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 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 V_S, 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, 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 size with increasing Y.

Let K be a number field, and let 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 2-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 $\mathbb{F}_p$. We denote by G_v the absolute Galois group of the maximal extension of the completion K_v of K at v.

It is well-known that $Ш^2_S$ is closely related to $Б_S = (\mathrm{V}_S/\mathrm{K}^{\times p})^\vee$, where

$$\mathrm{V}_S = \{x \in \mathrm{K}^\times, v(x) \equiv 0 \pmod p\ \forall v; x \in \mathrm{K}_v^p\ \forall v \in S\}.$$

Clearly $\mathrm{K}^{\times p} \subset \mathrm{V}_S$ and $S \subset T \implies \mathrm{V}_T \subset \mathrm{V}_S$. Namely, in the wild case, when S contains all the places above p and all archimedean places, by Poitou-Tate duality Theorem one has $Ш^2_S \simeq Б_S$. 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 $\mathrm{K}(\mu_p)$, so in the wild case one can, at least in theory, compute $d_p Ш^2_S$. For the more general tame situation, one only

This work started when the second author held 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 a 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.

has the following injection (due to Shafarevich and Koch, see for example [**3**, Chapter 11, §2] or [**5**, Chapter 10, §7])

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

At present there is no general algorithm to compute $d_p Ш^2_S$ *in the tame case, short of computing* G_S *itself.*

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 the quotient $\mathrm{G}_S \twoheadrightarrow \mathrm{G}_S(p)$ induces the injection $Ш^2_{S,p} \hookrightarrow Ш^2_S$, where $Ш^2_{S,p} := \ker\left(H^2(\mathrm{G}_S(p),\mathbb{F}_p) \to \oplus_{v\in S} H^2(\mathrm{G}_v,\mathbb{F}_p)\right)$. Observe that we can take $\mathrm{G}_v(p)$ instead of G_v, due to the fact that $H^2(\mathrm{G}_v(p),\mathbb{F}_p) \simeq H^2(\mathrm{G}_v,\mathbb{F}_p)$ (see for example [**5**, Chapter VII, §5]).
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

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

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

Observe that thanks to (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 S and X of places of K, one has:

$$Ш^2_{S\cup X,p} \hookrightarrow Ш^2_{S\cup X} \hookrightarrow Б_{S\cup X} \twoheadleftarrow Б_X \hookleftarrow Ш^2_X \hookleftarrow Ш^2_{X,p} \tag{2}$$

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

Theorem A. — *Let p 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:*

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

Moreover such S can be chosen of size $|S| \leqslant d_p Б_\varnothing$.

Set $m := d_p Б_\varnothing$. Note $\mathrm{K}^{\times p} \subset \mathrm{V}_S$ for all S. In particular, we have the exact sequence

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

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 $Ш^2_{\varnothing,p} \hookrightarrow Б_\varnothing$ is *not* an isomorphism are those in which we know the relation rank of $G_\varnothing(p)$ by knowing the full group itself. Using Theorem A, one may give situations where the value of $|Ш^2_S|$ is known without being trivial. As corollary, we get

Corollary A. — *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*

$$Ш^2_{S_i,p} \simeq Ш^2_{S_i} \simeq \mathbb{F}_p^{m-i}.$$

Remark. — *We will see that the sets S and S_i can be explicitly given by the Chebotarev density Theorem in some governing field extension over* K*.*

Remark. — *Let $\mathrm{K}_S^{ta}/\mathrm{K}$ be the maximal Galois extension of* K*, unramified outside S, and tamely ramified at S; put $\mathrm{G}_S^{ta} = \mathrm{Gal}(\mathrm{K}_S^{ta}/\mathrm{K})$. Then instead of considering G_S one may consider G_S^{ta} which also surjects onto $\mathrm{G}_S(p)$. Observe here that G_S^{ta} may be finite (typically when the discriminant of* K *and the norm of prime ideals of S are too small), even trivial (for example when $\mathrm{K} = \mathbb{Q}$ and $S = \emptyset$).*

