

On the Shafarevich Group of Restricted Ramification Extensions of Number Fields in the Tame Case

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 III_S^2 of maps $H^2(G_S, \mathbb{F}_p) \rightarrow \bigoplus_{v \in S} H^2(G_v, \mathbb{F}_p)$. There is a natural injection $\text{III}_S^2 \hookrightarrow \mathbb{B}_S$ into the dual \mathbb{B}_S of a certain readily computable Kummer group $V_S / (K^\times)^p$, 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 is a finite set of places S coprime to p such that $\text{III}_{S \cup X}^2 \xrightarrow{\cong} \mathbb{B}_{S \cup X} \xrightarrow{\cong} \mathbb{B}_X \hookrightarrow \text{III}_X^2$. In particular, we show that in the tame case, III_Y^2 can *increase* with increasing Y . This is in contrast with the wild case where III_Y^2 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 $G_S = \text{Gal}(K_S/K)$. Given a prime number p , let III_S^2 be the Shafarevich group associated with G_S and p . Specifically, it is the kernel of the localization map of the cohomology group $H^2(G_S, \mathbb{F}_p)$:

$$\text{III}_S^2 := \text{III}^2(G_S, \mathbb{F}_p) = \ker \left(H^2(G_S, \mathbb{F}_p) \rightarrow \bigoplus_{v \in S} H^2(G_v, \mathbb{F}_p) \right),$$

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

$$V_S = \{x \in K^\times \mid (x) = I^p \text{ as a fractional ideal of } K, x \in K_v^p \ \forall v \in S\}$$

and $B_S = (V_S / (K^\times)^p)^\vee$. Clearly, $(K^\times)^p \subset V_S$ and $S \subset T \implies V_T \subset V_S$. It is well known that III_S^2 is closely related to B_S . Specifically, in the wild case, when S contains all the places above p and all Archimedean places, by the Poitou-Tate duality theorem one has $\text{III}_S^2 \simeq B_S$ (see, e.g., [5, Chapter X, Section 7]). It is important to note that algorithms exist to compute B_S via ray class group computations over K , so in the wild case one can, at least in theory, compute $d_p \text{III}_S^2$, the dimension of this space. For the more general tame situation, one only has the following injection (due to Shafarevich and Koch; see, e.g., [3, Chapter 11, Section 2] or [5, Chapter 10, Section 7]):

$$(1) \quad \text{III}_S^2 \hookrightarrow B_S.$$

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

Let us write $K_S(p)/K$ as the maximal pro- p extension of K inside K_S , and set $G_S(p) = \text{Gal}(K_S(p)/K)$. It is an exercise to see that the quotient $G_S \twoheadrightarrow G_S(p)$ induces the injection $\text{III}_{S,p}^2 \hookrightarrow \text{III}_S^2$, where

$$\text{III}_{S,p}^2 := \ker(H^2(G_S(p), \mathbb{F}_p) \rightarrow \bigoplus_{v \in S} H^2(G_v, \mathbb{F}_p)).$$

As $H^2(G_v(p), \mathbb{F}_p) \simeq H^2(G_v, \mathbb{F}_p)$ (see, e.g., Proposition 7.5.8 in [5, Chapter VII, Section 5]), we can take G_v instead of $G_v(p)$.

The Shafarevich group III_S^2 is central to the study of the maximal pro- p quotient $G_S(p)$ of G_S , in particular when S is coprime to p : obviously, one gets

$$\begin{aligned} d_p H^2(G_S(p), \mathbb{F}_p) &\leq \sum_{v \in S} d_p H^2(G_v, \mathbb{F}_p) + d_p \text{III}_S^2 \leq \sum_{v \in S} \delta_{v,p} + d_p \text{III}_S^2 \\ &\leq |S| + d_p V_S / (K^\times)^p, \end{aligned}$$

where $\delta_{v,p} = 1$ or 0 as K_v contains or does not contain the p th roots of unity. This is sufficient to produce criteria involving the infiniteness of $G_S(p)$ (thanks to the Golod-Shafarevich theorem).

Using (1), one can force III_S^2 to be trivial (see the notion of saturated set S in Section 1.2), which can also yield situations where $G_S(p)$ 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

$$(2) \quad \text{III}_{Y \cup X, p}^2 \hookrightarrow \text{III}_{Y \cup X}^2 \hookrightarrow B_{Y \cup X} \leftarrow B_X \leftarrow \text{III}_X^2 \leftarrow \text{III}_{X, p}^2,$$

where the middle surjection follows as $V_{Y \cup X} \subset V_X$. We only consider the case where the finite places X and Y are coprime to \mathfrak{p} . Here, we prove the following result.

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

$$\text{III}_{S \cup X, \mathfrak{p}}^2 \simeq \text{III}_{S \cup X}^2 \simeq \mathbb{B}_{S \cup X} \simeq \mathbb{B}_X.$$

Moreover, such S can be chosen of size $|S| \leq d_{\mathfrak{p}} \mathbb{B}_{\emptyset}$.

The case $\mathfrak{p} = 2$ involves an exceptional situation.

Definition B. The situation is called exceptional if $\mathfrak{p} = 2$ and if one simultaneously has the following:

- (a) $\zeta_4 \notin K$.
- (b) $\mathcal{O}_K^{\times} \cap -4K^4 \neq \emptyset$.
- (c) X contains no real place, and for every prime $\mathfrak{p} \in X$ one has $\zeta_4 \in K_{\mathfrak{p}}$.

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

Theorem C. *Take $\mathfrak{p} = 2$. Let X be a finite set of places of K coprime to 2. Suppose the situation is not exceptional. Then, the conclusion of Theorem A holds. In the exceptional case, one only has*

$$d_2 \mathbb{B}_X - 1 \leq d_2 \text{III}_{S \cup X, 2}^2 = d_2 \text{III}_{S \cup X}^2 = d_2 \mathbb{B}_{S \cup X} \leq d_2 \mathbb{B}_X.$$

Set $m := d_{\mathfrak{p}} \mathbb{B}_{\emptyset}$. From [5, Section 10.7.2], we have the exact sequence

$$0 \rightarrow \mathcal{O}_K^{\times} / (\mathcal{O}_K^{\times})^{\mathfrak{p}} \rightarrow V_{\emptyset} / K^{\times \mathfrak{p}} \rightarrow \text{Cl}_K[\mathfrak{p}] \rightarrow 0,$$

so $m = d_{\mathfrak{p}} \text{Cl}_K + d_{\mathfrak{p}} \mathcal{O}_K^{\times}$.

