On the Quotients of the Maximal Unramified 2-Extension of a Number Field

Christian Maire

Received: June 14, 2018
Revised: July 26, 2018

Communicated by Otmar Venjakob

Abstract. Let K be a totally imaginary number field. Denote by $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ the Galois group of the maximal unramified pro-2 extension of K. By using cup-products in étale cohomology of $\mathrm{Spec}\mathcal{O}_{\mathrm{K}}$ we study situations where $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ has no quotient of cohomological dimension 2. For example, in the family of imaginary quadratic fields K, the group $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ almost never has a quotient of cohomological dimension 2 and of maximal 2-rank. We also give a relation between this question and that of the 4-rank of the class group of K, showing in particular that when ordered by absolute value of the discriminant, more than 99% of imaginary quadratic fields satisfy an alternative (but equivalent) form of the unramified Fontaine-Mazur conjecture (at $p = 2$).

2010 Mathematics Subject Classification: 11R37, 11R29.
Keywords and Phrases: Unramified extensions, cohomological dimension, uniform pro-2 groups.

1 Introduction

Let K be a number field. Given a prime number p, denote by $\mathrm{K}^{ur}(p)$ the maximal unramified pro-p extension of K; put $\mathrm{G}_{\mathrm{K}}^{ur}(p) := \mathrm{Gal}(\mathrm{K}^{ur}(p)/\mathrm{K})$. Here we are interested in the quotients of $\mathrm{G}_{\mathrm{K}}^{ur}(p)$, more precisely in their cohomological dimension, and in the comparison to their structure with those of p-adic analytic groups, a question which is related to the unramified Fontaine-Mazur conjecture.

1.1 On the cohomological dimension

Let S be a finite set of places of K. Denote by $\mathrm{K}_S(p)$ the maximal unramified outside S pro-p extension of K; put $\mathrm{G}_{\mathrm{K},S} = \mathrm{Gal}(\mathrm{K}_S(p)/\mathrm{K})$. For $p = 2$ and for a real archimedean place v not in S, we assume that v splits totally in $\mathrm{K}_S(p)/\mathrm{K}$. Hence, $\mathrm{K}^{ur}(p) = \mathrm{K}_\emptyset(p)$, $\mathrm{G}_\mathrm{K}^{ur}(p) = \mathrm{G}_{\mathrm{K},\emptyset}(p)$, and by class field theory the p-Sylow Cl_K of the class group of K is isomorphic to the abelianization of $\mathrm{G}_\mathrm{K}^{ur}(p)$. When S contains the set S_p of all p-adic places, and when moreover K is totally imaginary for $p = 2$, it has been known for a long time that the cohomological dimension $cd(\mathrm{G}_{\mathrm{K},S}(p))$ of the groups $\mathrm{G}_{\mathrm{K},S}(p)$ is at most 2 (See for example [12], [24, Chapter X, §2], etc.). In the two last decades, various results have completed this fact.

− First, when $S_p \subset S$, Schmidt in [29] completed the Galois cohomological study of $\mathrm{G}_{\mathrm{K},S}(p)$ at $p = 2$, proving in particular that if S contains a real place, then the group $\mathrm{G}_{\mathrm{K},S}(p)$ has some torsion (and then $cd(\mathrm{G}_{\mathrm{K},S}(p)) = \infty$).

− A short while later, Labute in [17] made a real breakthrough by giving some examples of pro-p groups of cohomological dimension 2 when $S \cap S_p = \emptyset$. Recall that in this tame context, the cohomological dimension $cd(\mathrm{G}_{\mathrm{K},S}(p))$ of $\mathrm{G}_{\mathrm{K},S}(p)$ is always > 1 (when $\mathrm{G}_{\mathrm{K},S}(p)$ is not trivial). Methods and ideas of Labute have been extended by many authors: Labute-Mináč [18], Schmidt [28] [30], Vogel [34], Forré [6], Gärtner [9], etc. Let us give probably the most complete result known due to Schmidt [30]: Given a finite set T of places of K with $T \cap S_p = \emptyset$, there exist infinitely many finite sets S of places of K with $T \subset S$ and $S \cap S_p = \emptyset$, such that $cd(\mathrm{G}_{\mathrm{K},S}(p)) = 2$.

In this work, when $p = 2$, we propose to give some families of imaginary quadratic number fields K for which $\mathrm{G}_\mathrm{K}^{ur}(2)$ has no quotient of cohomological dimension 2 and large 2-rank.

The starting point comes from the fact that $H^3_{et}(\mathrm{Spec}\mathcal{O}_\mathrm{K}, \mathbb{F}_2)$ is not trivial. Then we exploit a computation of cup-products in $H^3_{et}(\mathrm{Spec}\mathcal{O}_\mathrm{K}, \mathbb{F}_2)$ made by Carlson and Schlank in [3], thanks to the relationship between cohomology of number fields and étale cohomology (see the work of Mazur [23]).