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 $S = \emptyset$, we denote by $\mathrm{H} := \mathrm{K}_\emptyset^{ab}(p)$ 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_0 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 coprime to p; it is said to be tame if S is coprime to p and $S_\infty = \emptyset$.
– Put $\mathrm{V}_S = \{x \in \mathrm{K}^\times, v(x) \equiv 0\ (\mathrm{mod}\ p)\ \forall v; x \in \mathrm{K}_v^p\ \forall v \in S\}$. 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 totally ramified p-extension at some set S (and unramified outside S). Put $\mathrm{K}' := \mathrm{K}(\zeta_p)$ and consider the governing field $\mathrm{L}' := \mathrm{K}'(\sqrt[p]{\mathrm{V}_\emptyset})$. 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, we choose some place $w|v$ of L' above v, and we consider $\sigma_v \in \mathrm{Gal}(\mathrm{L}'/\mathrm{K}')$ defined as follows:

– if v corresponds to a prime ideal $\mathfrak{p}$ coprime to p, and $\mathfrak{P}$ to w, then $\mathfrak{P}$ is unramified in L'/K', and then $\sigma_v = \sigma_{\mathfrak{p}} = \left(\dfrac{\mathrm{L}'/\mathrm{K}'}{\mathfrak{P}}\right)$ corresponds to the Frobenius elements at $\mathfrak{P}$ in $\mathrm{Gal}(\mathrm{L}'/\mathrm{K}')$;
– if v corresponds to a real place, then σ_v is the Artin symbol at w: $\sigma_v(\sqrt{\varepsilon}) = +1$ is ε is positive at w, and -1 otherwise.

While σ_v does in fact depend on the choice of $\mathfrak{P}$, it is easy to see a different choice of $\mathfrak{P}$ gives a nonzero multiple of the previous choice of σ_v 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 $a_i \in \mathbb{F}_p^\times$, such that*

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

When S is as in the Gras-Munnier criterion, i.e. the necessary and sufficient condition of the theorem holds, one says that the elements σ_{v_i} satisfy a *strongly nontrivial relation*. When one only has $\prod_{i=1}^{t} \sigma_{v_i}^{a_i} = 1$, with the a_i not all zero, one says that the σ_{v_i}'s satisfy a *nontrivial relation*.

Remark 1.2. — In fact, we don't find Theorem 1.1 in [**1**] in this form, 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 the σ_v's, $v \in S_\infty$ (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**].

Remark 1.3. — The results of [**1**] allow us to also obtain the following: put $\mathrm{L}'_0 := \mathrm{K}'(\sqrt[p]{\mathscr{O}_\mathrm{K}^\times})$, then $\#\mathrm{G}_S^{ab}(p) > \#\mathrm{G}_\varnothing^{ab}(p)$ if and only if, there exists some nontrivial relation in $\mathrm{Gal}(\mathrm{L}'_0/\mathrm{K}')$ between the σ_v's, $v \in S$. See also Proposition 1.5.

As consequence of Theorem 1.1, one has:

Corollary 1.4. — *Given p and* K*, and two finite sets T and S of places of* K *coprime to p, there exists a cyclic degree p extension* L/K*, unramified outside $S \cup T$ and ramified at each place of S (no condition on the places of T), if and only if the σ_v's for $v \in S$ satisfy a strongly nontrivial relation in the quotient* $\mathrm{Gal}(\mathrm{L}'/\mathrm{K}')/\langle \sigma_v, v \in T\rangle$.

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)]. Put $B = \mathrm{Gal}(\mathrm{K}_S^{ab}(p)/\mathrm{H})$. Take Σ a finite set of places of K coprime to p (not necessarily satisfying the congruence $\mathrm{N}(\mathfrak{p}) \equiv 1(\bmod\ p^2)$ when $\mathfrak{p} \in \Sigma_0$). By class field theory, we get

$$1 \longrightarrow (B/B^{p^2})^* \xrightarrow{\rho} \bigoplus_{v\in\Sigma} (\mathscr{U}_v/(\mathscr{U}_v)^{p^2})^* \longrightarrow \left(\iota(\mathscr{O}_{\mathrm{K}}^\times)\right)^* \longrightarrow 1,$$

where $\iota : \mathscr{O}_{\mathrm{K}}^\times \longrightarrow \bigoplus_{v\in\Sigma} \mathscr{U}_v/(\mathscr{U}_v)^{p^2}$ is the diagonal embedding.