As mentioned above, the computation of III_S^2 is very difficult in the tame case. Using Theorem A, one may give situations where the value of $|\text{III}_S^2|$ is known without being trivial. As a corollary, we get the following result.

Corollary D. *Suppose that $\mathfrak{p} > 2$. Then, there exist infinitely many finite sets $S_0 \subset S_1 \subset \dots \subset S_m$ of finite places of K all coprime to \mathfrak{p} , such that for $i = 0, \dots, m$, one has $\text{III}_{S_i, \mathfrak{p}}^2 \simeq \text{III}_{S_i}^2 \simeq (\mathbb{Z}/\mathfrak{p})^{m-i}$. For $\mathfrak{p} = 2$, the result holds if either (a) or (b) of Definition B fails.*

Remark E. 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 $X = \emptyset$, (c) of Definition B is not relevant.

Notation

- We fix a prime number p and a number field K .
- Set $K' = K(\zeta_p)$ and $K'' = K(\zeta_{p^2})$, where ζ_{p^2} is some primitive p^2 -th root of unity, and $\zeta_p = \zeta_{p^2}^p$.
- We denote by \mathcal{O}_K the ring of integers of K , by \mathcal{O}_K^\times the group of units of \mathcal{O}_K , and by Cl_K the class group of K .
- We identify a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ with the place v it defines. We write K_v for the completion of K at v and \mathcal{U}_v for the units of the local field K_v ; when v is Archimedean, set $\mathcal{U}_v = K_v^\times$.
- One says that a prime ideal \mathfrak{p} is *tame* if $\#\mathcal{O}_K/\mathfrak{p} \equiv 1 \pmod{p}$, which is equivalent to \mathfrak{p} being coprime to p and $\mu_p \subset K_v$, that is, $\delta_{v,p} = 1$.
- If S is a finite set of places of K , we denote by $K_S(p)/K$ (respectively, $K_S^{\text{ab}}(p)/K$) the maximal pro- p extension (respectively, abelian) of K unramified outside S , and we set $G_S(p) = \text{Gal}(K_S(p)/K)$ (respectively, $G_S^{\text{ab}}(p) = \text{Gal}(K_S^{\text{ab}}(p)/K)$). For $S = \emptyset$, we denote by $H := K_\emptyset^{\text{ab}}(p)$ 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. Let

$$\delta_{2,p} = \begin{cases} 1 & p = 2, \\ 0 & \text{otherwise.} \end{cases}$$

- 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 $S_\infty = \emptyset$.
- Set

$$V_S = \{x \in K^\times \mid (x) = I^p \text{ as a fractional ideal of } K, x \in K_v^p \ \forall v \in S\}.$$

Note $K^{\times p} \subset V_S$ 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 Corollary 2.4.2 in [1, Chapter V, Section 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). Set $K' := K(\zeta_p)$, and consider the governing field $L := K'(\sqrt[p]{V_\emptyset})$. The extension L/K' has Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{r_1+r_2-1+\delta+d}$, where $d = d_p \text{Cl}_K$.

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

$$\sigma_v = \sigma_{\mathfrak{p}} = \left(\frac{L/K'}{\mathfrak{P}} \right)$$

corresponding to the Frobenius elements at \mathfrak{P} in $\text{Gal}(L/K')$.

- 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, by using that $L := K'(\sqrt[p]{V_{\emptyset}})$ and V_{\emptyset} 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 $\text{Gal}(L/K')$. This is all we need when invoking Theorem 1.1 below. By abuse, we will also call the values of σ_v *Frobenius elements*.

Theorem 1.1 (Gras-Munnier). *Let $S = \{v_1, \dots, v_t\}$ 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 $i = 1, \dots, t$, there exists $\alpha_i \in (\mathbb{Z}/p)^\times$, such that*

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

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 because of the fact that for $v \in S_\infty$, one has $\mathcal{U}_v/\mathcal{U}_v^2 = \mathbb{R}^\times/\mathbb{R}^{\times 2} \simeq \mathbb{Z}/2\mathbb{Z}$ (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, Section 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 $N(\mathfrak{p}) \equiv 1 \pmod{p^2}$ when $\mathfrak{p} \in \Sigma$). Set $B = \text{Gal}(K_\Sigma^{\text{ab}}(\mathfrak{p})/H)$.

By class field theory, we get

$$1 \rightarrow (B/B^{p^2})^\vee \xrightarrow{p} \bigoplus_{\mathfrak{p} \in \Sigma} (\mathcal{U}_{\mathfrak{p}}/(\mathcal{U}_{\mathfrak{p}})^{p^2})^\vee \rightarrow (\iota(\mathcal{O}_K^\times))^\vee \rightarrow 1,$$

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

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 $\psi_{\mathfrak{p}} \in (\mathcal{U}_{\mathfrak{p}}/(\mathcal{U}_{\mathfrak{p}})^{p^2})^\vee$ for all $\mathfrak{p} \in \Sigma$, there exists a character ψ of B/B^{p^2} such that $\psi|_{\mathcal{U}_{\mathfrak{p}}} = \psi_{\mathfrak{p}}$ if and only if

$$(1.1) \quad \forall \varepsilon \in \mathcal{O}_K^\times, \quad \prod_{\mathfrak{p} \in \Sigma} \psi_{\mathfrak{p}}(\iota_{\mathfrak{p}}(\varepsilon)) = 1,$$

where $\iota_{\mathfrak{p}} : \mathcal{O}_K^\times \rightarrow \mathcal{U}_{\mathfrak{p}}/(\mathcal{U}_{\mathfrak{p}})^{p^2}$. 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 now rephrase (1.1) with the governing field $L = K'' \left(\sqrt[p^2]{\mathcal{O}_K^\times} \right)$ (see [1, Chapter V, Section 2, d]), where $K'' = K(\zeta_{p^2})$. For the clarity of the exposition, let us develop this correspondence.

