ON THE SHAFAREVICH GROUP OF RESTRICTED RAMIFICATION EXTENSIONS OF NUMBER FIELDS IN THE TAME CASE

by

Farshid Hajir, Christian Maire, Ravi Ramakrishna

Abstract. — Let K be a number field and S be a finite set of places of K. We study the kernels $Ш^2_S$ of maps $H^2(\mathrm{G}_S,\mathbb{F}_p) \to \oplus_{v\in S} H^2(\mathrm{G}_v,\mathbb{F}_p)$. There is a natural injection $Ш^2_S \hookrightarrow Б_S$, into the dual $Б_S$ of a certain readily computable Kummer group $\mathrm{V}_S/(\mathrm{K}^\times)^p$, which is always an isomorphism in the wild case. The tame case is much more mysterious. Our main result is that given a finite X coprime to $p>2$, there exists a finite set of places S coprime to p such that $Ш^2_{S\cup X} \overset{\simeq}{\hookrightarrow} Б_{S\cup X} \overset{\simeq}{\twoheadleftarrow} Б_X \hookleftarrow Ш^2_X$. In particular, we show that in the tame case $Ш^2_Y$ can *increase* with increasing Y. This is in contrast with the wild case where $Ш^2_Y$ is nonincreasing in dimension with increasing Y. For $p=2$ we prove a slightly weaker unconditional result. With mild hypotheses we prove the full theorem for $p=2$.

Let K be a number field and S be a finite set of places of K. Denote by K_S the maximal extension of K unramified outside S, and set $G_S = \mathrm{Gal}(\mathrm{K}_S/\mathrm{K})$. Given a prime number p, let $Ш^2_S$ be the Shafarevich group associated to G_S and p: it is the kernel of the localization map of the cohomology group $H^2(\mathrm{G}_S,\mathbb{F}_p)$:

$$Ш^2_S := Ш^2(\mathrm{G}_S,\mathbb{F}_p) = \ker\big(H^2(\mathrm{G}_S,\mathbb{F}_p) \to \oplus_{v\in S} H^2(\mathrm{G}_v,\mathbb{F}_p)\big),$$

where G_S acts trivially on $\mathbb{F}_p$ and G_v is the absolute Galois group of the maximal extension of the completion K_v of K at v.

Set

$$\mathrm{V}_S = \{x\in \mathrm{K}^\times, (x) = I^p \text{ as a fractional ideal of } \mathrm{K}; x \in \mathrm{K}_v^p \ \forall v \in S\}$$

and $Б_S = (\mathrm{V}_S/(\mathrm{K}^\times)^p)^\vee$. Clearly $(\mathrm{K}^\times)^p \subset \mathrm{V}_S$ and $S\subset T \implies \mathrm{V}_T \subset \mathrm{V}_S$. It is well-known that $Ш^2_S$ is closely related to $Б_S$. Namely, in the wild case, when S contains all the places above p and all archimedean places, by the Poitou-Tate duality Theorem

The authors thank Georges Gras for helpful discussions and the anonymous referee for her/his comments. This work started when the second author held a visiting scholar position at Cornell University, funded by the program "Mobilité sortante" of the Région Bourgogne Franche-Comté, during the 2017-18 academic year. It has been finished during a visit at Harbin Institute of Technology. CM thanks the Department of Mathematics at Cornell University and the Institute for Advanced Study in Mathematics of HIT for providing beautiful research atmospheres. 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 supported by Simons Collaboration grant #524863. All three authors were supported by Mathematisches Forschunginstitut Oberwolfach for a Research in Pairs visit in January, 2019.

one has $\text{Ш}^2_S \simeq \text{Б}_S$. See for example [**5**, Chapter X, §7]. It is important to note that algorithms exist to compute Б_S via ray class group computations over K, so in the wild case one can, at least in theory, compute $d_p\text{Ш}^2_S$, the dimension of this space. For the more general tame situation, one only has the following injection (due to Shafarevich and Koch, see for example [**3**, Chapter 11, §2] or [**5**, Chapter 10, §7])

$$\text{Ш}^2_S \hookrightarrow \text{Б}_S. \tag{1}$$

Short of computing G_S itself, we know of no algorithm that computes $d_p\text{Ш}^2_S$ in the tame case.

Let us write $\mathrm{K}_S(p)/\mathrm{K}$ as the maximal pro-p extension of K inside K_S, and put $\mathrm{G}_S(p) = \mathrm{Gal}(\mathrm{K}_S(p)/\mathrm{K})$. It is an exercise to see that the quotient $\mathrm{G}_S \twoheadrightarrow \mathrm{G}_S(p)$ induces the injection $\text{Ш}^2_{S,p} \hookrightarrow \text{Ш}^2_S$, where $\text{Ш}^2_{S,p} := \ker\left(H^2(\mathrm{G}_S(p),\mathbb{F}_p) \to \oplus_{v\in S} H^2(\mathrm{G}_v,\mathbb{F}_p)\right)$. As $H^2(\mathrm{G}_v(p),\mathbb{F}_p) \simeq H^2(\mathrm{G}_v,\mathbb{F}_p)$ (see for example [**5**, Chapter VII, §5, Proposition 7.5.8]), we can take G_v instead of $\mathrm{G}_v(p)$.
The Shafarevich group Ш^2_S is central to the study of the maximal pro-p quotient $\mathrm{G}_S(p)$ of G_S, in particular when S is coprime to p: obviously, one gets

$$d_pH^2(\mathrm{G}_S(p),\mathbb{F}_p) \leqslant \sum_{v\in S} d_pH^2(\mathrm{G}_v,\mathbb{F}_p) + d_p\text{Ш}^2_S \leqslant \sum_{v\in S}\delta_{v,p} + d_p\text{Ш}^2_S \leqslant |S| + d_p\mathrm{V}_S/(\mathrm{K}^\times)^p,$$

where $\delta_{v,p} = 1$ or 0 as K_v contains or does not contain the pth roots of unity. This is sufficient to produce criteria involving the infinitess of $\mathrm{G}_S(p)$ (thanks to the Golod-Shafarevich Theorem).

Using (1), one can force Ш^2_S to be trivial (see the notion of saturated set S in §1.2), which can also yield situations where $\mathrm{G}_S(p)$ has cohomological dimension 2. See [**4**] for the first examples and [**6**] for general statements.

Before giving our main result, we make the following observation: given p a prime number, and two finite sets Y and X of places of K, one has:

$$\text{Ш}^2_{Y\cup X,p} \hookrightarrow \text{Ш}^2_{Y\cup X} \hookrightarrow \text{Б}_{Y\cup X} \twoheadleftarrow \text{Б}_X \hookleftarrow \text{Ш}^2_X \hookleftarrow \text{Ш}^2_{X,p} \tag{2}$$

where the middle surjection follows as $\mathrm{V}_{Y\cup X} \subset \mathrm{V}_X$. We only consider the case where the finite places X and Y are coprime to p. Here we prove:

Theorem A. — *Let $p > 2$ be a prime number, and let K be a number field. Let X be a finite set of places of K coprime to p. There exist infinitely many finite sets S of finite places of K, all coprime to p, such that:*

$$\text{Ш}^2_{S\cup X,p} \simeq \text{Ш}^2_{S\cup X} \simeq \text{Б}_{S\cup X} \simeq \text{Б}_X.$$

Moreover such S can be chosen of size $|S| \leqslant d_p\text{Б}_\varnothing$.

The case $p = 2$ involves *an exceptional situation.*

Definition 1. — *The situation is called exceptional if $p = 2$ and if one simultaneously has:*

(*a*) $\zeta_4 \notin \mathrm{K}$,

(*b*) $\mathscr{O}_\mathrm{K}^\times \cap -4\mathrm{K}^4 \neq \varnothing$,

(*c*) *X contains no real place, and for every prime $\mathfrak{p} \in X$ one has $\zeta_4 \in \mathrm{K}_\mathfrak{p}$.*

Observe that if there is a prime $\mathfrak{p}|2$ of K with odd ramification index, (*b*) fails.

Theorem B. — *Take $p=2$. Let X be a finite set of places of* K *coprime to* 2. *Suppose the situation not exceptional. Then the conclusion of Theorem A holds.*
In the exceptional case, one only has:

$$d_2\text{Б}_X - 1 \leqslant d_2\text{Ш}^2_{S\cup X,2} = d_2\text{Ш}^2_{S\cup X} = d_2\text{Б}_{S\cup X} \leqslant d_2\text{Б}_X.$$

Set $m := d_p\text{Б}_{\varnothing}$. From [**5**, §10.7.2], we have the exact sequence

$$0 \to \mathscr{O}_{\mathrm{K}}^{\times}/(\mathscr{O}_{\mathrm{K}}^{\times})^p \to \mathrm{V}_{\varnothing}/\mathrm{K}^{\times p} \to \mathrm{Cl}_{\mathrm{K}}[p] \to 0$$

so $m = d_p\mathrm{Cl}_{\mathrm{K}} + d_p\mathscr{O}_{\mathrm{K}}^{\times}$.