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 $\psi_v \in (\mathscr{U}_v/(\mathscr{U}_v)^{p^2})^*$ for all $v \in \Sigma$, there exists a character ψ of B/B^{p^2} such that $\psi_{|\mathscr{U}_v} = \psi_v$ if and only if,

$$\forall \varepsilon \in \mathscr{O}_{\mathrm{K}}^\times,\ \prod_{v\in\Sigma} \psi_v(\varepsilon) = 1. \tag{3}$$

As M/H is totally ramified at at least one prime ideal, at least one ψ_v has order p^2.

Now we will focus on the case where Σ contains only finite places, and we use the notation $\mathfrak{p}$ instead of v.

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 $\mathrm{N}(\mathfrak{q}) \equiv 1(\bmod\ p^2)$. Let us write now $\Sigma_\mathfrak{q} = S \cup T_\mathfrak{q}$, where $T_\mathfrak{q} = \{\mathfrak{q}\}$ is also tame. 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 $\Sigma_\mathfrak{q}$, such that $\mathrm{K}_\mathfrak{q}/\mathrm{H}$ has degree p^2 and for which the inertia degree at $\mathfrak{q}$ is exactly p.
For $\mathfrak{p} \in \Sigma_\mathfrak{q}$, let us fix $\chi_\mathfrak{p}$ a generator of $(\mathscr{U}_\mathfrak{p}/(\mathscr{U}_\mathfrak{p})^{p^2})^*$. By (3), $\mathrm{K}_\mathfrak{q}$ exists if and only if, there exist $a_\mathfrak{q} \in \mathbb{F}_p^\times$, and $b_\mathfrak{p} \in \mathbb{Z}/p^2$, $\mathfrak{p} \in S$, such that

$$\forall \varepsilon \in \mathscr{O}_{\mathrm{K}}^\times,\ \hat{\chi}_\mathfrak{q}^{a_\mathfrak{q}}(\varepsilon) \prod_{\mathfrak{p}\in S} \chi_\mathfrak{p}^{b_\mathfrak{p}}(\varepsilon) = 1,$$

where

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

and such that at least one $b_\mathfrak{p} \in (\mathbb{Z}/p^2\mathbb{Z})^\times$.
This last condition can be rephrased thanks to Kummer theory with the following governing field (see [**1**, Chapter V, §2, d)]):

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

where $\mathrm{K}'' = \mathrm{K}(\zeta_{p^2})$. For each prime $\mathfrak{p} \in \Sigma_\mathfrak{q}$ 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.
The above discussion allows us to obtain the following:

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

$$\hat{\sigma}_\mathfrak{q}^{a_\mathfrak{q}} \prod_{\mathfrak{p}\in S} \sigma_\mathfrak{p}^{b_\mathfrak{p}} = 1 \in \mathrm{Gal}(\mathrm{L}/\mathrm{K}''), \tag{4}$$

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 $b_{\mathfrak{p}} \in (\mathbb{Z}/p^2\mathbb{Z})^\times$.

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

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

Definition 1.6. — 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]):

$$d_p\mathrm{G}_S = |S_0| + |S_\infty|\delta_{2,p} - (r_1 + r_2) + 1 - \delta + d_p\mathrm{V}_S/(\mathrm{K}^\times)^p, \tag{5}$$

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

Proposition 1.7. — *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 place $v \notin S$, 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 (5) along with the first point. □

Theorem 1.8. — *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 totally 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 1.7. Then by the Gras-Munnier criterion, one has $\langle \sigma_v, v \in S\rangle = \mathrm{Gal}(\mathrm{L}'/\mathrm{K}')$. □

Corollary 1.9. — *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 1.8 the Frobenii σ_v, $v \in S$, generate $\mathrm{Gal}(\mathrm{L}'/\mathrm{K}')$, and the result follows by using Corollary 1.4.
• 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 Corollary 1.4 and the Chebotarev density theorem, $\mathrm{Gal}(\mathrm{L}'/\mathrm{K}') = \langle \sigma_v,\ v \in S\rangle$. By Theorem 1.8, S is saturated. □