For $\mathfrak{p} \in \Sigma_q$, denote $E_{\mathfrak{p}} = \{\varepsilon \in \mathcal{O}_K^\times, \varepsilon \in (\mathcal{U}_{\mathfrak{p}}^\times)^{p^2}\}$. We then have

$$1 \rightarrow E_{\mathfrak{p}}/(\mathcal{O}_K^\times)^{p^2} \rightarrow \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^{p^2} \rightarrow \iota_{\mathfrak{p}}(\mathcal{O}_K^\times) \rightarrow 1.$$

Lemma 1.3. *For $p = 2$ assume that $\zeta_4 \in K$. Let $\varepsilon \in \mathcal{O}_K^\times \cap (K'')^{p^2}$. Then, $\mathcal{O}_K^* \cap (K'')^{p^2} = (\mathcal{O}_K^*)^{p^2}$.*

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

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

$$\mathcal{O}_K^\times (K''^\times)^{p^2} / (K''^\times)^{p^2} \simeq \mathcal{O}_K^\times / (\mathcal{O}_K^\times \cap (K''^\times)^{p^2}) \simeq \mathcal{O}_K^\times / (\mathcal{O}_K^\times)^{p^2}.$$

Modding out by $E_{\mathfrak{p}}$, and noting $E_{\mathfrak{p}} \supseteq (\mathcal{O}_K^\times)^{p^2}$, we see

$$(1.2) \quad \mathcal{O}_K^\times (K''^\times)^{p^2} / E_{\mathfrak{p}} (K''^\times)^{p^2} \simeq \mathcal{O}_K^\times / E_{\mathfrak{p}}$$

so by Kummer duality,

$$(1.3) \quad \iota_{\mathfrak{p}}(\mathcal{O}_K^\times)^\vee \simeq (\mathcal{O}_K^\times / E_{\mathfrak{p}})^\vee \simeq \text{Gal}(L/K'' \left(\sqrt[p^2]{E_{\mathfrak{p}}} \right)).$$

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

Proof. If $\varepsilon \notin (\mathcal{O}_K^{\times})^4$, one knows that $\varepsilon = (1 + \zeta_4)^4 \gamma^4$ with $\gamma \in K$ (see Theorem 6.3.2 in [1, Chapter II]) which implies $\varepsilon \in (K_{\mathfrak{p}})^4$ when $\zeta_4 \in K_{\mathfrak{p}}$. \square

Hence, Lemma 1.4 shows that (1.2) and (1.3) also hold when $\zeta_4 \in K_{\mathfrak{p}}$.

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 $\text{Gal}(L/K'')$. As before, $\sigma_{\mathfrak{p}}$ depends on $\mathfrak{P}|\mathfrak{p}$ only up to a power coprime to p .

The Galois group $\text{Gal}(L/K''(\sqrt[p^2]{E_{\mathfrak{p}}}))$ is generated by $\sigma_{\mathfrak{p}}$, by Lemmas 1.3 and 1.4 (applied to $K_{\mathfrak{p}}$). Observe that the dual of the inertia group at \mathfrak{p} in B/B^{p^2} is isomorphic to

$$\ker((\mathcal{U}_{\mathfrak{p}}/(\mathcal{U}_{\mathfrak{p}})^{p^2})^{\vee} \rightarrow (\iota_{\mathfrak{p}}(\mathcal{O}_K^{\times}))^{\vee}),$$

where $(\iota_{\mathfrak{p}}(\mathcal{O}_K^{\times}))^{\vee} \simeq \text{Gal}(L/K''(\sqrt[p^2]{E_{\mathfrak{p}}})) = \langle \sigma_{\mathfrak{p}} \rangle$. Then, there is a generator $\chi_{\mathfrak{p}}$ of $(\mathcal{U}_{\mathfrak{p}}/(\mathcal{U}_{\mathfrak{p}})^{p^2})^{\vee}$ 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 (1.1) implies

$$(1.4) \quad \prod_{\mathfrak{p} \in \Sigma} \sigma_{\mathfrak{p}}^{a_{\mathfrak{p}}} = 1.$$

We show this is an equivalence. For the reverse, suppose (1.4) holds. Then, it implies the relation $\prod_{\mathfrak{p} \in \Sigma} \theta_{\mathfrak{p}} = 1$ in $(\mathcal{O}_K^{\times}(K'')^{p^2}/(K'')^{p^2})^{\vee}$, where $\theta_{\mathfrak{p}}$ is a character of $\mathcal{O}_K^{\times}(K'')^{p^2}/(K'')^{p^2}$ associated with $\sigma_{\mathfrak{p}}^{a_{\mathfrak{p}}}$, and trivial on $E_{\mathfrak{p}}(K'')^{p^2}/(K'')^{p^2}$; then, $\theta_{\mathfrak{p}}$ can be taken in

$$(\mathcal{O}_K^{\times}(K'')^{p^2}/E_{\mathfrak{p}}(K'')^{p^2})^{\vee} \simeq (\mathcal{O}_K^{\times}/E_{\mathfrak{p}})^{\vee} \simeq (\iota_{\mathfrak{p}}(\mathcal{O}_K^{\times}))^{\vee}.$$

Now, as $\chi_{\mathfrak{p}}$ is sent to $\sigma_{\mathfrak{p}}$, one deduces that $\theta_{\mathfrak{p}} = \chi_{\mathfrak{p}}^{a_{\mathfrak{p}}}$. To conclude, we now set $\psi_{\mathfrak{p}} := \chi_{\mathfrak{p}}^{a_{\mathfrak{p}}} \circ \iota_{\mathfrak{p}} \in (\mathcal{O}_K^{\times}/(\mathcal{O}_K^{\times})^p)^{\vee}$, then $\prod_{\mathfrak{p} \in \Sigma} \psi_{\mathfrak{p}}(\varepsilon) = 1$ for every $\varepsilon \in \mathcal{O}_K^{\times}$, and then recover relation (1.1).