As mentioned above, the computation of Ш^2_S is very difficult in the tame case. Indeed, the only examples we know of where the map $\text{Ш}^2_{\varnothing,p} \hookrightarrow \text{Б}_{\varnothing}$ is *not* an isomorphism are those in which we know the relation rank of $G_{\varnothing}(p)$ by knowing the full group itself. In all our computations $p=2$ and $G_{\varnothing}(p)$ is one of $\mathbb{Z}/2$, $\mathbb{Z}/2\times\mathbb{Z}/2$ and Q_8. Using Theorem A, one may give situations where the value of $|\text{Ш}^2_S|$ is known without being trivial. As a corollary, we get

Corollary A. — *Suppose $p>2$. Then there exist infinitely many finite sets $S_0 \subset S_1 \subset \cdots \subset S_m$ of finite places of* K *all coprime to p, such that for $i=0,\cdots,m$, one has*

$$\text{Ш}^2_{S_i,p} \simeq \text{Ш}^2_{S_i} \simeq (\mathbb{Z}/p)^{m-i}.$$

For $p=2$, the result holds if either (a) or (b) of Definition 1 fails.

Remark. — *We will see that the sets S_i can be explicitly given by applying the Chebotarev density Theorem in some governing field extension over* K. *As we will use $X=\varnothing$, (c) of Definition 1 is not relevant.*

Notations

– We fix a prime number p and a number field K.
– Put $\mathrm{K}' = \mathrm{K}(\zeta_p)$ and $\mathrm{K}'' = \mathrm{K}(\zeta_{p^2})$, where ζ_{p^2} is some primitive p^2th root of unity, and $\zeta_p = \zeta_{p^2}^p$.
– We denote by $\mathscr{O}_{\mathrm{K}}$ the ring of integers of K, by $\mathscr{O}_{\mathrm{K}}^{\times}$ the group of units of $\mathscr{O}_{\mathrm{K}}$, and by Cl_{K} the class group of K.
– We identify a prime ideal $\mathfrak{p} \subset \mathscr{O}_{\mathrm{K}}$ with the place v it defines. We write K_v for the completion of K at v and $\mathscr{U}_v$ for the units of the local field K_v; when v is archimedean, put $\mathscr{U}_v = \mathrm{K}_v^{\times}$.
– One says that a prime ideal $\mathfrak{p}$ is *tame* if $\#\mathscr{O}_{\mathrm{K}}/\mathfrak{p} \equiv 1 (\mathrm{mod}\ p)$, which is equivalent to $\mu_p \subset \mathrm{K}_v$, that is $\delta_{v,p}=1$.
– If S is a finite set of places of K, we denote by $\mathrm{K}_S(p)/\mathrm{K}$ (resp. $\mathrm{K}_S^{ab}(p)/\mathrm{K}$) the maximal pro-$p$ extension (resp. abelian) of K unramified outside S, and we put $\mathrm{G}_S(p) = \mathrm{Gal}(\mathrm{K}_S(p)/\mathrm{K})$ (resp. $\mathrm{G}_S^{ab}(p) = \mathrm{Gal}(\mathrm{K}_S^{ab}(p)/\mathrm{K})$). For $S=\varnothing$, we denote by $\mathrm{H} := \mathrm{K}_{\varnothing}^{ab}(p)$ the Hilbert p-class field of K.
– By convention, the infinite places in S are only real. Let us write $S = S_0 \cup S_\infty$, where S_0 contains only the finite places and S_∞ only the real ones. Put $\delta_{2,p} = \begin{cases} 1 & p=2 \\ 0 & \text{otherwise} \end{cases}$
– The set S is said to be coprime to p, if all finite places v of S are tame; it is said to be tame if S is coprime to p and $S_\infty = \varnothing$.

– Put $\mathrm{V}_S = \{x \in \mathrm{K}^\times, (x) = I^p$ as a fractional ideal of $\mathrm{K}; x \in \mathrm{K}_v^p \ \forall v \in S\}$. Note $\mathrm{K}^{\times p} \subset \mathrm{V}_S$ for all S.

1. Preliminaries

1.1. Extensions with prescribed ramification. — Let p be a prime number.

1.1.1. Governing fields. — We recall a result of Gras-Munnier (see [**1**, Chapter V, §2, Corollary 2.4.2], as well as [**2**]) which gives a criterion for the existence of a totally ramified $\mathbb{Z}/p$-extension at some set S (and unramified outside S). Put $\mathrm{K}' := \mathrm{K}(\zeta_p)$ and consider the governing field $\mathrm{L}' := \mathrm{K}'(\sqrt[p]{\mathrm{V}_\varnothing})$. The extension L'/K' has Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{r_1+r_2-1+\delta+d}$, where $d = d_p \mathrm{Cl}_\mathrm{K}$.

Given a place v of K coprime to p, we choose some place $w|v$ of K' above v, and we consider $\sigma_v \in \mathrm{Gal}(\mathrm{L}'/\mathrm{K}')$ defined as follows:

- if v corresponds to a tame prime ideal $\mathfrak{p}$, and $\mathfrak{P}$ to w, then $\mathfrak{P}$ is unramified in L'/K', and we set $\sigma_v = \sigma_\mathfrak{p} = \left(\dfrac{\mathrm{L}'/\mathrm{K}'}{\mathfrak{P}}\right)$ corresponding to the Frobenius elements at $\mathfrak{P}$ in $\mathrm{Gal}(\mathrm{L}'/\mathrm{K}')$;
- if v corresponds to a real place (when $p = 2$), then σ_v is the Artin symbol at w: $\sigma_v(\sqrt{\varepsilon}) = \varepsilon$ if $\sqrt{\varepsilon}$ is positive at w, and $-\sqrt{\varepsilon}$ otherwise.

While σ_v does in fact depend on the choice of w (and thus $\mathfrak{P}$), it is easy to see, using that $\mathrm{L}' := \mathrm{K}'(\sqrt[p]{\mathrm{V}_\varnothing})$ and $\mathrm{V}_\varnothing$ consists of elements of K, not K', that a different choice changes σ_v by a nonzero multiple in the $\mathbb{F}_p$-vector space $\mathrm{Gal}(\mathrm{L}'/\mathrm{K}')$. This is all we need when invoking Theorem 1.1 below. By abuse, we will also call the σ_v's Frobenius elements.

Theorem 1.1 **(Gras-Munnier)**. — *Let $S = \{v_1, \cdots, v_t\}$ be a set of places of* K *coprime to p. There exists a cyclic degree p extension* L/K*, unramified outside S and totally ramified at each place of S, if and only if, for $i = 1, \cdots, t$, there exists $a_i \in (\mathbb{Z}/p)^\times$, such that*

$$\prod_{i=1}^{t} \sigma_{v_i}^{a_i} = 1 \ \in \mathrm{Gal}(\mathrm{L}'/\mathrm{K}').$$

Remark 1.2. — In fact, Theorem 1.1 is presented in a slightly different form in [**1**], the difference coming from the real places (and then only for $p = 2$). Indeed, one starts with the following: for a real place v, in our context we speak of *ramification*, and in the context of [**1**] Gras speaks of *decomposition*. Hence the governing field in [**1**] is smaller than L' and the condition he obtains did not involve σ_v for $v \in S_\infty$ (in fact, in his case these σ_v are trivial). But the proof is the same, we can follow it without difficulty due to the fact that for $v \in S_\infty$, one has: $\mathscr{U}_v/\mathscr{U}_v^2 = \mathbb{R}^\times/\mathbb{R}^{\times 2} \simeq \mathbb{Z}/2\mathbb{Z}$; see Lemmas 2.3.1, 2.3.2, 2.3.4 and 2.3.5 of [**1**].

1.1.2. Extensions over the Hilbert p-class field of K *that are abelian over* K*.*— As noted in the beginning of Chapter V of [**1**], the result about the existence of a degree-p^e cyclic extension with prescribed ramification can be generalized in different forms. Let H be the Hilbert class field of K. In what follows, we only need the existence of a degree-p^2 cyclic extension of H, abelian over K, with prescribed ramification.

Now we follow the strategy of [**1**, Chapter V, §2, d)]. Since we will focus on the case where the set of ramification contains only finite places, we use the notation $\mathfrak{p}$ instead of v. Take Σ a finite set of tame places of K (not necessarily satisfying the congruence $\mathrm{N}(\mathfrak{p}) \equiv 1 (\bmod p^2)$ when $\mathfrak{p} \in \Sigma$). Put $B = \mathrm{Gal}(\mathrm{K}_\Sigma^{ab}(p)/\mathrm{H})$.
By class field theory, we get

$$1 \longrightarrow (B/B^{p^2})^\vee \xrightarrow{\rho} \bigoplus_{\mathfrak{p}\in\Sigma} (\mathscr{U}_\mathfrak{p}/(\mathscr{U}_\mathfrak{p})^{p^2})^\vee \longrightarrow \big(\iota(\mathscr{O}_\mathrm{K}^\times)\big)^\vee \longrightarrow 1,$$

where $\iota : \mathscr{O}_\mathrm{K}^\times \longrightarrow \bigoplus_{\mathfrak{p}\in\Sigma} \mathscr{U}_\mathfrak{p}/(\mathscr{U}_\mathfrak{p})^{p^2}$ is the diagonal embedding. Observe that $\mathscr{U}_\mathfrak{p}/(\mathscr{U}_\mathfrak{p})^{p^2} \simeq \mathbb{Z}/p^2$ if and only if $\zeta_{p^2} \in \mathscr{U}_\mathfrak{p}$.