We first prove that in the family of imaginary quadratic fields $\mathcal{F}^-$, there are few fields K for which $\mathrm{G}_\mathrm{K}^{ur}(2)$ has a quotient G of maximal 2-rank and of cohomological dimension 2, in particular, such that $cd(\mathrm{G}_\mathrm{K}^{ur}(2)) = 2$. Indeed, for $X \geq 2$ denote by

$$\mathcal{F}_X^- := \{\mathrm{K} \in \mathcal{F}^-,\ |\mathrm{disc}_\mathrm{K}| \leq X\},$$

and

$$\mathcal{D}_X^- = \{\mathrm{K} \in \mathcal{F}_X^-, \mathrm{G}_\mathrm{K}^{ur}(2) \text{ has no quotient G s.t. } cd(\mathrm{G}) = 2 \ \&\ d_2\mathrm{G} = d_2\mathrm{G}_\mathrm{K}^{ur}(2)\}.$$

THEOREM 1. *One has:*

$$0 \leq 1 - \frac{\#\mathcal{D}_X^-}{\#\mathcal{F}_X^-} \leq C\frac{\log\log X}{\sqrt{\log X}},$$

where C is an absolute constant.

Next, we extend this result by using a bilinear form that appears in the study of the 4-rank of the class group of number fields. Let us be more precise. Let $(x_i)_{i=1,\cdots,n}$ be an $\mathbb{F}_2$-basis of $H^1(\mathrm{G}_{\mathrm{K}}^{ur}(2),\mathbb{F}_2) \simeq H^1_{et}(\mathrm{Spec}\mathcal{O}_{\mathrm{K}},\mathbb{F}_2)$, and consider the $n \times n$-square matrix $\mathrm{M}_{\mathrm{K}} := (a_{i,j})_{i,j}$ with coefficients in $\mathbb{F}_2$, where the $a_{i,j}$'s are cup-products $a_{i,j} = x_i \cup x_i \cup x_j$, thanks to the fact that here $H^3_{et}(\mathrm{Spec}\mathcal{O}_{\mathrm{K}},\mathbb{F}_2) \simeq \mathbb{F}_2$. As we will see, this is the Gram matrix of a certain bilinear form defined, via the Artin symbol, on the Kummer radical of the 2-elementary abelian maximal unramified extension $\mathrm{K}^{ur,2}/\mathrm{K}$ of K. We also will see that for imaginary quadratic number fields, this matrix is often of large rank.

For a profinite group G, as usual we denote by $d_p\mathrm{G} := \dim_{\mathbb{F}_p} H^1(\mathrm{G},\mathbb{F}_p)$ the p-rank of G.

We can now present the second result of our work:

THEOREM 2. *Let* K *be a totally imaginary number field. Then the pro-*2 *group* $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ *has no quotient* G *for which* $cd(\mathrm{G}) = 2$ *and* $d_2\mathrm{G} > d_2\mathrm{Cl}_{\mathrm{K}} - \frac{1}{2}\mathrm{rk}(\mathrm{M}_{\mathrm{K}})$.

Now the key fact is the following: by relating the matrix M_{K} to a Rédei-matrix type, and thanks to the work of Gerth [10] and Fouvry-Klüners [8], one can also deduce some density information when K varies in $\mathcal{F}^-$. For $n, d, X \geq 0$, denote by

$$\mathcal{F}_{n,X} := \{\mathrm{K} \in \mathcal{F}_X^-, \quad d_2\mathrm{Cl}_{\mathrm{K}} = n\},$$

$$\mathcal{D}_{n,X}^{(d)} := \{\mathrm{K} \in \mathcal{F}_{n,X},\ \mathrm{G}_{\mathrm{K}}^{ur}(2) \text{ has no quotient G s.t. } cd(\mathrm{G}) = 2 \ \&\ d_2\mathrm{G} \geq d\},$$

and consider the limit:

$$\mathcal{D}_n^{(d)} := \liminf_{X\to+\infty} \frac{\#\mathcal{D}_{n,X}^{(d)}}{\#\mathcal{F}_{n,X}}.$$

In the family of imaginary quadratic fields K where the 2-rank of the class group is equal to n, the quantity $\mathcal{D}_n^{(d)}$ measures the proportion of fields K for which $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ has no quotient G of cohomological dimension 2 and of 2-rank $d_2\mathrm{G} \geq d$.

Then [10] allows us to obtain the following densities:

COROLLARY i. *One has:*

(*i*) $\mathcal{D}_5^{(3)} \geq .33129$, $\mathcal{D}_5^{(4)} \geq .99062$, $\mathcal{D}_5^{(5)} \geq .99999$,

(*ii*) $\mathcal{D}_6^{(4)} \geq .86718$, $\mathcal{D}_6^{(5)} \geq .99925$, $\mathcal{D}_6^{(6)} \geq 1 - 5.2 \cdot 10^{-8}$.

Moreover, for large n, $\mathcal{D}_n^{(2+n/2)} \geq .99995$.

To conclude, let us mention a general asymptotic estimate thanks to [8]. Put

$$\mathcal{D}_X^{[i]} := \{\mathrm{K} \in \mathcal{F}_X^-,\ \mathrm{G}_{\mathrm{K}}^{ur}(2) \text{ has no quotient G s.t. } cd(\mathrm{G}) = 2 \ \&\ d_2\mathrm{G} \geq i + \frac{d_2\mathrm{Cl}_{\mathrm{K}}}{2}\}$$

and

$$\mathcal{D}^{[i]} := \liminf_{X\to+\infty} \frac{\#\mathcal{D}_X^{[i]}}{\#\mathcal{F}_X^-}.$$

Our work allows us to obtain:

COROLLARY ii. *One has:*

$$\mathcal{D}^{[1]} \geq .28878, \quad \mathcal{D}^{[2]} \geq 0.99471, \quad \text{and} \quad \mathcal{D}^{[3]} \geq 1 - 9.7\cdot 10^{-8}.$$