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 $N(\mathfrak{p}) \equiv 1 \pmod{p^2}$. We are interested in the existence of a degree- p^2 cyclic extension $K_{\mathfrak{q}}/H$, abelian over K and unramified outside $\Sigma := S \cup \{\mathfrak{q}\}$, such that $K_{\mathfrak{q}}/H$ 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 result.

Proposition 1.5. Let $p > 2$. There exists a degree- p^2 cyclic extension $K_{\mathfrak{q}}/H$, 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 exist $a_q \in (\mathbb{Z}/p)^\times$, and $b_p \in \mathbb{Z}/p^2\mathbb{Z}$, $p \in S$, such that

$$(1.5) \quad \hat{\sigma}_q^{a_q} \prod_{p \in S} \sigma_p^{b_p} = 1 \in \text{Gal}(L/K''),$$

where

$$\hat{\sigma}_q = \begin{cases} \sigma_q & \text{if } N(q) \not\equiv 1 \pmod{p^2}, \\ \sigma_q^p & \text{if } N(q) \equiv 1 \pmod{p^2}, \end{cases}$$

with at least one $b_p \in (\mathbb{Z}/p^2\mathbb{Z})^\times$. When $p = 2$ the result holds, if we assume that $\zeta_4 \in K_q$.

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 $\mathcal{O}_K^\times \cap -4K^4 = \emptyset$. Let $\varepsilon \in \mathcal{O}_K^\times \cap (K'')^{p^2}$. Then, $\varepsilon \in (\mathcal{O}_K^\times)^{p^2}$.

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

Assume now $\mathcal{O}_K^\times \cap -4K^4 = \emptyset$. By Lemma 1.7 the Kummer radical of L/K'' is isomorphic to $\mathcal{O}_K^\times / (\mathcal{O}_K^\times)^2$, and the isomorphism (1.2) still holds. Then, we can follow the discussion before Proposition 1.5 by observing that the main difference is that one only has $E_p \subset \mathcal{O}_K^\times \cap (K_p(\zeta_4))^4$, meaning that $\text{Gal}(L(\sqrt[4]{\mathcal{O}_K^\times})/K''(\sqrt[4]{E_p}))$ contains the decomposition group of \mathfrak{p} , but *may be larger*. Let σ'_p be a generator of $\text{Gal}(L/K''(\sqrt[4]{E_p}))$.

Proposition 1.8. Suppose $\mathcal{O}_K^\times \cap -4K^4 = \emptyset$. Take q such that $\zeta_4 \notin K_q$.

There exists a degree-4 cyclic extension K_q/H , abelian over K , and unramified outside $S \cup \{q\}$, for which the inertia degree at q is exactly 2, if and only if there exists $a_q \in (\mathbb{Z}/2)^\times$, and $b_p \in \mathbb{Z}/4\mathbb{Z}$, $p \in S$, such that

$$(\sigma'_q)^{a_q} \prod_{p \in S} \sigma_p^{b_p} = 1 \in \text{Gal}(L/K''),$$

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

Example 1.9. Take $K = \mathbb{Q}$, $p = 2$ and $\mathfrak{p} = (3)$. Then, the governing extension is $\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4)$, in which \mathfrak{p} splits. But here, $E_p = \{1\}$, and

$$\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4, \sqrt[4]{E_p})) = \langle \sigma'_p \rangle \simeq \mathbb{Z}/2,$$

showing the difference between σ'_p and the Frobenius σ_p . Take now the prime 5 which is inert in the governing extension. Proposition 1.8 applies: there exists 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 $V_S / (K^\times)^p = \{1\}$.

Recall the following equality due to Shafarevich (see, e.g., Corollary 10.7.7 in [5, Chapter X, Section 7]):

$$(1.6) \quad d_p G_S = |S_0| + |S_\infty| \delta_{2,p} - (r_1 + r_2) + 1 - \delta + d_p V_S / (K^\times)^p,$$

showing that $d_p G_S$ 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, the following hold:*

- If $S \subset T$, then T is saturated.
- For every tame prime $\mathfrak{p} \notin S$, one has $d_p G_{S \cup \{\mathfrak{p}\}} = d_p G_S + 1$.

Proof. The first point is due to the fact that $V_T \subset V_S$, and the second point is a consequence of (1.6) 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 $\text{Gal}(K'(\sqrt[p]{V_\emptyset})/K')$.*

Proof.

- Suppose the Frobenii generate the full Galois group. By hypothesis, for each degree- p extension L/K' in $K'(\sqrt[p]{V_\emptyset})/K'$, 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 $x \in V_S$: then, every $v \in S$ splits completely in $K'(\sqrt[p]{x})/K'$. As $K'(\sqrt[p]{x}) \subset K'(\sqrt[p]{V_\emptyset})$, one deduces that $K'(\sqrt[p]{x}) = K'$, and then $x \in (K')^p$. As $[K' : K]$ is coprime to p , one finally obtains that $x \in (K^\times)^p$, so $B_S = \{0\}$.
- If S is saturated, then for every finite set T of tame places of K with $T \cap S = \emptyset$, one has $d_p G_{S \cup T} = d_p G_S + |T|$ by Proposition 1.11. Then, by the Gras-Munnier criterion, one has $\langle \sigma_v, v \in S \rangle = \text{Gal}(L/K')$. □

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 $\text{Gal}(L/K')$, 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, $\text{Gal}(L/K') = \langle \sigma_v, v \in S \rangle$. By Theorem 1.12, S is saturated. □

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

$$(1.7) \quad 1 \rightarrow H_{S,T} \rightarrow G_{S \cup T}(\mathfrak{p}) \rightarrow G_S(\mathfrak{p}) \rightarrow 1.$$

Definition 1.14. Set

$$X_{S,T} := H_{S,T} / [H_{S,T}, H_{S,T}] H_{S,T}^{\mathfrak{p}}$$

and

$$X_{S,T} := (X_{S,T})_{G_S(\mathfrak{p})} = H_{S,T} / [H_{S,T}, G_S(\mathfrak{p})] H_{S,T}^{\mathfrak{p}}.$$

Recall that as $G_S(\mathfrak{p})$ is a pro- \mathfrak{p} group, so $\mathbb{F}_p[[G_S(\mathfrak{p})]]$ is a local ring.