A cyclic degree-p^2 extension M of H, abelian over K and unramified outside Σ is given by a character ψ of B/B^{p^2} of order p^2 as follows:
Given $\psi_\mathfrak{p} \in (\mathscr{U}_\mathfrak{p}/(\mathscr{U}_\mathfrak{p})^{p^2})^\vee$ for all $\mathfrak{p} \in \Sigma$, there exists a character ψ of B/B^{p^2} such that $\psi_{|\mathscr{U}_\mathfrak{p}} = \psi_\mathfrak{p}$ if and only if,

$$\forall \varepsilon \in \mathscr{O}_\mathrm{K}^\times,\ \prod_{\mathfrak{p}\in\Sigma} \psi_\mathfrak{p}(\iota_\mathfrak{p}(\varepsilon)) = 1, \tag{3}$$

where $\iota_\mathfrak{p} : \mathscr{O}_\mathrm{K}^\times \to \mathscr{U}_\mathfrak{p}/(\mathscr{U}_\mathfrak{p})^{p^2}$. As M/H is totally ramified at at least one prime ideal, at least one $\psi_\mathfrak{p}$ has order p^2.
Using Kummer theory, we rephrase (3) with the following governing field (see [**1**, Chapter V, §2, d)]):

$$\mathrm{L} = \mathrm{K}''\left(\sqrt[p^2]{\mathscr{O}_\mathrm{K}^\times}\right),$$

where $\mathrm{K}'' = \mathrm{K}(\zeta_{p^2})$. For the clarity of the exposition, let us develop this correspondence. For $\mathfrak{p} \in \Sigma_\mathfrak{q}$, denote by $\mathrm{E}_\mathfrak{p} = \{\varepsilon \in \mathscr{O}_\mathrm{K}^\times, \varepsilon \in ({\mathscr{U}_\mathfrak{p}}^\times)^{p^2}\}$. We then have

$$1 \longrightarrow \mathrm{E}_\mathfrak{p}/(\mathscr{O}_\mathrm{K}^\times)^{p^2} \longrightarrow \mathscr{O}_\mathrm{K}^\times/(\mathscr{O}_\mathrm{K}^\times)^{p^2} \longrightarrow \iota_\mathfrak{p}(\mathscr{O}_\mathrm{K}^\times) \longrightarrow 1.$$

Lemma 1.3. — *For $p = 2$ assume that $\zeta_4 \in \mathrm{K}$. Let $\varepsilon \in \mathscr{O}_\mathrm{K}^\times \cap (\mathrm{K}'')^{p^2}$. Then $\varepsilon \in (\mathscr{O}_\mathrm{K}^\times)^{p^2}$.*

Proof. — One knows that for $p > 2$, $\mathrm{K} \cap (\mathrm{K}'')^{p^2} = \mathrm{K}^{p^2}$ (see [**1**, Chapter II, Theorem 6.3.2]). ☐

For abelian groups M, N contained in a larger group, it is an elementary fact that $MN/N \simeq M/(M \cap N)$. Set $M = \mathscr{O}_\mathrm{K}^\times$ and $N = (\mathrm{K}''^\times)^{p^2}$ so when $p > 2$ or when $\zeta_4 \in \mathrm{K}$ for $p = 2$

$$\mathscr{O}_\mathrm{K}^\times(\mathrm{K}''^\times)^{p^2}/(\mathrm{K}''^\times)^{p^2} \simeq \mathscr{O}_\mathrm{K}^\times/(\mathscr{O}_\mathrm{K}^\times \cap (\mathrm{K}''^\times)^{p^2}) \simeq \mathscr{O}_\mathrm{K}^\times/(\mathscr{O}_\mathrm{K}^\times)^{p^2}.$$

Modding out by $\mathrm{E}_\mathfrak{p}$ and noting $\mathrm{E}_\mathfrak{p} \supseteq (\mathscr{O}_\mathrm{K}^\times)^{p^2}$, we see

$$\mathscr{O}_\mathrm{K}^\times(\mathrm{K}''^\times)^{p^2}/\mathrm{E}_\mathfrak{p}(\mathrm{K}''^\times)^{p^2} \simeq \mathscr{O}_\mathrm{K}^\times/\mathrm{E}_\mathfrak{p} \tag{4}$$

so by Kummer duality,

$$\iota_\mathfrak{p}(\mathscr{O}_\mathrm{K}^\times)^\vee \simeq \big(\mathscr{O}_\mathrm{K}^\times/\mathrm{E}_\mathfrak{p}\big)^\vee \simeq \mathrm{Gal}(\mathrm{L}/\mathrm{K}''(\sqrt[p^2]{\mathrm{E}_\mathfrak{p}}))\cdot \tag{5}$$

Lemma 1.4. — *Take $p = 2$, and let $\mathfrak{p}$ be a tame prime such that $\zeta_4 \in \mathrm{K}_\mathfrak{p}$. Let $\varepsilon \in \mathscr{O}_\mathrm{K}^\times \cap (\mathrm{K}'')^4$. Then $\varepsilon \in ({\mathscr{U}_\mathfrak{p}}^\times)^4$.*

Proof. — If $\varepsilon \notin (\mathscr{O}_{\mathrm{K}}^{\times})^4$, one knows that $\varepsilon = (1+\zeta_4)^4 y^4$ with $y \in \mathrm{K}$ (see [**1**, Chapter II, Theorem 6.3.2]) which implies $x \in (\mathrm{K}_{\mathfrak{p}})^4$ when $\zeta_4 \in \mathrm{K}_{\mathfrak{p}}$. □

Hence Lemma 1.4 shows that (4) and (5) also hold when $\zeta_4 \in \mathrm{K}_{\mathfrak{p}}$.
For each prime $\mathfrak{p} \in \Sigma$ let us choose a prime $\mathfrak{P}|\mathfrak{p}$ of K'', and denote by $\sigma_{\mathfrak{p}}$ the Frobenius of $\mathfrak{P}$ in $\mathrm{Gal}(\mathrm{L}/\mathrm{K}'')$. As before, $\sigma_{\mathfrak{p}}$ depends on $\mathfrak{P}|\mathfrak{p}$ only up to a power coprime to p.
By Lemmas 1.3 and 1.4 (applied to $\mathrm{K}_{\mathfrak{p}}$), the Galois group $\mathrm{Gal}(\mathrm{L}/\mathrm{K}''(\sqrt[p^2]{\mathrm{E}_{\mathfrak{p}}}))$ is generated by $\sigma_{\mathfrak{p}}$. Observe that the dual of the inertia group at $\mathfrak{p}$ in B/B^{p^2} is isomorphic to

$$\ker\left(\left(\mathscr{U}_{\mathfrak{p}}/(\mathscr{U}_{\mathfrak{p}})^{p^2}\right)^{\vee} \twoheadrightarrow \left(\iota_{\mathfrak{p}}(\mathscr{O}_{\mathrm{K}}^{\times})\right)^{\vee}\right),$$

where $\left(\iota_{\mathfrak{p}}(\mathscr{O}_{\mathrm{K}}^{\times})\right)^{\vee} \simeq \mathrm{Gal}(\mathrm{L}/\mathrm{K}''(\sqrt[p^2]{\mathrm{E}_{\mathfrak{p}}})) = \langle\sigma_{\mathfrak{p}}\rangle$. Then there is a generator $\chi_{\mathfrak{p}}$ of $\left(\mathscr{U}_{\mathfrak{p}}/(\mathscr{U}_{\mathfrak{p}})^{p^2}\right)^{\vee}$ which is sent to $\sigma_{\mathfrak{p}}$.