REMARK. *At this point, one should make three observations.*
1) Perhaps for many $\mathrm{K} \in \mathcal{F}_{3,X}$ *and* $\mathcal{F}_{4,X}$*, the pro-2 group* $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ *is finite but, by the Theorem of Golod-Shafarevich (see for example [16]), for every* $\mathrm{K} \in \mathcal{F}_{n,X}$*,* $n \geq 5$*, the pro-2 group* $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ *is infinite.*
2) In our work, it will appear that we have no information about the cohomological dimension of the quotients of $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ *for number fields* K *for which the* 4*-rank of the class group is large. Typically, in the estimates of* $\mathcal{D}_i^{(*)}$ *one keeps out all the number fields having maximal* 4*-rank.*
3) A part of the computation of [3] has been extended in [1] by Bleher, Chinburg, Greenberg, Kakde, Pappas and Taylor, at all p *and number fields* K *containing* μ_p*.*

1.2 ON THE UNRAMIFIED FONTAINE-MAZUR CONJECTURE AT $p = 2$

Now we also propose to give a relation between the unramified Fontaine-Mazur conjecture (conjecture (5b) of [5]) and the matrix M_{K} defined before. More precisely, here we are interested in uniform quotients of $\mathrm{G}_{\mathrm{K}}^{ur}(p)$ (see section 2.2 for definition) which are related to the unramified Fontaine-Mazur conjecture thanks to the following equivalent version:

CONJECTURE 1.1. *Every uniform quotient* G *of* $\mathrm{G}_{\mathrm{K}}^{ur}(p)$ *is trivial.*

Remark that Conjecture 1.1 can be rephrased as follows: the pro-p group $\mathrm{G}_{\mathrm{K}}^{ur}(p)$ has no uniform quotient G of dimension d for all $d > 0$. As we will see, the matrix M_{K} dectects the 4-rank of the class group of K, and the 4-rank is a first test for Conjecture 1.1. We also obtain:

THEOREM 3. *Let* $\mathrm{K}/\mathbb{Q}$ *be a number field.*

(*i*) *Suppose that the* 4*-rank of the class group of* K *is at most* 2*. Then Conjecture 1.1 holds for* K *(at* $p = 2$*).*

(*ii*) *Suppose* K *is totally imaginary. Then the pro-*2 *group* $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ *has no uniform quotient of dimension* $d > d_2\mathrm{Cl}_{\mathrm{K}} - \mathrm{rk}(\mathrm{M}_{\mathrm{K}})$*. In particular, Conjecture 1.1 holds (for* $\mathrm{G}_{\mathrm{K}}^{ur}(2)$*) when* $\mathrm{rk}(\mathrm{M}_{\mathrm{K}}) \geq d_2\mathrm{Cl}_{\mathrm{K}} - 2$*.*

Now as for the cohomological dimension, one can also deduce a general asymptotic estimate when K varies in the family $\mathcal{F}^-$ (resp. $\mathcal{F}^+$) of imaginary (resp.

real) quadratic fields. For $n, d, X \geq 0$, denote by $\mathcal{F}_X^{\pm} := \{\mathrm{K} \in \mathcal{F}^{\pm},\ |\mathrm{disc_K}| \leq X\}$. Put

$$\mathrm{FM}_X^{\pm} := \{\mathrm{K} \in \mathcal{F}_X^{\pm}, \text{Conjecture 1.1 holds for K }\}$$

and

$$\mathrm{FM}^{\pm} := \liminf_{X \to +\infty} \frac{\#\mathrm{FM}_X^{\pm}}{\#\mathcal{F}_X^{\pm}}.$$

COROLLARY iii. *One has*

$$\mathrm{FM}^{-} \geq .99471, \text{ and } \mathrm{FM}^{+} \geq .99929.$$

This paper has five sections. In Section 2, we give the elementary tools concerning the étale cohomology of number fields and p-adic analytic groups. In section 3, we develop some basic facts about bilinear forms over $\mathbb{F}_2$, specially for the form introduced in our study (which is defined on a certain Kummer radical). In particular, we emphasize the role played by totally isotropic subspaces. Section 4 is devoted to considerations of cohomological dimension. After proving Theorem 1 and Theorem 2 we consider a relation with a Rédei matrix that allows us to obtain density information. In Section 5, we consider the unramified Fontaine-Mazur conjecture at $p = 2$ by showing the relation with the bilinear form studied in the previous sections. We finish this section by giving a computational approach of this conjecture.

NOTATIONS

• Let p be a prime number and let K be a number field. Denote by

- $p^* = (-1)^{(p-1)/2}p$, when p is odd;
- $\mathcal{O}_\mathrm{K}$ the ring of integers of K;
- $\mathrm{Cl_K}$ the p-Sylow of the class group of $\mathcal{O}_\mathrm{K}$;
- $d_p\mathrm{Cl_K}$ the p-rank of $\mathrm{Cl_K}$: it is the dimension over $\mathbb{F}_p$ of $\mathbb{F}_p \otimes \mathrm{Cl_K}$;
- $\mathrm{K}^{ur}(p)$ the maximal pro-p extension of K unramified everywhere. Put $\mathrm{G}_\mathrm{K}^{ur}(p) := \mathrm{Gal}(\mathrm{K}^{ur}(p)/\mathrm{K})$.