1.3. 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

$$1 \longrightarrow \mathrm{H}_{S,T} \longrightarrow \mathrm{G}_{S\cup T}(p) \longrightarrow \mathrm{G}_S(p) \longrightarrow 1. \tag{6}$$

Definition 1.10. — 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 1.11. — *The abelian group $\mathscr{X}_{S,T}$ is a $\mathbb{F}_p[\![\mathrm{G}_S(p)]\!]$-module (with continuous action) that can be generated by $d_p\mathrm{X}_{S,T}$ generators. Moreover, $d_p\mathrm{X}_{S,T} \leqslant |T|$.*

Proof. — The first part follows from 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 $\mathbb{F}_p^t \twoheadrightarrow \mathrm{X}_{S,T}$. □

Applying the Hochschild-Serre spectral sequence to (6), one gets:

Lemma 1.12. — *Let S, T be two finite sets of places of K coprime to p. Then one has :*

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

Furthermore, the cokernel of the natural injection $Ш_{X,p} \hookrightarrow Б_X$ decreases in dimension as X increases.

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

$$\begin{array}{ccccccccc}
H^1(\mathrm{G}_S(p),\mathbb{F}_p) & \hookrightarrow & H^1(\mathrm{G}_{S\cup T}(p),\mathbb{F}_p) & \longrightarrow & \mathrm{X}_{S,T}^\vee & \longrightarrow & H^2(\mathrm{G}_S(p),\mathbb{F}_p) & \longrightarrow & H^2(\mathrm{G}_{S\cup T}(p),\mathbb{F}_p) \\
 & & & & & & \downarrow & & \downarrow \\
 & & & & & & \oplus_{v\in S} H^2(\mathrm{G}_v,\mathbb{F}_p) & \hookrightarrow & \oplus_{v\in S\cup T} H^2(\mathrm{G}_v,\mathbb{F}_p)
\end{array}$$

Chasing the trangression map $\mathrm{X}_{S,T}^\vee \xrightarrow{tg} H^2(G_S(p))$ 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

$$\begin{array}{ccccccccc}
1 \longrightarrow H^1(\mathrm{G}_S(p),\mathbb{F}_p) & \longrightarrow & H^1(\mathrm{G}_{S\cup T}(p),\mathbb{F}_p) & \longrightarrow & \mathrm{X}_{S,T}^\vee & \longrightarrow & Ш^2_{S,p} & \longrightarrow & Ш^2_{S\cup T,p} \\
 & & & & & & \downarrow & & \downarrow \\
 & & & & & & Б_S & \twoheadrightarrow & Б_{S\cup T}
\end{array}$$

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 1.13. — *If the natural injection $Ш_{X,p} \hookrightarrow Б_X$ is an ismorphism, then for any set Y we have $Ш_{X\cup Y,p} \overset{\simeq}{\hookrightarrow} Б_{X\cup Y}$*

Let us give an obvious consequence of Lemma 1.12.

Lemma 1.14. — *Suppose that $H^1(\mathrm{G}_S(p),\mathbb{F}_p) \simeq H^1(\mathrm{G}_{S\cup T}(p),\mathbb{F}_p)$, then $\mathrm{X}_{S,T}^\vee \hookrightarrow Ш^2_{S,p}$. If moreover $S \cup T$ is saturated then $\mathrm{X}_{S,T}^\vee \simeq Ш^2_{S,p}$.*

Proof. — If $S \cup T$ is saturated then $\mathrm{V}_{S\cup T}/\mathrm{K}^{\times p} = \{1\}$, which implies that $Б_{S\cup T} = \{1\}$. Hence, by (1) $Ш^2_{S\cup T} = \{0\}$, and the same holds for $Ш^2_{S\cup T,p}$. We conclude with Lemma 1.12. □

An important consequence of Lemmas 1.12 and 1.14 is that elements of $\mathrm{X}_{S,T}^\vee$ 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 $d_p Б_S$ such elements, we have established $Ш^2_{S,p} \overset{\simeq}{\hookrightarrow} Ш^2_S \overset{\simeq}{\hookrightarrow} Б_S$, and thus computed $d_p Ш^2_S$.