Let us write $\psi_{\mathfrak{p}} = \chi_{\mathfrak{p}}^{a_{\mathfrak{p}}}$. Then via the Kummer duality map, equation (3) implies

$$\prod_{\mathfrak{p}\in\Sigma} \sigma_{\mathfrak{p}}^{a_{\mathfrak{p}}} = 1. \tag{6}$$

We show this is an equivalence. For the reverse, suppose (6) holds. Then it implies the relation $\prod_{\mathfrak{p}\in\Sigma}\theta_{\mathfrak{p}} = 1$ in $\left(\mathscr{O}_{\mathrm{K}}^{\times}(\mathrm{K}'')^{p^2}/(\mathrm{K}'')^{p^2}\right)^{\vee}$, where $\theta_{\mathfrak{p}}$ is a character of $\mathscr{O}_{\mathrm{K}}^{\times}(\mathrm{K}'')^{p^2}/(\mathrm{K}'')^{p^2}$ associated to $\sigma_{\mathfrak{p}}^{a_{\mathfrak{p}}}$, and trivial on $\mathrm{E}_{\mathfrak{p}}(\mathrm{K}'')^{p^2}/(\mathrm{K}'')^{p^2}$; then $\theta_{\mathfrak{p}}$ can be taken in $\left(\mathscr{O}_{\mathrm{K}}^{\times}(\mathrm{K}'')^{p^2}/\mathrm{E}_{\mathfrak{p}}(\mathrm{K}'')^{p^2}\right)^{\vee} \simeq \left(\mathscr{O}_{\mathrm{K}}^{\times}/\mathrm{E}_{\mathfrak{p}}\right)^{\vee} \simeq \left(\iota_{\mathfrak{p}}(\mathscr{O}_{\mathrm{K}}^{\times})\right)^{\vee}$. Now as $\chi_{\mathfrak{p}}$ is sent to $\sigma_{\mathfrak{p}}$, one deduced that $\theta_{\mathfrak{p}} = \chi_{\mathfrak{p}}^{a_{\mathfrak{p}}}$. To conclude, set $\psi_{\mathfrak{p}} := \chi_{\mathfrak{p}}^{a_{\mathfrak{p}}} \circ \iota_{\mathfrak{p}} \in \left(\mathscr{O}_{\mathrm{K}}^{\times}/(\mathscr{O}_{\mathrm{K}}^{\times})^p\right)^{\vee}$, then $\prod_{\mathfrak{p}\in\Sigma}\psi_{\mathfrak{p}}(\varepsilon) = 1$ for every $\varepsilon \in \mathscr{O}_{\mathrm{K}}^{\times}$, and then recover relation (3).

We want to apply this discussion in the following context.
Let S be a finite non-empty set of tame places of K where each prime $\mathfrak{p}$ (corresponding to $v \in S$) is such that $\mathrm{N}(\mathfrak{p}) \equiv 1 (\mathrm{mod}\ p^2)$. We are interested in the existence of a degree-p^2 cyclic extension $\mathrm{K}_{\mathfrak{q}}/\mathrm{H}$, abelian over K and unramified outside $\Sigma := S \cup \{\mathfrak{q}\}$, such that $\mathrm{K}_{\mathfrak{q}}/\mathrm{H}$ has degree p^2 and for which the inertia degree at $\mathfrak{q}$ is exactly p and for some prime in S the inertia degree is p^2.
The above discussion allows us to obtain the following:

Proposition 1.5. — *Let $p > 2$. There exists a degree-p^2 cyclic extension* $\mathrm{K}_{\mathfrak{q}}/\mathrm{H}$*, abelian over* K*, unramified outside $S \cup \{\mathfrak{q}\}$, for which the inertia degree at $\mathfrak{q}$ is exactly p, if and only if, there exists $a_{\mathfrak{q}} \in (\mathbb{Z}/p)^{\times}$, and $b_{\mathfrak{p}} \in \mathbb{Z}/p^2\mathbb{Z}$, $\mathfrak{p} \in S$, such that*

$$\hat{\sigma}_{\mathfrak{q}}^{a_{\mathfrak{q}}} \prod_{\mathfrak{p}\in S} \sigma_{\mathfrak{p}}^{b_{\mathfrak{p}}} = 1 \in \mathrm{Gal}(\mathrm{L}/\mathrm{K}''), \tag{7}$$

where

$$\hat{\sigma}_{\mathfrak{q}} = \begin{cases} \sigma_{\mathfrak{q}} & \text{if } \mathrm{N}(\mathfrak{q}) \not\equiv 1 (\mathrm{mod}\ p^2) \\ \sigma_{\mathfrak{q}}^{p} & \text{if } \mathrm{N}(\mathfrak{q}) \equiv 1 (\mathrm{mod}\ p^2) \end{cases},$$

with at least one $b_{\mathfrak{p}} \in (\mathbb{Z}/p^2\mathbb{Z})^{\times}$. When $p = 2$ the result holds if we assume that $\zeta_4 \in \mathrm{K}_{\mathfrak{q}}$.

Remark 1.6. — Infinitely many such sets exist by the Chebotarev Density Theorem.

The case $p = 2$ involves an exceptional situation.

Lemma 1.7. — *Assume* $\mathscr{O}_{\mathrm{K}}^{\times} \cap -4\mathrm{K}^{4} = \varnothing$. *Let* $\varepsilon \in \mathscr{O}_{\mathrm{K}}^{\times} \cap (\mathrm{K}'')^{p^2}$. *Then* $\varepsilon \in (\mathscr{O}_{\mathrm{K}}^{\times})^{p^2}$.

Proof. — As in the proof of Lemma 1.4, one has $\varepsilon \in (\mathscr{O}_{\mathrm{K}}^{\times})^4$ or $\varepsilon = (1+\zeta_4)^4 y^4$ with $y \in \mathrm{K}$ (see [**1**, Chapter II, Theorem 6.3.2]). The second case would imply that $\varepsilon \in -4\mathrm{K}^4$ which is absurd by assumption. □

Assume now $\mathscr{O}_{\mathrm{K}}^{\times} \cap -4\mathrm{K}^4 = \varnothing$. By Lemma 1.7 the Kummer radical of L/K'' is isomorphic to $\mathscr{O}_{\mathrm{K}}^{\times}/(\mathscr{O}_{\mathrm{K}}^{\times})^2$, and the isomorphism (4) still holds. Then we can follow the discussion before Proposition 1.5 by observing that the main difference is: one only has $\mathrm{E}_{\mathfrak{p}} \subset \mathscr{O}_{\mathrm{K}}^{\times} \cap (\mathrm{K}_{\mathfrak{p}}(\zeta_4))^4$, meaning that $\mathrm{Gal}(\mathrm{L}(\sqrt[4]{\mathscr{O}_{\mathrm{K}}^{\times}})/\mathrm{K}''(\sqrt[4]{\mathrm{E}_{\mathfrak{p}}}))$ contains the decomposition group of $\mathfrak{p}$, but *may be larger*. Let $\sigma'_{\mathfrak{p}}$ be a generator of $\mathrm{Gal}(\mathrm{L}/\mathrm{K}(\sqrt[4]{\mathrm{E}_{\mathfrak{p}}}))$.

Proposition 1.8. — *Suppose* $\mathscr{O}_{\mathrm{K}}^{\times} \cap -4\mathrm{K}^4 = \varnothing$. *Take* $\mathfrak{q}$ *such that* $\zeta_4 \notin \mathrm{K}_{\mathfrak{q}}$.
There exists a degree-4 cyclic extension $\mathrm{K}_{\mathfrak{q}}/\mathrm{H}$, *abelian over* K, *unramified outside* $S \cup \{\mathfrak{q}\}$, *for which the inertia degree at* $\mathfrak{q}$ *is exactly* 2, *if and only if, there exists* $a_{\mathfrak{q}} \in (\mathbb{Z}/2)^{\times}$, *and* $b_{\mathfrak{p}} \in \mathbb{Z}/4\mathbb{Z}$, $\mathfrak{p} \in S$, *such that*

$$(\sigma'_{\mathfrak{q}})^{a_{\mathfrak{q}}} \prod_{\mathfrak{p}\in S} \sigma_{\mathfrak{p}}^{b_{\mathfrak{p}}} = 1 \in \mathrm{Gal}(\mathrm{L}/\mathrm{K}''), \tag{8}$$

with at least one $b_{\mathfrak{p}} \in (\mathbb{Z}/4\mathbb{Z})^{\times}$.

Example 1.9. — Take $\mathrm{K} = \mathbb{Q}$, $p = 2$ and $\mathfrak{p} = (3)$. Then the governing extension is $\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4)$, in which $\mathfrak{p}$ splits. But here $\mathrm{E}_{\mathfrak{p}} = \{1\}$, and $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4, \sqrt[4]{\mathrm{E}_{\mathfrak{p}}})) = \langle \sigma'_{\mathfrak{p}} \rangle \simeq \mathbb{Z}/2$, showing the difference between $\sigma'_{\mathfrak{p}}$ and the Frobenius $\sigma_{\mathfrak{p}}$. Take now the prime 5 which is inert in the governing extension. Proposition 1.8 applies: there exists of a cyclic degree-4 extension of $\mathbb{Q}$, unramified outside $\{3,5\}$, totally ramified at 5 and having inertial degree 2 at 3,

1.2. Saturated sets. — Take p and K as before, and let S be a finite set of places of K, coprime to p.

Definition 1.10. — The S set of places K is called saturated if $\mathrm{V}_S/(\mathrm{K}^{\times})^p = \{1\}$.