Recall that the group $\mathrm{G}_\mathrm{K}^{ur}(p)$ is a finitely presented pro-p group (due to Koch [16]). See also for example [24, Chapter X, §7] or [11, Appendix]. Moreover $\mathrm{Cl_K}$ is isomorphic to the abelianization of $\mathrm{G}_\mathrm{K}^{ur}(p)$. In particular it implies that every open subgroup $\mathcal{H}$ of $\mathrm{G}_\mathrm{K}^{ur}(p)$ has finite abelianization: this property is known as "FAb".

• If G is a finitely generated pro-p group, denote by

- $H^i(\mathrm{G}) := H^i(\mathrm{G}, \mathbb{F}_p)$, $i \in \mathbb{Z}_{\geq 0}$;
- $d_p\mathrm{G} = \dim_{\mathbb{F}_p} H^1(\mathrm{G})$ the p-rank of G;

– $cd(\mathrm{G})$ the cohomological dimension of G: it is the smallest integer $n \geq 0$ such that $H^{n+m}(\mathrm{G}) = \{0\}, \forall m > 0$.

ACKNOWLEDGEMENTS. This work has been done during a visiting scholar position at Cornell University for the academic year 2017-18, and funded by the program "Mobilité sortante" of the Région Bourgogne Franche-Comté. The author thanks the Department of Mathematics at Cornell University for providing a beautiful research atmosphere. He also thanks Georges Gras and Farshid Hajir for encouragement and useful remarks, Ravi Ramakrishna for very inspiring discussions, Alexander Schmidt for helpful comments, and constructive observations concerning the cup-products, Etienne Fouvry for stimulating exchanges and the computation of Proposition 4.7 which is central for Theorem 1, Magnus Carlson for his interest and comments, Christophe Delaunay for some references, and Bill Allombert for the support concerning the use of GP-Pari [25].

2 GENERALITIES

2.1 CUP-PRODUCTS AND ETALE COHOMOLOGY: WHAT WE NEED

Assume K is totally imaginary when $p = 2$, and put $\mathrm{X_K} = \mathrm{Spec}\mathcal{O}_\mathrm{K}$. We use the formalism of étale cohomology H^i_{et} of the site $\mathrm{X_K}$ that we can find for example in [23] (see also for example [28], [29]). The Hochschild-Serre spectral sequence gives for every $i \geq 1$ a map

$$\alpha_i : H^i(\mathrm{G}_\mathrm{K}^{ur}(p)) \longrightarrow H^i_{et}(\mathrm{X_K}),$$

where the coefficients are in $\mathbb{F}_p$ (meaning the constant sheaf for the étale site $\mathrm{X_K}$). Remark that α_1 is an isomorphism. As $H^1_{et}(\mathrm{X}_{\mathrm{K}^{ur}(p)})$ is trivial, one obtains the long exact sequence (see for example [24, Chapter I, Proposition 1.6.7]):

$$H^2(\mathrm{G}_\mathrm{K}^{ur}(p)) \hookrightarrow H^2_{et}(\mathrm{X_K}) \longrightarrow H^2_{et}(\mathrm{X}_{\mathrm{K}^{ur}(p)})^{\mathrm{G}_\mathrm{K}^{ur}(p)} \longrightarrow H^3(\mathrm{G}_\mathrm{K}^{ur}(p)) \longrightarrow H^3_{et}(\mathrm{X_k}) \tag{1}$$

where $H^3_{et}(\mathrm{X_k}) \simeq (\mu_{\mathrm{K},p})^\vee$, here $(\mu_{\mathrm{K},p})^\vee$ is the Pontryagin dual of the group of pth-roots of unity in K.
For the two next subsections, take $p = 2$.

2.1.1 CUP-PRODUCTS IN H^2_{et}

Recall a result concerning cup-products in H^2.

PROPOSITION 2.1. *Let* G *be a finitely presented pro-2 group. Take* $x \in H^1(\mathrm{G})$. *Then* x *lifts in* $H^1(\mathrm{G}, \mathbb{Z}/4\mathbb{Z})$ *if and only if,* $x \cup x = 0 \in H^2(\mathrm{G})$. *In particular, the cup-product* $H^1(\mathrm{G}) \otimes H^1(\mathrm{G}) \to H^2(\mathrm{G})$ *is alternating (*$x \cup x = 0$ *for all* $x \in H^1(\mathrm{G})$*) if and only if,* $\mathrm{G}/\mathrm{G}^4[\mathrm{G},\mathrm{G}] \simeq (\mathbb{Z}/4\mathbb{Z})^n$, *where* $n = d_2\mathrm{G}$.

Proof. See for example [31, Chapter 1, §1.2]. □

Take x a non-trivial character of $H^1(\mathrm{G}^{ur}(p)) \simeq H^1_{et}(\mathrm{X_K})$. Put $\mathrm{K}_x = (\mathrm{K}^{ur})^{ker(x)}$. Hence the previous proposition allows us to recover the following corollary of Carlson and Schlank [3, Corollary 5.14]:

COROLLARY 2.2. *The cup-product $x \cup x \in H^2_{et}(\mathrm{X_K})$ is trivial if and only, the quadratic extension K_x/K embeds in an unramified degree 4 cyclic extension.*