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:*

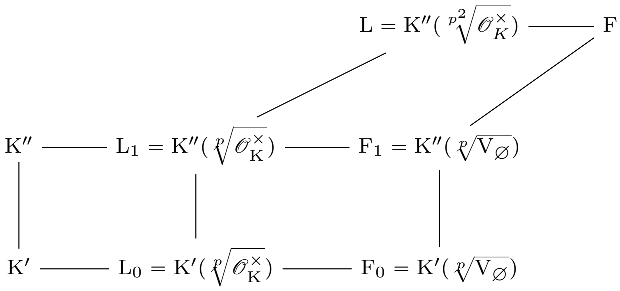
- *(i)* $T \cup X$ *is saturated and* $d_p\mathrm{G}_{T\cup X} = d_p\mathrm{G}_X$*;*
- *(ii)* $d_p\mathrm{G}_{S\cup T\cup X} = d_p\mathrm{G}_{S\cup X}$*;*
- *(iii)* $|T| \leqslant d_p\mathrm{Cl}_\mathrm{K} + r_1 + r_2 - 1 + \delta$ *and* $|S| \leqslant r_1 + r_2 - 1 + \delta$*;*
- *(iv) for each prime $\mathfrak{q} \in T$, there exists a degree-p^2 cyclic extension $\mathrm{K}_\mathfrak{q}$ 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 prime $\mathfrak{p}$ of $\mathscr{O}_\mathrm{K}$, coprime to p, 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. As mentioned earlier, this is well-defined up to a nonzero scalar multiple in $\mathrm{Gal}(\mathrm{F}/\mathrm{K}')$ and that is all we need.

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 $m_\mathrm{X} = d_p\mathrm{V}_\varnothing - d_pE_X$.

a) Assume first that $\mathrm{F}_0 \cap \mathrm{K}'' = \mathrm{K}'$.



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 $\mathrm{N}(\mathfrak{q}) \neq 1 \pmod{p^2}$), 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 $\mathrm{Gal}(\mathrm{F}/\mathrm{F}'')$.

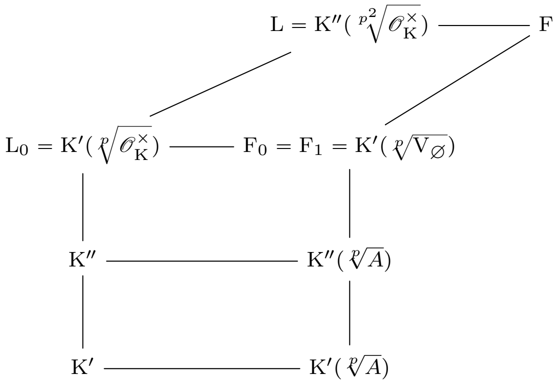
By Theorem 1.8 the set $T \cup X$ is saturated. Moreover thanks to the condition on the direct sum for the Frobenius at $\mathfrak{p} \in T$, by Theorem 1.1, there is no cyclic degree-p extension of K, unramified outside $T \cup X$ and totally ramified at any nonempty subset of places of T: thus $d_p\mathrm{G}_{T\cup X} = d_p\mathrm{G}_X$, and (i) holds.

Moreover as each place of S splits totally 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 a relation of type (4) 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 $\mathrm{K}' = \mathrm{K}$.
Moreover $\mathrm{L}_0 \cap \mathrm{K}''(\sqrt[p]{A}) = \mathrm{K}''$.



Now take T and S as in case a). □

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. — Let S and T as in Proposition 2.1. As $X \cup T$ is saturated, by (i) of Proposition 2.1 and (5), 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), 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 1.12:

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

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 $d_p Ш^2_{S\cup X,p} = |T|$.