Lemma 1.15. *The abelian group $X_{S,T}$ is a compact $\mathbb{F}_p[[G_S(\mathfrak{p})]]$ -module (with continuous action) that can be topologically generated by $d_p X_{S,T}$ generators. Moreover, $d_p X_{S,T} \leq |T|$.*

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

$$\bigoplus_{i=1}^t \mathbb{F}_p[[G_S(\mathfrak{p})]] \rightarrow \langle I_w, w|v \in T \rangle = X_{S,T},$$

where $t = |T|$. Taking the $G_S(\mathfrak{p})$ -coinvariants, we obtain $\mathbb{F}_p^t \rightarrow X_{S,T}$. □

Applying the Hochschild-Serre spectral sequence to (1.7), one gets the following result.

Lemma 1.16. *Let S, T be two finite sets of places of K coprime to \mathfrak{p} . Then, one has*

$$\begin{aligned} 0 &\rightarrow H^1(G_S(\mathfrak{p}), \mathbb{F}_p) \rightarrow H^1(G_{S \cup T}(\mathfrak{p}), \mathbb{F}_p) \\ &\rightarrow X_{S,T}^{\vee} \rightarrow \text{III}_{S,p}^2 \rightarrow \text{III}_{S \cup T,p}^2. \end{aligned}$$

Furthermore, the cokernel of the natural injection $\text{III}_{X,p}^2 \hookrightarrow \mathbb{B}_X$ is nonincreasing in dimension as X increases.

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

$$\begin{array}{ccccccc} H^1(G_S(\mathfrak{p}), \mathbb{F}_p) & \hookrightarrow & H^1(G_{S \cup T}(\mathfrak{p}), \mathbb{F}_p) & \rightarrow & X_{S,T}^{\vee} & \rightarrow & H^2(G_S(\mathfrak{p}), \mathbb{F}_p) & \longrightarrow & H^2(G_{S \cup T}(\mathfrak{p}), \mathbb{F}_p) \\ & & & & & & \downarrow & & \downarrow \\ & & & & & & \oplus_{v \in S} H^2(G_v, \mathbb{F}_p) & \hookrightarrow & \oplus_{v \in S \cup T} H^2(G_v, \mathbb{F}_p) \end{array}$$

Chasing the transgression map $X_{S,T}^\vee \xrightarrow{\text{tg}} H^2(G_S(\mathfrak{p}))$ to the right gives that its image lies in $\text{III}_{S,p}^2$ whose image to the right lies in $\text{III}_{S \cup T,p}^2$. We now have the diagram

$$\begin{array}{ccccccc}
 0 & \longrightarrow & H^1(G_S(\mathfrak{p}), \mathbb{F}_p) & \longrightarrow & H^1(G_{S \cup T}(\mathfrak{p}), \mathbb{F}_p) & \longrightarrow & X_{S,T}^\vee \longrightarrow \text{III}_{S,p}^2 \longrightarrow \text{III}_{S \cup T,p}^2 \\
 & & & & & & \downarrow & & \downarrow \\
 & & & & & & \mathbb{B}_S & \longrightarrow & \mathbb{B}_{S \cup T}
 \end{array}$$

where the bottom horizontal map is surjective, as the inclusion

$$V_{S \cup T} / (\mathbb{K}^\times)^p \hookrightarrow V_S / (\mathbb{K}^\times)^p$$

is immediate from the definition of V_X . The second result follows. □

Corollary 1.17. *If the natural injection $\text{III}_{X,p}^2 \hookrightarrow \mathbb{B}_X$ is an isomorphism, then for any set Y we have $\text{III}_{X \cup Y,p}^2 \xrightarrow{\cong} \mathbb{B}_{X \cup Y}$.*

Let us give an obvious consequence of Lemma 1.16.

Lemma 1.18. *Suppose that $H^1(G_S(\mathfrak{p}), \mathbb{F}_p) \simeq H^1(G_{S \cup T}(\mathfrak{p}), \mathbb{F}_p)$; then,*

$$X_{S,T}^\vee \hookrightarrow \text{III}_{S,p}^2.$$

If, moreover, $S \cup T$ is saturated, then $X_{S,T}^\vee \simeq \text{III}_{S,p}^2$.

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

Remark 1.19. An important consequence of Lemmas 1.16 and 1.18 is that elements of $X_{S,T}^\vee$ can give rise to elements of $\text{III}_{S,p}^2$. The former can be found via ray class group computations. We thus have a method of producing independent elements of $\text{III}_{S,p}^2$. If we find $d_p \mathbb{B}_S$ such elements, we have established $\text{III}_{S,p}^2 \xrightarrow{\cong} \text{III}_S^2 \xrightarrow{\cong} \mathbb{B}_S$, and thus computed $d_p \text{III}_S^2$.

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 the following hold:*

- (i) $T \cup X$ is saturated and $d_p G_{T \cup X} = d_p G_X$.
- (ii) $d_p G_{S \cup T \cup X} = d_p G_{S \cup X}$.

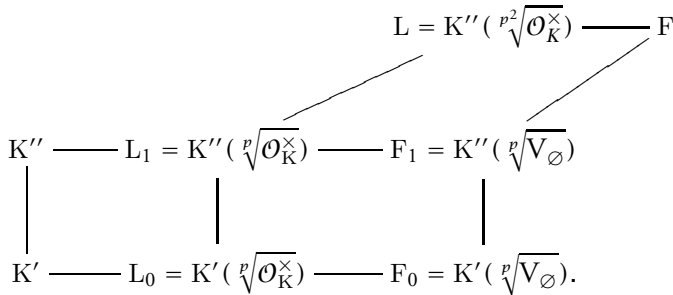
- (iii) $|T| \leq d_p \text{Cl}_K + r_1 + r_2 - 1 + \delta$ and $|S| \leq r_1 + r_2 - 1 + \delta$.
- (iv) For each prime $q \in T$, with at most one exception if we are in the situation of Definition B, there exists a degree- p^2 cyclic extension M of K^H , abelian over K , and unramified outside $S \cup X \cup \{q\}$ where the inertia group at q is of order p .