Recall the following equality due to Shafarevich (see for example [**5**, Chapter X, §7, Corollary 10.7.7]):

$$d_p\mathrm{G}_S = |S_0| + |S_\infty|\delta_{2,p} - (r_1 + r_2) + 1 - \delta + d_p\mathrm{V}_S/(\mathrm{K}^{\times})^p, \tag{9}$$

showing that $d_p\mathrm{G}_S$ is easy to compute when S is saturated.

Proposition 1.11. — *Let S and T be two finite sets of places of* K *coprime to p. Suppose S is saturated. Then*

- *if $S \subset T$, then T is saturated;*
- *for every tame prime $\mathfrak{p} \notin S$, one has $d_p\mathrm{G}_{S\cup\{\mathfrak{p}\}} = d_p\mathrm{G}_S + 1$.*

Proof. — The first point is due to the fact that $\mathrm{V}_T \subset \mathrm{V}_S$, and the second point is a consequence of (9) along with the first point. □

Theorem 1.12. — *A finite set S coprime to p is saturated if and only if, the Frobenii σ_v, $v \in S$, generate the whole group* $\mathrm{Gal}(\mathrm{K}'(\sqrt[p]{\mathrm{V}_\varnothing})/\mathrm{K}')$.

Proof. — • Suppose the Frobenii generate the full Galois group. By hypothesis, for each degree-p extension L/K' in $\mathrm{K}'(\sqrt[p]{\mathrm{V}_\varnothing})/\mathrm{K}'$, there exists a place $v \in S$ such that v is inert in L/K' (when $v \in S_\infty$, v is ramified in L/K'). Let us take now $x \in \mathrm{V}_S$: then every $v \in S$ splits completely in $\mathrm{K}'(\sqrt[p]{x})/\mathrm{K}'$. As $\mathrm{K}'(\sqrt[p]{x}) \subset \mathrm{K}'(\sqrt[p]{\mathrm{V}_\varnothing})$, one deduces that $\mathrm{K}'(\sqrt[p]{x}) = \mathrm{K}'$, and then $x \in (\mathrm{K}')^p$. As $[\mathrm{K}' : \mathrm{K}]$ is coprime to p, one finally obtains that $x \in (\mathrm{K}^\times)^p$, so $Б_S = \{0\}$.
• If S is saturated, then for every finite set T of tame places of K with $T \cap S = \varnothing$, one has $d_p\mathrm{G}_{S\cup T} = d_p\mathrm{G}_S + |T|$ by Proposition 1.11. Then by the Gras-Munnier criterion, one has $\langle \sigma_v, v \in S\rangle = \mathrm{Gal}(\mathrm{L}'/\mathrm{K}')$. $\square$

Corollary 1.13. — *The finite set S coprime to p is saturated if and only if, for every finite set T of tame places of* K*, there exists a cyclic degree p-extension of* K *unramified outside $S \cup T$ but ramified at each place of T.*

Proof. — • If S is saturated, then by Theorem 1.12 the Frobenii σ_v, $v \in S$, generate $\mathrm{Gal}(\mathrm{L}'/\mathrm{K}')$, and the result follows from Theorem 1.1.
• Suppose that S is such that for every finite set T of tame places of K, there exists a cyclic degree p-extension unramified outside $S \cup T$ and ramified at each place of T. Then by Theorem 1.1 and the Chebotarev density theorem, $\mathrm{Gal}(\mathrm{L}'/\mathrm{K}') = \langle \sigma_v,\ v \in S\rangle$. By Theorem 1.12, S is saturated. $\square$

1.3. A spectral sequence. — Let S and T be two finite sets of places of K coprime to p. Consider the following exact sequence of pro-p groups

$$1 \longrightarrow \mathrm{H}_{S,T} \longrightarrow \mathrm{G}_{S\cup T}(p) \longrightarrow \mathrm{G}_S(p) \longrightarrow 1. \tag{10}$$

Definition 1.14. — Put

$$\mathscr{X}_{S,T} := \mathrm{H}_{S,T}/[\mathrm{H}_{S,T},\mathrm{H}_{S,T}]\mathrm{H}_{S,T}^p,$$

and

$$\mathrm{X}_{S,T} := (\mathscr{X}_{S,T})_{\mathrm{G}_S(p)} = \mathrm{H}_{S,T}/[\mathrm{H}_{S,T},\mathrm{G}_S(p)]\mathrm{H}_{S,T}^p.$$

Recall that as $\mathrm{G}_S(p)$ is a pro-p group, then $\mathbb{F}_p[\![\mathrm{G}_S(p)]\!]$ is a local ring.

Lemma 1.15. — *The abelian group $\mathscr{X}_{S,T}$ is a compact $\mathbb{F}_p[\![\mathrm{G}_S(p)]\!]$-module (with continuous action) that can be topologically generated by $d_p\mathrm{X}_{S,T}$ generators. Moreover, $d_p\mathrm{X}_{S,T} \leqslant |T|$.*

Proof. — The first part follows from the topological Nakayama's lemma. For the second, the fact that $\mathrm{G}_S(p)$ acts transitively on the inertia groups I_w of $w|v \in T$ in $\mathscr{X}(S,T)$ implies

$$\bigoplus_{i=1}^{t} \mathbb{F}_p[\![\mathrm{G}_S(p)]\!] \twoheadrightarrow \langle I_w, w|v \in T\rangle = \mathscr{X}_{S,T},$$

where $t = |T|$. Taking the $\mathrm{G}_S(p)$-coinvariants, we obtain $\mathbb{F}_p^t \twoheadrightarrow \mathrm{X}_{S,T}$. $\square$

Applying the Hochschild-Serre spectral sequence to (10), one gets:

Lemma 1.16. — *Let S,T be two finite sets of places of* K *coprime to p. Then one has :*

$$0 \longrightarrow H^1(\mathrm{G}_S(p),\mathbb{F}_p) \longrightarrow H^1(\mathrm{G}_{S\cup T}(p),\mathbb{F}_p) \longrightarrow \mathrm{X}_{S,T}^\vee \longrightarrow Ш^2_{S,p} \longrightarrow Ш^2_{S\cup T,p}.$$

Furthermore, the cokernel of the natural injection $Ш^2_{X,p} \hookrightarrow Б_X$ is noncreasing in dimension as X increases.

Proof. — The Hochschild-Serre spectral sequence gives the exact commutative diagram:

$$\begin{tikzcd} H^1(\mathrm{G}_S(p),\mathbb{F}_p) \arrow[r, hook] & H^1(\mathrm{G}_{S\cup T}(p),\mathbb{F}_p) \arrow[r] & \mathrm{X}^\vee_{S,T} \arrow[r] & H^2(\mathrm{G}_S(p),\mathbb{F}_p) \arrow[r] \arrow[d] & H^2(\mathrm{G}_{S\cup T}(p),\mathbb{F}_p) \arrow[d] \\ & & & \oplus_{v\in S} H^2(\mathrm{G}_v,\mathbb{F}_p) \arrow[r, hook] & \oplus_{v\in S\cup T} H^2(\mathrm{G}_v,\mathbb{F}_p) \end{tikzcd}$$

Chasing the trangression map $\mathrm{X}^\vee_{S,T} \xrightarrow{tg} H^2(G_S(p))$ to the right gives that its image lies in $Ш^2_{S,p}$ whose image to the right lies in $Ш^2_{S\cup T,p}$. We now have the diagram

$$\begin{tikzcd} 0 \arrow[r] & H^1(\mathrm{G}_S(p),\mathbb{F}_p) \arrow[r] & H^1(\mathrm{G}_{S\cup T}(p),\mathbb{F}_p) \arrow[r] & \mathrm{X}^\vee_{S,T} \arrow[r] & Ш^2_{S,p} \arrow[r] \arrow[d, hook] & Ш^2_{S\cup T,p} \arrow[d, hook] \\ & & & & Б_S \arrow[r, two heads] & Б_{S\cup T} \end{tikzcd}$$

where the bottom horizontal map is surjective as the inclusion $\mathrm{V}_{S\cup T}/(\mathrm{K}^\times)^p \hookrightarrow \mathrm{V}_S/(\mathrm{K}^\times)^p$ is immediate from the definition of V_X. The second result follows. □

Corollary 1.17. — *If the natural injection $Ш^2_{X,p} \hookrightarrow Б_X$ is an isomorphism, then for any set Y we have $Ш^2_{X\cup Y,p} \stackrel{\simeq}{\hookrightarrow} Б_{X\cup Y}$*

Let us give an obvious consequence of Lemma 1.16.