Proof. Indeed, as $H^2(\mathrm{G}^{ur}_{\mathrm{K}}(2)) \hookrightarrow H^2_{et}(\mathrm{X_K})$, see (1), the cup-product $x \cup x$ vanishes in $H^2(\mathrm{G}^{ur}_{\mathrm{K}}(2))$ if and only if, it vanishes in $H^2_{et}(\mathrm{X_K})$. Then, apply Proposition 2.1 to $\mathrm{G} = \mathrm{G}^{ur}_{\mathrm{K}}(2)$. □

REMARK 2.3. *It is not difficult to see that Corollary 2.2 allows us to obtain the following equivalence (see [3]): $x \cup x = 0 \in H^2_{et}(\mathrm{X_K})$ if and only if, for all $h \in \mathrm{Cl_K}[2]$, h is a norm in K_x/K. Here $\mathrm{Cl_K}[2]$ denotes the kernel of the map $\mathrm{Cl_K} \overset{h \mapsto h^2}{\longrightarrow} \mathrm{Cl_K}$.*

2.1.2 CUP-PRODUCTS IN H^3_{et}

Take x and y two non-trivial characters of $H^1(\mathrm{G}^{ur}(p)) \simeq H^1_{et}(\mathrm{X})$. By Kummer theory, there exist $a_x, a_y \in \mathrm{K}^\times/(\mathrm{K}^\times)^2$ such that $\mathrm{K}_x = \mathrm{K}(\sqrt{a_x})$ and $\mathrm{K}_y = \mathrm{K}(\sqrt{a_y})$. As the extension K_y/K is unramified, for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_\mathrm{K}$, the $\mathfrak{p}$-valuation $v_\mathfrak{p}(a_y)$ is even, and then $\sqrt{(a_y)}$ is well-defined (as an ideal of $\mathcal{O}_\mathrm{K}$). Let us write

$$\sqrt{(a_y)} := \prod_i (\mathfrak{p}_{y,i})^{e_{y,i}}.$$

Denote by I_x the set of prime ideals $\mathfrak{p}$ of $\mathcal{O}_\mathrm{K}$ such that $\mathfrak{p}$ is inert in K_x/K (or equivalently, I_x is the set of primes of K such that the Frobenius at $\mathfrak{p}$ generates $\mathrm{Gal}(\mathrm{K}_x/\mathrm{K})$). In [3, Proposition 3.3], Carlson and Schlank prove:

PROPOSITION 2.4. *The cup-product $x \cup x \cup y \in H^3_{et}(X)$ is non-zero if and only if, $\sum_{\mathfrak{p}_{y,i} \in I_x} e_{y,i}$ is odd.*

REMARK 2.5. *The condition of Proposition 2.4 is equivalent to the triviality of the Artin symbol $\left(\dfrac{\mathrm{K}_x/\mathrm{K}}{\sqrt{(a_y)}}\right)$.*

2.2 UNIFORM PRO-p GROUPS: WHAT WE NEED

2.2.1

Let us recall the p-central descending series $(\mathrm{G}_i)_i$ of a pro-p group G:

$$\mathrm{G}_1 = \mathrm{G},\ \mathrm{G}_{i+1} = \mathrm{G}_i^p[\mathrm{G}_i, \mathrm{G}],\ i \geq 1.$$

Let us give the definition of a uniform pro-p group (see for example [4, Chapter 4, §4.1]).

DEFINITION 2.6. *Let* G *be a finitely generated pro-p group. We say that* G *is uniform if:*

(*i*) $[\mathrm{G}, \mathrm{G}] \subset \mathrm{G}^{2p}$, *and*

(*ii*) *for* $i \geq 1$, $[\mathrm{G}_{i+1} : \mathrm{G}_i] = [\mathrm{G}_2 : \mathrm{G}]$.

REMARK 2.7. *For a uniform group* G*, the p-rank of* G *coincides with the dimension of* G *(as p-adic manifold). See [4, Chapter 4 and 8].*

The uniform pro-p groups play a central role in the study of analytic pro-p groups, indeed:

THEOREM 2.8 (Lazard [19]). *Let* G *be a profinite group. Then* G *is p-adic analytic* i.e. G *embeds as a closed subgroup of* $\mathrm{Gl}_m(\mathbb{Z}_p)$ *for some positive integer* m*, if and only if,* G *contains an open uniform subgroup* $\mathcal{H}$*.*

For different equivalent definitions of p-adic analytic groups, see [4, Interlude A]. See also [22].

2.2.2 COHOMOLOGY

Recall by Lazard [19] (see also [33] for an alternative proof):

THEOREM 2.9 (Lazard). *Let* G *be a uniform pro-p group (of dimension* $d > 0$*). Then for all* $i \geq 1$*, one has:*

$$H^i(\mathrm{G}) \simeq \bigwedge^i (H^1(\mathrm{G})),$$

where here the exterior product is induced by the cup-product.