Let $F_0 = K'(\sqrt[p]{V_\emptyset})$, $L_0 = K'(\sqrt[p]{\mathcal{O}_K^\times})$, $K'' = K(\zeta_{p^2})$, $L_1 = K''(\sqrt[p^2]{\mathcal{O}_K^\times})$, $F_1 = K''(\sqrt[p]{V_\emptyset})$, and $F = LF_0 = K''(\sqrt[p^2]{\mathcal{O}_K^\times}, \sqrt[p]{V_\emptyset})$. Let $G = \text{Gal}(F/K')$.

Proof of Proposition 2.1. Given a tame prime p of \mathcal{O}_K , we choose a prime $\mathfrak{P}|p$ of F , and we consider its Frobenius $\sigma_{\mathfrak{P}} := \sigma_{\mathfrak{P}}$ in the Galois group $\text{Gal}(F/K')$ 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 $\text{Gal}(F/K')$, and that is all we need. In part a), $\text{Gal}(F/K')$ 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.

Let $E_X = \langle \sigma_{\mathfrak{p}|F_0}, \mathfrak{p} \in X \rangle \subset \text{Gal}(F_0/K')$ the subgroup of $\text{Gal}(F_0/K')$ generated by the Frobenii of the primes $\mathfrak{p} \in X$. Let $m_X = d_p V_\emptyset - d_p E_X$.

a) Assume first that $F_0 \cap K'' = K'$. When $p = 2$, one has $K = K' = K''$, and then $\zeta_4 \in K$. We have



We choose S and T as follows:

- Let T be any set of primes q whose Frobenii σ_q in G are such that the restriction in $\text{Gal}(F_0/K')$ forms an \mathbb{F}_p -basis of a subspace in direct sum with E_X ; in other words,

$$\text{Gal}(F_0/K') = \langle \sigma_{q|F_0}, q \in T \rangle \oplus E_X,$$

and $\langle \sigma_{q|F_0}, q \in T \rangle = \bigoplus_{q \in T} \langle \sigma_{q|F_0} \rangle$.

- Let \tilde{X} be those places of X whose Frobenii lie in $\text{Gal}(F/F_1)$, and let S be any set of primes p whose Frobenii σ_p in G form in direct sum with the Frobenii in \tilde{X} a basis of $\text{Gal}(F/F_1)$.

As $\text{Gal}(F_1/K')$ has exponent p , we see for each $q \in T$ that $\sigma_q^p \in \text{Gal}(F/F_1)$.

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 $d_p G_{T \cup X} = d_p G_X$, and (i) holds.

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

The condition on S gives relation (1.5) in $\text{Gal}(F/F_1) \subset \text{Gal}(F/L_1)$ for the set $S \cup \bar{X} \cup \{q\}$, $q \in T$. After taking the quotient of this relation by $\text{Gal}(F/L)$, we obtain by Proposition 1.5 that, for each prime $q \in T$, there exists a degree- p^2 cyclic extension K_q/H , abelian over K and unramified outside $S \cup X \cup \{q\}$, for which the inertia at q is of order p , proving (iv).

(iii) is obvious.

b) Assume now that $K'' \subset F_0$. Let \mathfrak{a}_i , $i = 1, \dots, d$ be ideals of \mathcal{O}_K , whose classes are a system of minimal generators of $\text{Cl}_K[p]$, and let $a_i \in \mathcal{O}_K^\times$ such that $(a_i) = \mathfrak{a}_i^p$. Let $A = \langle a_1, \dots, a_d \rangle K^{\times p} / (K^\times)^p \subset V_\emptyset / (K^\times)^p$. Note $K'(\sqrt[p]{V_\emptyset}) = K'(\sqrt[p]{A}, \sqrt[p]{\mathcal{O}_K^\times})$.

As F_0/K' and K''/K' are abelian p -extensions, the containment $K'' \subset F_0$ implies $K' = K$. We have

$$\begin{array}{ccc}
 L = K''(\sqrt[p^2]{\mathcal{O}_K^\times}) & \text{-----} & F \\
 \downarrow & & \downarrow \\
 L_0 = K''(\sqrt[p]{\mathcal{O}_K^\times}) & \text{-----} & F_0 = F_1 = K''(\sqrt[p]{V_\emptyset}) \\
 \downarrow & & \downarrow \\
 K'' & \text{-----} & K''(\sqrt[p]{A}) \\
 \downarrow & & \downarrow \\
 K' & \text{-----} & K'(\sqrt[p]{A})
 \end{array}$$

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

Now, take $p = 2$. One has $K'' = K''(\sqrt[4]{\mathcal{O}_K^\times}) \cap K''(\sqrt{A})$. Indeed, by Kummer theory the intersection is characterized by elements $\varepsilon \in \mathcal{O}_K^\times$ and $x \in A$ such that $x\varepsilon = \alpha^2$ with $\alpha \in K''$. If $\alpha \notin K'$, since $[K'' : K'] = 2$, we get $K'' = K'(\alpha) = K'(\sqrt{x\varepsilon})$. By uniqueness of the Kummer radical, one has $x\varepsilon = -\gamma^2$ with $\gamma \in K'$, and then $(x) = (\gamma)^2$ which implies $x \in A$ trivial; in other words, $\varepsilon \in (K'')^2$, 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 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 $\zeta_4 \in K_{\mathfrak{p}}$, as in case a), we can apply Proposition 1.5.