Lemma 1.18. — *Suppose that $H^1(\mathrm{G}_S(p),\mathbb{F}_p) \simeq H^1(\mathrm{G}_{S\cup T}(p),\mathbb{F}_p)$, then $\mathrm{X}^\vee_{S,T} \hookrightarrow Ш^2_{S,p}$. If moreover $S\cup T$ is saturated then $\mathrm{X}^\vee_{S,T} \simeq Ш^2_{S,p}$.*

Proof. — If $S\cup T$ is saturated then $\mathrm{V}_{S\cup T}/(\mathrm{K}^\times)^p = \{1\}$, which implies that $Б_{S\cup T} = \{0\}$. Hence, by (1) $Ш^2_{S\cup T} = \{0\}$, and the same holds for $Ш^2_{S\cup T,p}$. The result follows by Lemma 1.16. □

Remark. — *An important consequence of Lemmas 1.16 and 1.18 is that elements of $\mathrm{X}^\vee_{S,T}$ can give rise to elements of $Ш^2_{S,p}$. The former can be found via ray class group computations. We thus have a method of producing independent elements of $Ш^2_{S,p}$. If we find $d_pБ_S$ such elements, we have established $Ш^2_{S,p} \stackrel{\simeq}{\hookrightarrow} Ш^2_S \stackrel{\simeq}{\hookrightarrow} Б_S$, and thus computed $d_pШ^2_S$.*

2. Proof of the results

2.1. A key Proposition. — Let p be a prime number. Let K be a number field and let X be a finite set of places of K coprime to p. The proof of Theorem 1.1 is a consequence of the following proposition.

Proposition 2.1. — *There exist (infinitely many) pairs of finite sets of tame places S and T of K such that:*

(i) *$T\cup X$ is saturated and $d_p\mathrm{G}_{T\cup X} = d_p\mathrm{G}_X$;*

(ii) *$d_p\mathrm{G}_{S\cup T\cup X} = d_p\mathrm{G}_{S\cup X}$;*

(iii) *$|T| \leqslant d_p\mathrm{Cl}_\mathrm{K} + r_1 + r_2 - 1 + \delta$ and $|S| \leqslant r_1 + r_2 - 1 + \delta$;*

(*iv*) *for each prime* $\mathfrak{q} \in T$*, with at most one exception if we are in the situation of Definition 1, there exists a degree-*p^2 *cyclic extension* M *of* K^H*, abelian over* K*, unramified outside* $S \cup X \cup \{\mathfrak{q}\}$ *where the inertia group at* $\mathfrak{q}$ *is of order* p*.*

Put $\mathrm{F}_0 = \mathrm{K}'(\sqrt[p]{\mathrm{V}_\varnothing})$, $\mathrm{L}_0 = \mathrm{K}'(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times})$, $\mathrm{K}'' = \mathrm{K}(\zeta_{p^2})$, $\mathrm{L}_1 = \mathrm{K}''(\sqrt[p^2]{\mathscr{O}_\mathrm{K}^\times})$, $\mathrm{F}_1 = \mathrm{K}''(\sqrt[p]{\mathrm{V}_\varnothing})$, and $\mathrm{F} = \mathrm{L}\mathrm{F}_0 = \mathrm{K}''(\sqrt[p^2]{\mathscr{O}_\mathrm{K}^\times}, \sqrt[p]{\mathrm{V}_\varnothing})$. Put $\mathrm{G} = \mathrm{Gal}(\mathrm{F}/\mathrm{K}')$.

Proof. — (of Proposition 2.1.)
Given a tame prime $\mathfrak{p}$ of $\mathscr{O}_\mathrm{K}$, we choose a prime $\mathfrak{P}|\mathfrak{p}$ of F, and we consider its Frobenius $\sigma_\mathfrak{p} := \sigma_\mathfrak{P}$ in the Galois group $\mathrm{Gal}(\mathrm{F}/\mathrm{K}')$ and its quotients. In the diagram of part b) below all extensions are abelian so, as mentioned earlier, $\sigma_\mathfrak{P}$ is well-defined up to a nonzero scalar multiple in $\mathrm{Gal}(\mathrm{F}/\mathrm{K}')$ and that is all we need. In part a), $\mathrm{Gal}(\mathrm{F}/\mathrm{K}')$ need not be abelian, but the three drawn squares in the diagram are abelian and it is in these squares where we study the Frobenii, so again they are well-defined up to a nonzero scalar multiple. All extensions in both diagrams are Galois.

Put $E_X = \langle \sigma_{\mathfrak{p}|\mathrm{F}_0}, \mathfrak{p} \in X \rangle \subset \mathrm{Gal}(\mathrm{F}_0/\mathrm{K}')$ the subgroup of $\mathrm{Gal}(\mathrm{F}_0/\mathrm{K}')$ generated by the Frobenii of the primes $\mathfrak{p} \in X$. Put $m_\mathrm{X} = d_p\mathrm{V}_\varnothing - d_p E_X$.

a) Assume first that $\mathrm{F}_0 \cap \mathrm{K}'' = \mathrm{K}'$. When $p = 2$, one has $\mathrm{K} = \mathrm{K}' = \mathrm{K}''$, and then $\zeta_4 \in \mathrm{K}$.

$$\begin{tikzcd}
 & & \mathrm{L} = \mathrm{K}''(\sqrt[p^2]{\mathscr{O}_K^\times}) \arrow[r, dash] \arrow[dl, dash] & \mathrm{F} \arrow[dl, dash] \\
\mathrm{K}'' \arrow[r, dash] \arrow[d, dash] & \mathrm{L}_1 = \mathrm{K}''(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times}) \arrow[r, dash] \arrow[d, dash] & \mathrm{F}_1 = \mathrm{K}''(\sqrt[p]{\mathrm{V}_\varnothing}) \arrow[d, dash] & \\
\mathrm{K}' \arrow[r, dash] & \mathrm{L}_0 = \mathrm{K}'(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times}) \arrow[r, dash] & \mathrm{F}_0 = \mathrm{K}'(\sqrt[p]{\mathrm{V}_\varnothing}) &
\end{tikzcd}$$

We choose S and T as follows:

– let T be *any* set of primes $\mathfrak{q}$ whose Frobenii $\sigma_\mathfrak{q}$ in G are such that the restriction in $\mathrm{Gal}(\mathrm{F}_0/\mathrm{K}')$ forms an $\mathbb{F}_p$-basis of a subspace in direct sum with E_X: in other words,
$$\mathrm{Gal}(\mathrm{F}_0/\mathrm{K}') = \langle \sigma_{\mathfrak{q}|\mathrm{F}_0}, \mathfrak{q} \in T \rangle \bigoplus E_X,$$
and $\langle \sigma_{\mathfrak{q}|\mathrm{F}_0}, \mathfrak{q} \in T \rangle = \bigoplus_{\mathfrak{q} \in T} \langle \sigma_{\mathfrak{q}|\mathrm{F}_0} \rangle$.

– let $\tilde{X}$ be those places of X whose Frobenii lie in $\mathrm{Gal}(\mathrm{F}/\mathrm{F}_1)$ and let S be *any* set of primes $\mathfrak{p}$ whose Frobenii $\sigma_\mathfrak{p}$ in G form in direct sum with the Frobenii in $\tilde{X}$ a basis of $\mathrm{Gal}(\mathrm{F}/\mathrm{F}_1)$.

As $\mathrm{Gal}(\mathrm{F}_1/\mathrm{K}')$ has exponent p, we see for each $\mathfrak{q} \in T$, $\sigma_\mathfrak{q}^p \in \mathrm{Gal}(\mathrm{F}/\mathrm{F}_1)$. Observe also that if $\sigma_{\mathfrak{q}|\mathrm{K}''}$ is not trivial (which is equivalent to $\#\mathscr{O}_\mathrm{K}/\mathfrak{q} \neq 1 \pmod{p^2}$), then $\sigma_\mathfrak{q}^p$ is the Frobenius at $\mathfrak{P}$ in $\mathrm{Gal}(\mathrm{F}/\mathrm{F}'')$; otherwise $\sigma_\mathfrak{q}^p$ is the p-power of the Frobenius at $\mathfrak{Q} \mid \mathfrak{q}$ in $\mathrm{Gal}(\mathrm{F}/\mathrm{F}'')$.

By Theorem 1.12 the set $T \cup X$ is saturated. Moreover thanks to the condition on the direct sum for the Frobenius at $\mathfrak{p} \in T$, by Theorem 1.1, there is no cyclic degree-p extension of K, unramified outside $T \cup X$ and totally ramified at any nonempty subset of places of T: thus $d_p\mathrm{G}_{T\cup X} = d_p\mathrm{G}_X$, and (*i*) holds.

Moreover as each place of S splits completely in the governing extension F_0/K', then again by Theorem 1.1, $d_p\mathrm{G}_{S\cup T\cup X} = d_p\mathrm{G}_{S\cup X}$, and (ii) holds.

