,

(ii) $G^S_{F,T} \simeq G$.

As before, we will abusively denote by $S := S_F$ the set of primes of F above those in S.

Proof. — We begin by applying Corollary B: there exists an extension $\tilde{F}/K$ such that $L^S_p(\tilde{F}) = L_p(\tilde{F})$ and $Gal(L_p(\tilde{F})/\tilde{F}) \simeq G$. We then note that the proof guarantees enough Minkowski units, *i.e.*, $\lambda_{\tilde{F}} \geq h^1_G$. By Propositions 1.13 and 1.14, it is then possible to use the stability theorem 1.15 to obtain an extension $F/\tilde{F}$ such that $L^S_p(F) = L_p(F)$, $Gal(L_p(F)/F) \simeq G$, and $\lambda_F \geq n$.

Thus $M_{L_p(F)} = \mathbb{F}_p[G]^n \oplus M_0$. For $i = 1, \cdots, n$, define $x_i = ((0, \cdots, 0, 1, 0, \cdots 0), 0) \in M_{L_p(F)}$. As an $\mathbb{F}_p[G]$-module, the elements x_i form a basis of a free subspace of dimension n. For $i = 1, \cdots, n$, by the Chebotarev density theorem, choose a tame prime $\mathfrak{q}_i$ of F such that $\sigma_{\mathfrak{q}_i} = x_i \in M_{L_p(F)}$.

By the theorem of Gras 1.5, there is no extension of $L_p(F)$ that is exactly ramified at any non-trivial subfamily of $T = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_n\}$ (see also Remark 1.11). Since $p \nmid \#Cl_{L_p(F)}$, we conclude that $L_p(F) = L^S_{p,T}(F)$. Hence, the result follows. □

References

[1] E. S. Golod and I. R. Šafarevič. *On the class field tower*. Izv. Akad. Nauk SSSR Ser. Mat., 28:261–272, 1964.

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

[3] F. Hajir, C. Maire, R. Ramakrishna, *On Ozaki's theorem realizing prescribed p-groups as p-class tower groups*, Algebra Number Theory **18** no.4 (2024), 771-786.

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

[5] T.Y. Lam, Lectures on Modules and Rings, GTM 189, Springer-Verlag. Berlin Heidelberg, 1999.

[6] C. Maire, *Genus theory and governing fields*, New York Journal of Mathematics **24** (2018), 1056-1067.

[7] C. Maire, *Finitude de tours et p-tours T-ramifiées modérées, S-décomposées*, Journal de Théorie des Nombres de Bordeaux **8** no. 1 (1996), 47-73.

[8] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of Number Fields, GMW 323, Springer-Verlag Berlin Heidelberg, 2000.

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

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

August 9, 2025

Christian Maire, Université Marie et Louis Pasteur, CNRS, Institut FEMTO-ST, F-25000 Besançon, France • *E-mail :* christian.maire@univ-fcomte.fr

Karim Sankara, Nazi Boni University, Bobo-Dioulasso, Burkina Faso & Université Marie et Louis Pasteur, CNRS, Institut FEMTO-ST, F-25000 Besançon, France
E-mail : karim.sankara@femto-st.fr