Suppose now there is one prime $\mathfrak{p} \in T$ such that $\zeta_4 \notin K_{\mathfrak{p}}$, and assume that $\mathcal{O}_K^{\times} \cap -4K^4 = \emptyset$. Because of the remark regarding the linear disjunction, every element $g \in \text{Gal}(L/L_0)$ can be lifted in $\text{Gal}(F/F_0)$. 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 Proposition 2.1 (iv) applies for every $\mathfrak{q} \in T$. \square

Remark 2.2. Observe one can take T such that $|T| \leq m_X = d_p V_{\emptyset} - d_p E_X$.

2.2. Proof of Theorem A and Theorem C. Suppose $p > 2$ or, when $p = 2$, one of the conditions (a), (b), or (c) of the exceptional situation fails. Let S and T as in Proposition 2.1. As $X \cup T$ is saturated, by Proposition 2.1 (i) and (1.6), one obtains $|T| = d_p B_X$. Moreover, $S \cup X \cup T$ is also saturated and, in particular, $B_{S \cup X \cup T} \simeq \coprod_{S \cup X \cup T, p}^2 = \{0\}$. With Proposition 2.1 (ii), we see that $d_p B_{S \cup X} = |T|$, so (i) and (ii) imply $B_{S \cup X} \simeq B_X$.

Now, let us take the spectral sequence of the short exact sequence

$$1 \rightarrow H_{S \cup X, T} \rightarrow G_{S \cup X \cup T}(p) \rightarrow G_{S \cup X}(p) \rightarrow 1,$$

to obtain by Lemma 1.16

$$\begin{aligned} 1 &\rightarrow H^1(G_{S \cup X}(p), \mathbb{F}_p) \rightarrow H^1(G_{S \cup X \cup T}(p), \mathbb{F}_p) \rightarrow X_{S \cup X, T}^{\vee} \\ &\rightarrow \coprod_{S \cup X, p}^2 \rightarrow \coprod_{S \cup X \cup T, p}^2 = \{0\}. \end{aligned}$$

Hence, $X_{S \cup X, T}^{\vee} \simeq \coprod_{S \cup X, p}^2$. Now, (iv) of Proposition 2.1 implies that $d_p X_{S \cup X, T} \geq |T|$, and since obviously $d_p X_{S \cup X, T} \leq |T|$, we finally get $d_p \coprod_{S \cup X, p}^2 = |T|$.

Hence, $d_p \coprod_{S \cup X, p}^2 = |T| = d_p B_{S \cup X} = d_p B_X$. Thanks to (2), one has

$$\coprod_{S \cup X, p}^2 \simeq \coprod_{S \cup X}^2 \simeq B_{S \cup X} \simeq B_X.$$

This completes the proof of Theorem A.

Suppose now $p = 2$, and we are in the exceptional situation of Definition B. 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), so by the previous result, we get the existence of a set S' such that

$$\coprod_{S' \cup X', 2}^2 \simeq \coprod_{S' \cup X'}^2 \simeq B_{S' \cup X'} \simeq B_{X'}.$$

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

$$\text{III}_{S \cup X, 2}^2 \simeq \text{III}_{S \cup X}^2 \simeq \mathbb{B}_{S \cup X} \simeq \mathbb{B}_{X'}.$$

To conclude, let us observe that $d_2 \mathbb{B}_X - 1 \leq d_2 \mathbb{B}_{X'} \leq d_2 \mathbb{B}_X$.

2.3. Proof of Corollary D. When (a) or (b) of the exceptional case fails, take $X = \emptyset$; otherwise take $X = \{p\}$ where p is a prime such that $\zeta_4 \notin K_p$. We then avoid the exceptional situation.

Let us choose S and T as in the proof of Proposition 2.1. Let us write $T = \{p_1, \dots, p_{m_X}\}$, where $m_X = d_p \mathbb{B}_\emptyset - d_p E_X$. Let $S_0 = S \cup X$ and, for $i \geq 0$, $S_i = S \cup X \cup \{p_1, p_2, \dots, p_i\}$. Here, as $d_p G_{S_i} = d_p G_{S_{m_X}}$, the spectral sequence shows that

$$(2.1) \quad \mathbb{Z}/p \hookrightarrow \text{III}_{S_i, p}^2 \rightarrow \text{III}_{S_{i+1}, p}^2,$$

in particular, $d_p \text{III}_{S_i, p}^2 \leq d_p \text{III}_{S_{i+1}, p}^2 + 1$. After noting that $d_p \text{III}_{S_{m_X}, p}^2 = 0$ (the set $X \cup T$ is saturated) and that $d_p \text{III}_{S_0, p}^2 = |T| = m_X$, then we conclude that $d_p \text{III}_{S_i, p}^2 = m_X - i$. Observe also that (2.1) induces

$$\mathbb{Z}/p \hookrightarrow \text{III}_{S_i}^2 \rightarrow \text{III}_{S_{i+1}}^2,$$

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

We have thus proved the following result.

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

Take $X = \emptyset$ to have Corollary D. To be complete, observe that when $X = \{p\}$, 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

$$\text{III}_\emptyset^2 \hookrightarrow \mathbb{B}_\emptyset \rightarrow \mathbb{B}_S \hookrightarrow \text{III}_S^2,$$

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 III_X^2 increases as X does, in contrast to the wild case.

In the third example we establish

$$\text{III}_\emptyset^2 \hookrightarrow \mathbb{B}_\emptyset \xrightarrow{\cong} \mathbb{B}_S \xleftarrow{\cong} \text{III}_S^2,$$

but do not know whether $d_p \text{III}_\emptyset^2 < d_p \text{III}_S^2$. Indeed, we suspect equality in that case.

In the examples below, p_i refers to the i th 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 3.1. 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, $d_p \mathbb{B}_\emptyset = d_p \mathcal{O}_K^\times / \mathcal{O}_K^{\times 2} + d_p \text{Cl}_K[2] = 3$. Clearly, $G_\emptyset = \{e\}$ and $d_p \text{III}_\emptyset^2 = 0$, so $\text{III}_\emptyset^2 \hookrightarrow \mathbb{B}_\emptyset$ has three-dimensional cokernel. Set $S = \{37_1, 181_1, 293_1\}$ and $T = \{307_1, 311_1, 349_1\}$. One computes $d_p H^1(G_T, \mathbb{F}_2) = 0$, 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 map $H^1(G_S, \mathbb{F}_2) \rightarrow H^1(G_{S \cup T}, \mathbb{F}_2)$ is an isomorphism and $d_p X_{S \cup T}^\vee \geq 3$. As $d_p \text{III}_S^2 \leq d_p \mathbb{B}_S \leq d_p \mathbb{B}_\emptyset = 3$, we see that $d_p \text{III}_S^2 = 3$.