As consequence, one has immediately:

COROLLARY 2.10. *Let* G *be a uniform pro-2 group of dimension* d*. Then for all* $x \in H^1(\mathrm{G})$*, one has* $x \cup x = 0 \in H^2(\mathrm{G})$*. In particular,* $\mathrm{G}^{ab} \twoheadrightarrow (\mathbb{Z}/4\mathbb{Z})^d$*.*

Proof. By Theorem 2.9, the cup-product form on $H^1(\mathrm{G})$ is alternating, then apply Proposition 2.1. □

REMARK 2.11. *For* $p > 2$*, Theorem 2.9 is an equivalence: a pro-p group* G *is uniform if and only if, for* $i \geq 1$*,* $H^i(\mathrm{G}) \simeq \bigwedge^i (H^1(\mathrm{G}))$*. (See [33, Corollary 5.1.7].)*

Let us mention another consequence useful in our context:

COROLLARY 2.12. *Let* G *be a FAb uniform pro-p group of dimension* $d > 0$*. Then* $d \geq 3$*.*

Proof. This is well-known. Let G be a uniform pro-p group of dimension d. If $\dim \mathrm{G} = 1$, then $\mathrm{G} \simeq \mathbb{Z}_p$ (G is pro-p free) and, if $\dim \mathrm{G} = 2$, then by Theorem 2.9, $H^2(\mathrm{G}) \simeq \mathbb{F}_p$ and then, by taking homology long exact sequence of the exact sequence $1 \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \longrightarrow \mathbb{F}_p \longrightarrow 1$, one gets

$$\cdots \longrightarrow H_2(\mathrm{G}, \mathbb{F}_p) \longrightarrow \mathrm{G}^{ab} \longrightarrow \mathrm{G}^{ab} \longrightarrow \mathrm{G}^{ab}/p \longrightarrow 1$$

and then $d_p(\mathrm{G}^{ab}[p]) \leq 1$, and $\mathrm{G}^{ab} \twoheadrightarrow \mathbb{Z}_p$. Hence, if we assume moreover that G is FAb, then $\dim \mathrm{G}$ should be at least 3. □

2.2.3 FILTRATIONS

Let us start with a finitely generated pro-p group G with its p-central descending series $(\mathrm{G}_i)_i$. Usually one has $[\mathrm{G}_i, \mathrm{G}_j] \subset \mathrm{G}_{i+j}$, but when $p = 2$ and when G is uniform, let us give a refinement of this inclusion. To do this, we need the following result (see [4, Chapter 3, Theorem 3.6]):

PROPOSITION 2.13. *When* G *is uniform, one has for* $i, k \geq 1$, $\mathrm{G}_{i+k} = \mathrm{G}_i^{p^k}$.

Here as usual, for a pro-p group G, we note by G^{p^k} the subgroup of G generated by the p^k-powers. One can now deduce the following:

COROLLARY 2.14. *Let* G *be an uniform pro-*2 *group. Then, for all* $i, j \geq 1$, *one has:* $[\mathrm{G}_i, \mathrm{G}_j] \subset \mathrm{G}_{i+j+1}$.

Proof. We prove it by induction. When $i = j = 1$, $[\mathrm{G}, \mathrm{G}] \subset \mathrm{G}^4 = \mathrm{G}_3$, and the statement holds. Suppose now that $[\mathrm{G}_i, \mathrm{G}_j] \subset \mathrm{G}_{i+j+1}$, and let us look at $[\mathrm{G}_{i+1}, \mathrm{G}_j]$. Let us apply Hall's formula:

$$[xy, z] = y^{-1}[x, z]y[x, z]^{-1}[x, z][y, z] = [y, [x, z]^{-1}][x, z][y, z],$$

to note that $[xy, z] \in \mathrm{G}_{i+j+2}$ when $[x, z]$ and $[y, z]$ are in G_{i+j+2}. Moreover, for $x \in \mathrm{G}_i$ and $z \in \mathrm{G}_j$, one has $[x, [x, z]^{-1}] \in \mathrm{G}_{2i+j+1}$ and $[x, z]^2 \in \mathrm{G}_{i+j+2}$, by hypothesis. As $[x^2, z] = [x, [x, z]^{-1}][x, z]^2$, one obtains $[x^2, z] \in \mathrm{G}_{i+j+2}$ when $x \in \mathrm{G}_i$ and $z \in \mathrm{G}_j$. One conludes thanks to the fact that $\mathrm{G}_{i+1} = \mathrm{G}_i^2$. □

In [14], the authors show that when G is uniform of dimension d then $\mathrm{G}_i/\mathrm{G}_i^{p^i}[\mathrm{G}_i, \mathrm{G}_i] \simeq (\mathbb{Z}/p^i\mathbb{Z})^d$. In fact, for $p = 2$, one can say a little bit more:

PROPOSITION 2.15. *Let* G *be an uniform pro-*2 *group of dimension* d. *Then for* $i \geq 1$, *one has*

$$\mathrm{G}_i/\mathrm{G}_i^{2^{i+1}}[\mathrm{G}_i, \mathrm{G}_i] \simeq (\mathbb{Z}/2^{i+1})^d.$$

When $i = 1$, it is an alternative proof to Corollary 2.10.

Proof. Let $S = \{g_1, \cdots, g_d\}$ be a set of generators of G. Then the elements $g_j^{2^{i-1}}$, $j = 1, \cdots, d$, generate the uniform group G_i. Let $g \in S$ and suppose that $(g^{2^{i-1}})^{2^i} \in [\mathrm{G}_i, \mathrm{G}_i]$. As $[\mathrm{G}_i, \mathrm{G}_i] \subset \mathrm{G}_{2i+1}$ by Corollary 2.14, one gets

$g^{2^{2i-1}} \in \mathrm{G}_{2i+1}$. Now let us recall that $z \mapsto z^{2^{2i-1}}$ induces an isomorphism φ_i between G/G_2 and $\mathrm{G}_{2i}/\mathrm{G}_{2i+1}$ (see [4, Chapter 4, §4.1]). But as $\varphi_i(g) = 0$, one has $g = 0$ which is a contraction. Hence, for $j = 1, \cdots, d$, the element $g_j^{2^{i-1}}$ is of order at least 2^{i+1} in $\mathrm{G}_i/[\mathrm{G}_i, \mathrm{G}_i]$. □

3 Bilinear form over the 2-elementary maximal unramified extension

3.1 Bilinear forms over $\mathbb{F}_2$

Let $\mathcal{B}$ be a bilinear form over an $\mathbb{F}_2$-vector space V of finite dimension. Denote by n the dimension of V and by $\mathrm{rk}(\mathcal{B})$ the rank of $\mathcal{B}$.