The condition on S gives relation (7) in $\mathrm{Gal}(\mathrm{F}/\mathrm{F}_1) \subset \mathrm{Gal}(\mathrm{F}/\mathrm{L}_1)$ for the set $S \cup \tilde{X} \cup \{\mathfrak{q}\}$, $\mathfrak{q} \in T$. After taking the quotient of this relation by $\mathrm{Gal}(\mathrm{F}/\mathrm{L})$, we obtain by Proposition 1.5 that for each prime $\mathfrak{q} \in T$, the existence of a degree-p^2 cyclic extension $\mathrm{K}_\mathfrak{q}/\mathrm{H}$, abelian over K and unramified outside $S \cup X \cup \{\mathfrak{q}\}$ for which the inertia at $\mathfrak{q}$ is of order p, proving (iv).

(iii) is obvious.

b) Assume now that that $\mathrm{K}'' \subset \mathrm{F}_0$.
Let $\mathfrak{A}_i, i = 1, \cdots, d$ be ideals of $\mathscr{O}_\mathrm{K}$, whose classes are a system of minimal generators of $\mathrm{Cl}_\mathrm{K}[p]$, and let $a_i \in \mathscr{O}_\mathrm{K}^\times$ such that $(a_i) = \mathfrak{A}_i^p$. Put $A = \langle a_1, \cdots, a_d\rangle \mathrm{K}^{\times p}/(\mathrm{K}^\times)^p \subset \mathrm{V}_\varnothing/(\mathrm{K}^\times)^p$. Note $\mathrm{K}'(\sqrt[p]{\mathrm{V}_\varnothing}) = \mathrm{K}'(\sqrt[p]{A}, \sqrt[p]{\mathscr{O}_\mathrm{K}^\times})$.
As F_0/K' and K''/K' are abelian p-extensions, the containment $\mathrm{K}'' \subset \mathrm{F}_0$ implies $\mathrm{K}' = \mathrm{K}$.

$$\begin{tikzcd}[arrows=dash]
\mathrm{L} = \mathrm{K}''(\sqrt[p^2]{\mathscr{O}_\mathrm{K}^\times}) \arrow[r] \arrow[d] & \mathrm{F} \arrow[d] \\
\mathrm{L}_0 = \mathrm{K}'(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times}) \arrow[r] \arrow[d] & \mathrm{F}_0 = \mathrm{F}_1 = \mathrm{K}'(\sqrt[p]{\mathrm{V}_\varnothing}) \arrow[d] \\
\mathrm{K}'' \arrow[r] \arrow[d] & \mathrm{K}''(\sqrt[p]{A}) \arrow[d] \\
\mathrm{K}' \arrow[r] & \mathrm{K}'(\sqrt[p]{A})
\end{tikzcd}$$

When $p > 2$, take T and S as in case a).

Now take $p = 2$. One has $\mathrm{K}'' = \mathrm{K}''(\sqrt[4]{\mathscr{O}_\mathrm{K}^\times}) \cap \mathrm{K}''(\sqrt[p]{A})$. Indeed by Kummer theory the intersection is characterized by elements $\varepsilon \in \mathscr{O}_\mathrm{K}^\times$ and $x \in A$ such that $x\varepsilon = \alpha^2$ with $\alpha \in \mathrm{K}''$. If $\alpha \notin \mathrm{K}'$, since $[\mathrm{K}'' : \mathrm{K}'] = 2$, we get $\mathrm{K}'' = \mathrm{K}'(\alpha) = \mathrm{K}'(\sqrt{x\varepsilon})$. By uniqueness of the Kummer radical, one has $x\varepsilon = -y^2$ with $y \in \mathrm{K}'$, and then $(x) = (y)^2$ which implies $x \in A$ trivial; in other words, $\varepsilon \in (\mathrm{K}'')^2$, proving that the intersection is trivial.
We first choose T as in case a) by noting that, with perhaps one exception, the primes $\mathfrak{p} \in T$ can be chosen with norm equal to 1 modulo 4. Observe that there is no exception if the Frobenius of at least one place of X is not trivial in K''/K'. We then choose S as in case a).
For each place $\mathfrak{p} \in T$ for which $\zeta_4 \in \mathrm{K}_\mathfrak{p}$, as in case a), we can apply Proposition 1.5.
Suppose now that there is one prime $\mathfrak{p} \in T$ such that $\zeta_4 \notin \mathrm{K}_\mathfrak{p}$. And assume $\mathscr{O}_\mathrm{K}^\times \cap -4\mathrm{K}^4 = \varnothing$. Due to the remark regarding the linear disjunction, every element $g \in \mathrm{Gal}(\mathrm{L}/\mathrm{L}_0)$ can be lifted in $\mathrm{Gal}(\mathrm{F}/\mathrm{F}_0)$. Then, by Proposition 1.8, one can use the same strategy as in case a).
In conclusion, we have proved that if one of the conditions $(a), (b), (c)$ of the exceptional situation fails then (iv) of Proposition 2.1 applies for **every** $\mathfrak{q} \in T$. $\square$

Remark 2.2. — Observe that one can take T such that $|T| \leqslant m_\mathrm{X} = d_p\mathrm{V}_\varnothing - d_pE_X$.

2.2. Proof of Theorem A and Theorem B. — Suppose $p > 2$ or when $p = 2$, one of the conditions $(a), (b), (c)$ of the exceptional situation fails. Let S and T as in Proposition 2.1. As $X \cup T$ is saturated, by (i) of Proposition 2.1 and (9), one obtains $|T| = d_p Б_X$. Moreover, $S \cup X \cup T$ is also saturated and in particular, $Б_{S\cup X\cup T} \simeq Ш^2_{S\cup X\cup T,p} = \{0\}$. With (ii) of Proposition 2.1, we see that $\mathrm{d}_p Б_{S\cup X} = |T|$ so (i) and (ii) imply: $Б_{S\cup X} \simeq Б_X$. Now let us take the spectral sequence of the short exact sequence

$$1 \longrightarrow \mathrm{H}_{S\cup X,T} \longrightarrow \mathrm{G}_{S\cup X\cup T}(p) \longrightarrow \mathrm{G}_{S\cup X}(p) \longrightarrow 1$$

to obtain by Lemma 1.16:

$$1 \to H^1(\mathrm{G}_{S\cup X}(p),\mathbb{F}_p) \to H^1(\mathrm{G}_{S\cup X\cup T}(p),\mathbb{F}_p) \to \mathrm{X}^\vee_{S\cup X,T} \to Ш^2_{S\cup X,p} \to Ш^2_{S\cup X\cup T,p} = \{0\}.$$

Hence, $\mathrm{X}^\vee_{S\cup X,T} \simeq Ш^2_{S\cup X,p}$. Now (iv) of Proposition 2.1 implies that $d_p\mathrm{X}_{S\cup X,T} \geqslant |T|$, and as obviously $d_p\mathrm{X}_{S\cup X,T} \leqslant |T|$, we finally get $d_pШ^2_{S\cup X,p} = |T|$.
Hence $d_pШ^2_{S\cup X,p} = |T| = d_pБ_{S\cup X} = d_pБ_X$. Thanks to (2), one has

$$Ш^2_{S\cup X,p} \simeq Ш^2_{S\cup X} \simeq Б_{S\cup X} \simeq Б_X.$$

This completes the proof of Theorem A.

Suppose now $p = 2$ and we are in the exceptional situation of Definition 1. Let us choose v_0 a place of K such that v_0 is inert in K''/K (or ramified if v_0 is real). Set $X' = X \cup \{v_0\}$. The situation with such X' is then not exceptional (condition (c) fails), then by the previous result, we get the existence of a set S' such that:

$$Ш^2_{S'\cup X',2} \simeq Ш^2_{S'\cup X'} \simeq Б_{S'\cup X'} \simeq Б_{X'}.$$

Set $S = S' \cup \{v_0\}$. The previous isomorphisms can be reformulated as:

$$Ш^2_{S\cup X,2} \simeq Ш^2_{S\cup X} \simeq Б_{S\cup X} \simeq Б_{X'}.$$

To conclude, let us observe that $d_2Б_X - 1 \leqslant d_2Б_{X'} \leqslant d_2Б_X$.

2.3. Proof of Corollary A. — When (a) or (b) of the exceptional case fails take $X = \varnothing$, otherwise take $X = \{\mathfrak{p}\}$ where $\mathfrak{p}$ is a prime such that $\zeta_4 \notin \mathrm{K}_\mathfrak{p}$. We then avoid the exceptional situation.
Let us choose S and T as in proof of Proposition 2.1. Let us write $T = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_{m_X}\}$, where $m_X = d_pБ_\varnothing - d_pE_X$. Put $S_0 = S \cup X$ and, for $i \geqslant 0$, $S_{i+1} = S \cup X \cup \{\mathfrak{p}_i\}$. Here, as $d_p\mathrm{G}_{S_i} = d_p\mathrm{G}_{S_{m_X}}$, the spectral sequence shows that

$$\mathbb{Z}/p \hookrightarrow Ш^2_{S_i,p} \longrightarrow Ш^2_{S_{i+1},p}, \tag{11}$$

in particular $d_pШ^2_{S_i,p} \leqslant d_pШ^2_{S_{i+1},p} + 1$. After noting that $d_pШ^2_{S_{m_X},p} = 0$ (the set $X \cup T$ is saturated) and that $d_pШ^2_{S_0,p} = |T| = m_X$, then we conclude that $d_pШ^2_{S_i,p} = m_\mathrm{X} - i$. Observe also that (11) induces:

$$\mathbb{Z}/p \hookrightarrow Ш^2_{S_i} \longrightarrow Ш^2_{S_{i+1}},$$

and as before $d_pШ^2_{S_i} = m - i$. The isomorphisms $Ш^2_{S_i,p} \simeq Ш^2_{S_i}$'s become obvious.
We have proved:

Corollary 2.3. — *One has* $Ш^2_{S_i} \simeq (\mathbb{Z}/p)^{m_X - i}$.