Hence $d_p Ш^2_{S\cup X,p} = |T| = d_p Б_{S\cup X} = d_p Б_X$. Thanks to (2), one has

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

2.3. Proof of Corollary A. — 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 $m_X = d_p Б_\varnothing - d_p E_X$. 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

$$\mathbb{F}_p \hookrightarrow Ш^2_{S_i,p} \longrightarrow Ш^2_{S_{i+1},p}, \tag{7}$$

in particular $d_p Ш^2_{S_i,p} \leqslant d_p Ш^2_{S_{i+1},p} + 1$. After noting that $d_p Ш^2_{S_{m_X},p} = 0$ (the set $X \cup T$ is saturated) and that $d_p Ш^2_{S_0,p} = |T| = m_X$, then we conclude that $d_p Ш^2_{S_i,p} = m_{\mathrm{X}} - i$. Observe also that (7) induces:

$$\mathbb{F}_p \hookrightarrow Ш^2_{S_i} \longrightarrow Ш^2_{S_{i+1}},$$

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

We have proved:

Corollary 2.3. — *One has* $Ш^2_{S_i} \simeq \mathbb{F}_p^{m_X - i}$.

Take $X = \varnothing$ to have Corollary A.

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. 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

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

but do not know whether $d_p Ш^2_\varnothing < d_p Ш^2_S$. 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,* $d_p\text{Б}_\varnothing = d_p\mathscr{O}_\text{K}^\times/\mathscr{O}_\text{K}^{\times 2} + d_p Cl_\text{K}[2] = 3$. *Clearly* $G_\varnothing = \{e\}$ *and* $d_p\text{Ш}^2_\varnothing = 0$ *so* $\text{Ш}^2_\varnothing \hookrightarrow \text{Б}_\varnothing$ *has* 3*-dimensional cokernel. Set* $S = \{37_1, 181_1, 293_1\}$ *and* $T = \{307_1, 311_1, 349_1\}$. *One computes* $d_pH^1(G_T, \mathbb{F}_2) = 0$ *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* $H^1(G_S, \mathbb{F}_2) \to H^1(G_{S\cup T}, \mathbb{F}_2)$ *is an isomorphism and* $d_p\text{X}^\vee_{S\cup X,T} \geqslant 3$. *As* $d_p\text{Ш}^2_S \leqslant d_p\text{Б}_S \leqslant d_p\text{Б}_\varnothing = 3$, *we see* $d_p\text{Ш}^2_S = 3$.

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* $d_p\text{Б}_\varnothing = d_p\mathscr{O}_\text{K}^\times/\mathscr{O}_\text{K}^{\times 2} + d_p Cl_\text{K}[2] = 5$. *One computes the class group of the Hilbert class field of* K *is trivial so* $\text{G}_\varnothing = \mathbb{Z}/2 \times \mathbb{Z}/2$ *and has three relations. Thus* $d_p\text{Ш}^2_\varnothing = d_pH^2(G_\varnothing, \mathbb{F}_2) = 3$ *so the map* $\text{Ш}^2_\varnothing \hookrightarrow \text{Б}_\varnothing$ *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* $d_pH^1(G_T, \mathbb{F}_2) = 2$ *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* $H^1(G_S, \mathbb{F}_2) \to H^1(G_{S\cup T}, \mathbb{F}_2)$ *is an isomorphism and* $d_p\text{X}^\vee_{S\cup X,T} \geqslant 5$. *As* $d_p\text{Ш}^2_S \leqslant d_p\text{Б}_S \leqslant d_p\text{Б}_\varnothing = 5$, *we see* $d_p\text{Ш}^2_S = 5$.

Example 3. — *Let* $\text{K} = \mathbb{Q}[x]/(f(x))$ *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,*

$$d_p\text{Б}_\varnothing = d_p\mathscr{O}_\text{K}^\times/\mathscr{O}_\text{K}^{\times 2} + d_p Cl_\text{K}[2] = 6 + 6 = 12 = \#T.$$

One computes $d_pH^1(G_T, \mathbb{F}_2) = 6$ *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* $H^1(G_S, \mathbb{F}_2) \to H^1(G_{S\cup T}, \mathbb{F}_2)$ *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 Angew. Math. **596** (2006), 155–182.

[5] J. Neukirck, A. Schmidt and K. Wingberg, Cohomology of Number Fields, second editiion, 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 5, 2019

Farshid Hajir, Christian Maire, Ravi Ramakrishna, Department of Mathematics, University of Massachussetts, Amherst, MA 01003, USA • FEMTO-ST Institute, Université Bourgogne Franche-Comté, CNRS, 15B avenue des Montboucons, 25000 Besancon, 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