DEFINITION 3.1. *Given a bilinear form $\mathcal{B}$, one defines the index $\nu(\mathcal{B})$ of $\mathcal{B}$ by*

$$\nu(\mathcal{B}) := \max_{W \subset \mathrm{V}} \{\dim W,\ \mathcal{B}(W, W) = 0\}.$$

One has:

PROPOSITION 3.2. *The index $\nu(\mathcal{B})$ of a bilinear form $\mathcal{B}$ is at most $n - \frac{1}{2}\mathrm{rk}(\mathcal{B})$.*

Proof. Let W be a totally isotropic subspace of V of dimension i. Let us complete a basis of W to a basis B of V. It is then easy to see that the Gram matrix of $\mathcal{B}$ in B is of rank at most $2n - 2i$. □

This bound is in a certain sense optimal as we can achieve it in the symmetric case.

DEFINITION 3.3. (*i*) *Given $a \in \mathbb{F}_2$. The bilinear form $\mathcal{H}(a)$ with matrix* $\begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}$ *is called a metabolic plane.*
(*ii*) *A symmetric bilinear form $(V, \mathcal{B})$ is called alternating if $\mathcal{B}(x, x) = 0$ for all $x \in V$. Otherwise $\mathcal{B}$ is called nonalternating.*

Recall the Witt decomposition Theorem for symmetric bilinear forms over $\mathbb{F}_2$ (see for example [15, Chapter I, §2, Remark 5 of Theorem 1]).

THEOREM 3.4. *Let $(V, \mathcal{B})$ be a symmetric bilinear form of dimension n over $\mathbb{F}_2$. Denote by r the rank of $\mathcal{B}$. Write $r = 2r_0 + \delta$, with $\delta = 0$ or 1, and $r_0 \in \mathbb{N}$.*

(*i*) *If $\mathcal{B}$ is nonalternating, then $(V, \mathcal{B})$ is isometric to*

$$\overbrace{\mathcal{H}(1) \perp \cdots \perp \mathcal{H}(1)}^{r_0} \perp \overbrace{\langle 1 \rangle}^{\delta} \perp \overbrace{\langle 0 \rangle \perp \cdots \perp \langle 0 \rangle}^{n-r} \simeq \overbrace{\langle 1 \rangle \perp \cdots \perp \langle 1 \rangle}^{r} \perp \overbrace{\langle 0 \rangle \perp \cdots \perp \langle 0 \rangle}^{n-r};$$

(*ii*) *If $\mathcal{B}$ is alternating, then $\mathcal{B}$ is isometric to*

$$\overbrace{\mathcal{H}(0) \perp \cdots \perp \mathcal{H}(0)}^{r_0} \perp \overbrace{\langle 0 \rangle \perp \cdots \perp \langle 0 \rangle}^{n-r}.$$

Moreover, $\nu(\mathcal{B}) = n - r + r_0 = n - r_0 - \delta$.

When $(\mathrm{V}, \mathcal{B})$ is not necessary symmetric, let us introduce the symmetrization $\mathcal{B}^{sym}$ of $\mathcal{B}$ by

$$\mathcal{B}^{sym}(x, y) = \mathcal{B}(x, y) + \mathcal{B}(y, x), \quad \forall x, y \in \mathrm{V}.$$

One has:

COROLLARY 3.5. *Let* $(\mathrm{V}, \mathcal{B})$ *be a bilinear form of dimension* n *over* $\mathbb{F}_2$. *Then*

$$\nu(\mathcal{B}) \geq n - \lfloor \frac{1}{2}\mathrm{rk}(\mathcal{B}^{\mathrm{sym}}) \rfloor - \lfloor \frac{1}{2}\mathrm{rk}(\mathcal{B}) \rfloor.$$

In particular, $\nu(\mathcal{B}) \geq \min\{n - \frac{3}{2}\mathrm{rk}(\mathcal{B}), \frac{1}{2}(n - \mathrm{rk}(\mathcal{B})\}$.

Proof. It is easy. Let us start with a maximal totally isotropic subspace W of $(\mathrm{V}, \mathcal{B}^{sym})$. Then $\mathcal{B}_{|\mathrm{W}}$ is symmetric: indeed, for any two $x, y \in \mathrm{W}$, we get $0 = \mathcal{B}^{sym}(x, y) = \mathcal{B}(x, y) + \mathcal{B}(y, x)$, and then $\mathcal{B}(x, y) = \mathcal{B}(y, x)$ (recall that V is defined over $\mathbb{F}_2$). Hence by Theorem 3.4, $\mathcal{B}_{|\mathrm{W}}$ has a totally isotropic subspace of dimension $\nu(\mathcal{B}_{|\mathrm{W}}) = \dim \mathrm{W} - \lfloor \frac{1}{2}\mathrm{rk}(\mathcal{B}_{|\mathrm{W}}) \rfloor$. As $\dim \mathrm{W} = n - \lfloor \frac{1}{2}\mathrm{rk}(\mathcal{B}^{\mathrm{sym}}) \rfloor$ (by Theorem 3.4), one obtains the first assertion. For the second one, it is enough to note that $\mathrm{rk}(\mathcal{B}^{\mathrm{sym}}) \leq \max\{2\mathrm{rk}(\mathcal{B}), n\}$. □

3.2 BILINEAR FORM AND KUMMER RADICAL

Let us start with a number field K. Denote by n the 2-rank of $\mathrm{G}_{\mathrm{K}}^{ur}(2)$, in other words, $n = d_2\mathrm{Cl}_{\mathrm{K}}$.