Take $X = \varnothing$ to have Corollary A. To be complete, observe that when $X = \{\mathfrak{p}\}$, one has $m_X = m - 1$.

3. Examples

In this section we give a few examples of fields K and sets S such that in the diagram

$$Ш^2_\varnothing \hookrightarrow Б_\varnothing \twoheadrightarrow Б_S \hookleftarrow Ш^2_S,$$

the two maps on the right are isomorphisms. Here $p = 2$, and the three examples we give are not exceptional situations.

In our first two examples we show the left map is *not* an isomorphism. Thus we give explicit examples where $Ш^2_X$ increases as X does, in contrast to the wild case.

In the third example we establish

$$Ш^2_\varnothing \hookrightarrow Б_\varnothing \overset{\simeq}{\twoheadrightarrow} Б_S \overset{\simeq}{\hookleftarrow} Ш^2_S,$$

but do not know whether $d_pШ^2_\varnothing < d_pШ^2_S$. Indeed, we suspect equality in that case.

In the examples below, p_i refers to the ith prime of K above the rational prime p as MAGMA presents the factorization. All code was run unconditionally, that is we did *not* use GRH bounds for computing ray class groups.

Example 1. — *Let* K *be the unique degree* 3 *subfield of* $\mathbb{Q}(\zeta_7)$ *and let* $p = 2$. *Then one can easily compute that* K *has trivial class group and, since* K *is totally real,* $d_pБ_\varnothing = d_p\mathscr{O}^\times_{\mathrm{K}}/\mathscr{O}^{\times 2}_{\mathrm{K}} + d_p\mathrm{Cl}_{\mathrm{K}}[2] = 3$. *Clearly* $\mathrm{G}_\varnothing = \{e\}$ *and* $d_pШ^2_\varnothing = 0$ *so* $Ш^2_\varnothing \hookrightarrow Б_\varnothing$ *has* 3*-dimensional cokernel. Set* $S = \{37_1, 181_1, 293_1\}$ *and* $T = \{307_1, 311_1, 349_1\}$. *One computes* $d_pH^1(\mathrm{G}_T, \mathbb{F}_2) = 0$ *so* T *and* $S \cup T$ *are saturated. The* 2*-parts of the ray class groups for conductors* $S \cup T$ *and* S *are* $(\mathbb{Z}/4)^3$ *and* $(\mathbb{Z}/2)^3$ *respectively, so the the map* $H^1(\mathrm{G}_S, \mathbb{F}_2) \to H^1(\mathrm{G}_{S\cup T}, \mathbb{F}_2)$ *is an isomorphism and* $d_p\mathrm{X}^\vee_{S\cup X,T} \geqslant 3$. *As* $d_pШ^2_S \leqslant d_pБ_S \leqslant d_pБ_\varnothing = 3$, *we see* $d_pШ^2_S = 3$.

Example 2. — *Let* K *be the unique degree* 3 *subfield of* $\mathbb{Q}(\zeta_{349})$ *and let* $p = 2$. *Here* K *has class group* $(\mathbb{Z}/2)^2$ *and is again totally real, so* $d_pБ_\varnothing = d_p\mathscr{O}^\times_{\mathrm{K}}/\mathscr{O}^{\times 2}_{\mathrm{K}} + d_p\mathrm{Cl}_{\mathrm{K}}[2] = 5$. *One computes the class group of the Hilbert class field of* K *is trivial so* $\mathrm{G}_\varnothing = \mathbb{Z}/2 \times \mathbb{Z}/2$ *and has three relations. Thus* $d_pШ^2_\varnothing = d_pH^2(\mathrm{G}_\varnothing, \mathbb{F}_2) = 3$ *so the map* $Ш^2_\varnothing \hookrightarrow Б_\varnothing$ *has* 2*-dimensional cokernel. Set* $S = \{701_1, 2857_1, 3169_1\}$ *and* $T = \{367_1, 397_1, 401_1, 409_1, 449_1\}$. *One computes* $d_pH^1(\mathrm{G}_T, \mathbb{F}_2) = 2$ *so* T *and* $S\cup T$ *are saturated. The* 2*-parts of the ray class groups for conductors* $S\cup T$ *and* S *are* $\mathbb{Z}/4 \times (\mathbb{Z}/8)^2 \times \mathbb{Z}/16 \times \mathbb{Z}/32$ *and* $(\mathbb{Z}/2)^5$ *respectively, so the the map* $H^1(\mathrm{G}_S, \mathbb{F}_2) \to H^1(\mathrm{G}_{S\cup T}, \mathbb{F}_2)$ *is an isomorphism and* $d_p\mathrm{X}^\vee_{S\cup X,T} \geqslant 5$. *As* $d_pШ^2_S \leqslant d_pБ_S \leqslant d_pБ_\varnothing = 5$, *we see* $d_pШ^2_S = 5$.

Example 3. — *Let* $\mathrm{K} = \mathbb{Q}[x]/(f(x))$ *where* $f(x) = x^{12} + 339x^{10} - 19752x^8 - 2188735x^6 + 284236829x^4 + 4401349506x^2 + 15622982921$. *This polynomial is irreducible and* K *is totally complex with small root discriminant and has class group* $(\mathbb{Z}/2)^6$. *The field* K *has been used as a starting point in finding infinite towers of totally complex number fields whose root discriminants are the smallest currently known. Set*

$$S = \{7_2, 11_1, 43_1, 47_3, 67_3, 97_1\},\ T = \{5_1, 13_1, 19_1, 19_2, 23_1, 23_2, 23_3, 29_1, 31_1, 61_1, 149_1, 149_4\}.$$

As K *is totally complex,*

$$d_pБ_\varnothing = d_p\mathscr{O}^\times_{\mathrm{K}}/\mathscr{O}^{\times 2}_{\mathrm{K}} + d_pCl_{\mathrm{K}}[2] = 6 + 6 = 12 = \#T.$$

One computes $d_pH^1(\mathrm{G}_T, \mathbb{F}_2) = 6$ *so* T *and* $S \cup T$ *are saturated. The* 2*-parts of the ray class groups for conductors* $S\cup T$ *and* S *are* $(\mathbb{Z}/4)^5 \times (\mathbb{Z}/8)^4 \times (\mathbb{Z}/16)^3$ *and* $(\mathbb{Z}/2)^{11} \times \mathbb{Z}/8$. *respectively, so the the map* $H^1(\mathrm{G}_S, \mathbb{F}_2) \to H^1(\mathrm{G}_{S\cup T}, \mathbb{F}_2)$ *is an isomorphism. From this* *data one can only conclude* $d_p\text{X}^\vee_{S\cup X,T} \geqslant 11$*. On the other hand, for every* $v \in T$ *one computes the* 2*-part of the ray class group for conductor* $S \cup \{v\}$ *has order at least* $2^{15} > 2^{14}$*. As the latter quantity is the order of the* 2*-part of the ray class group with conductor* S*, we get* $\#T = 12$ *independent elements of* $\text{X}^\vee_{S\cup X,T}$ *so* $d_p\text{Ш}^2_S \geqslant 12$*. As* $d_p\text{Б}_S \leqslant d_p\text{Б}_\varnothing = 12$*, we have* $d_p\text{Ш}^2_S = 12$*. We suspect that in this case* $d_p\text{Ш}^2_\varnothing = 12$*.*

References

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

[2] G. Gras and A. Munnier, *Extensions cycliques T-totalement ramifiées*, Publ. Math. Besançon, 1997/98.

[3] H. Koch, Galoissche Theorie der p-Erweiterungen, Deutscher Verl. der Wiss. Berlin, 1970.

[4] J. Labute, *Mild pro-p-groups and Galois groups of p-extensions of* $\mathbb{Q}$, J. reine u. angew. Math. **596** (2006), 155–182.

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

[6] A. Schmidt, *Über Pro-p-Fundamentalgruppen markierter arithmetischer Kurven*, J. reine u. angew. Math. **640** (2010), 203-235.

September 8, 2020

FARSHID HAJIR, CHRISTIAN MAIRE, RAVI RAMAKRISHNA, Department of Mathematics and Statistics, University of Massachusetts, Amherst, MA 01003, USA • FEMTO-ST Institute, Université Bourgogne Franche-Comté, CNRS, 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