Example 3.2. 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 $d_p \mathbb{B}_\emptyset = d_p \mathcal{O}_K^\times / \mathcal{O}_K^{\times 2} + d_p \text{Cl}_K[2] = 5$. One computes the class group of the Hilbert class field of K is trivial, so $G_\emptyset = \mathbb{Z}/2 \times \mathbb{Z}/2$ and has three relations. Thus, $d_p \text{III}_\emptyset^2 = d_p H^2(G_\emptyset, \mathbb{F}_2) = 3$, so the map $\text{III}_\emptyset^2 \hookrightarrow \mathbb{B}_\emptyset$ has two-dimensional cokernel. Set $S = \{701_1, 2857_1, 3169_1\}$ and $T = \{367_1, 397_1, 401_1, 409_1, 449_1\}$. One computes $d_p H^1(G_T, \mathbb{F}_2) = 2$, 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 map $H^1(G_S, \mathbb{F}_2) \rightarrow H^1(G_{S \cup T}, \mathbb{F}_2)$ is an isomorphism and $d_p X_{S \cup T}^\vee \geq 5$. As $d_p \text{III}_S^2 \leq d_p \mathbb{B}_S \leq d_p \mathbb{B}_\emptyset = 5$, we see $d_p \text{III}_S^2 = 5$.

Example 3.3. Let $K = \mathbb{Q}[x]/(f(x))$ where we have $f(x) = x^{12} + 339x^{10} - 19752x^8 - 2188735x^6 + 284236829x^4 + 4401349506x^2 + 15622982921$. This polynomial is irreducible, and K is totally complex with small root discriminant and 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,

$$d_p \mathbb{B}_\emptyset = d_p \mathcal{O}_K^\times / \mathcal{O}_K^{\times 2} + d_p \text{Cl}_K[2] = 6 + 6 = 12 = \#T.$$

One computes $d_p H^1(G_T, \mathbb{F}_2) = 6$, 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 $H^1(G_S, \mathbb{F}_2) \rightarrow H^1(G_{S \cup T}, \mathbb{F}_2)$ is an isomorphism. From this data, one can only conclude $d_p X_{S \cup T}^\vee \geq 11$. On

the other hand, for every $v \in T$ one computes that 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 $X_{S \cup X, T}^\vee$, so $d_p \text{III}_S^2 \geq 12$. As $d_p \mathbb{B}_S \leq d_p \mathbb{B}_\emptyset = 12$, we have $d_p \text{III}_S^2 = 12$. We suspect that in this case $d_p \text{III}_\emptyset^2 = 12$.

Acknowledgements. The authors thank Georges Gras for helpful discussions, and the anonymous referee for the comments on the manuscript.

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 was finished during a visit at Harbin Institute of Technology. Thanks are also due to the Department of Mathematics at Cornell University and the Institute for Advanced Study in Mathematics of HIT for providing conducive research atmosphere. Finally, partial support is acknowledged from the Agence Nationale de la Recherche project FLAIR (ANR-17-CE40-0012) and by the EIPHI Graduate School (ANR-17-EURE-0002).

The third author received support from the Simons Collaboration (grant no. 524863). All three authors were also supported by Mathematisches Forschungsinstitut Oberwolfach for a Research in Pairs visit in January 2019.

REFERENCES

- [1] G. GRAS, *Class Field Theory: From Theory to Practice*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003, Translated from the French manuscript by Henri Cohen. <http://dx.doi.org/10.1007/978-3-662-11323-3>. MR1941965
- [2] G. GRAS and A. MUNNIER, *Extensions cycliques T-totalement ramifiées*, Théorie des nombres, Années 1996/97–1997/98, Publ. Math. UFR Sci. Tech. Besançon, Univ. Franche-Comté, Besançon, 1999, pp. 16 (French). MR1735371
- [3] H. KOCH, *Galoissche Theorie der p-Erweiterungen*, with Geleitwort [Foreword] by I. R. ŠAFAREVIČ, Springer-Verlag, Berlin-New York; VEB Deutscher Verlag der Wissenschaften, Berlin, 1970 (German). MR0291139
- [4] J. LABUTE, *Mild pro-p-groups and Galois groups of p-extensions of \mathbb{Q}* , J. Reine Angew. Math. **596** (2006), 155–182. <http://dx.doi.org/10.1515/CRELLE.2006.058>. MR2254811
- [5] J. NEUKIRCH, A. SCHMIDT, and K. WINGBERG, *Cohomology of Number Fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. <http://dx.doi.org/10.1007/978-3-540-37889-1>. MR2392026
- [6] A. SCHMIDT, *Über Pro-p-Fundamentalgruppen markierter arithmetischer Kurven*, J. Reine Angew. Math. **640** (2010), 203–235 (German, with English summary). <http://dx.doi.org/10.1515/CRELLE.2010.025>. MR2629694

FARSHID HAJIR:
 Department of Mathematics and Statistics
 University of Massachusetts
 710 N Pleasant St
 Amherst, MA 01003
 USA
 E-MAIL: hajir@math.umass.edu

2710 FARSHID HAJIR, CHRISTIAN MAIRE & RAVI RAMAKRISHNA

CHRISTIAN MAIRE:
FEMTO-ST Institute
Université Bourgogne Franche-Comté, CNRS
15B avenue des Montboucons
25000 Besançon
France
E-MAIL: christian.maire@univ-fcomte.fr

RAVI RAMAKRISHNA:
Department of Mathematics
Cornell University
310 Malott Hall
Ithaca, NY 14853-4201
USA
E-MAIL: ravi@math.cornell.edu

Received: September 14, 2019.