Let $V = \langle a_1, \cdots, a_n \rangle (\mathrm{K}^\times)^2 \in \mathrm{K}^\times/(\mathrm{K}^\times)^2$ be the Kummer radical of the 2-elementary abelian maximal unramified extension $\mathrm{K}^{ur,2}/\mathrm{K}$. Then V is an $\mathbb{F}_2$-vector space of dimension n. For $a \in V$, denote $\mathrm{K}_a := \mathrm{K}(\sqrt{a})$, and $\mathfrak{a}(a) := \sqrt{(a)} \in \mathcal{O}_{\mathrm{K}}$ (see section 2.1.2). We can now introduce the bilinear form $\mathcal{B}_{\mathrm{K}}$ that plays a central role in our work.

DEFINITION 3.6. *For* $a, b \in V$, *put:*

$$\mathcal{B}_{\mathrm{K}}(a, b) = \left(\frac{\mathrm{K}_a/\mathrm{K}}{\mathfrak{a}(b)} \right) \cdot \sqrt{a} \Big/ \sqrt{a} \in \mathbb{F}_2,$$

where here we use the additive notation.

Of course, we have:

LEMMA 3.7. *The application* $\mathcal{B}_{\mathrm{K}} : V \times V \to \mathbb{F}_2$ *is a bilinear form on* V.

Proof. The linearity on the right comes from the linearity of the Artin symbol. Let us show that $\mathcal{B}_{\mathrm{K}}$ is linear on the left. Take $a_1 \neq a_2 \in \mathrm{V}$, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{\mathrm{K}}$. Let us remark the following:

• If $\mathfrak{p}$ splits in $\mathrm{K}_{a_1}/\mathrm{K}$ and in $\mathrm{K}_{a_2}/\mathrm{K}$, then $\mathfrak{p}$ splits in $\mathrm{K}_{a_1a_2}/\mathrm{K}$;
• If $\mathfrak{p}$ is inert in $\mathrm{K}_{a_1}/\mathrm{K}$ and in $\mathrm{K}_{a_2}/\mathrm{K}$, then $\mathfrak{p}$ splits in $\mathrm{K}_{a_1a_2}/\mathrm{K}$;
• If $\mathfrak{p}$ is inert in $\mathrm{K}_{a_1}/\mathrm{K}$ but splits in $\mathrm{K}_{a_2}/\mathrm{K}$, then $\mathfrak{p}$ is inert in $\mathrm{K}_{a_1a_2}/\mathrm{K}$.

Hence for each case one has $\left(\frac{\mathrm{K}_{a_1a_2}/\mathrm{K}}{\mathfrak{p}}\right) = \left(\frac{\mathrm{K}_{a_1}/\mathrm{K}}{\mathfrak{p}}\right) + \left(\frac{\mathrm{K}_{a_2}/\mathrm{K}}{\mathfrak{p}}\right)$, and we conclude by using again the linearity of the Artin symbol. □

The bilinear form $\mathcal{B}_{\mathrm{K}}$ is not necessarily symmetric, but we will give later some situations where $\mathcal{B}_{\mathrm{K}}$ is symmetric.

REMARK 3.8. *Assume* K *is totally imaginary. If we denote by* x_i *a generator of* $H^1(\mathrm{Gal}(\mathrm{K}(\sqrt{a_i})/\mathrm{K}))$*, then the Gram matrix of the bilinear form* $\mathcal{B}_{\mathrm{K}}$ *in the basis* $\{a_1(\mathrm{K}^\times)^2, \cdots, a_n(\mathrm{K}^\times)^2\}$ *is exactly the matrix* $(x_i \cup x_i \cup x_j)_{i,j}$ *of the cup-products in* $H^3_{et}(\mathrm{Spec}\mathcal{O}_{\mathrm{K}})$*. See Proposition 2.4 and Remark 2.5. Hence the bilinear form* $\mathcal{B}_{\mathrm{K}}$ *coincides with the bilinear form* $\mathcal{B}^{et}_{\mathrm{K}}$ *on* $H^1_{et}(\mathrm{Spec}\mathcal{O}_{\mathrm{K}})$ *defined by* $\mathcal{B}^{et}_{\mathrm{K}}(x,y) = x \cup x \cup y \ \in H^3_{et}(\mathrm{Spec}\mathcal{O}_{\mathrm{K}})$*.*

Recall that the right-radical (resp. left-radical) $\mathcal{R}ad_r$ (resp. $\mathcal{R}ad_l$) of a bilinear form $\mathcal{B}$ on V is the subspace defined by: $\mathcal{R}ad_r := \{x \in \mathrm{V},\ \mathcal{B}(V,x) = 0\}$ (resp. $\mathcal{R}ad_l := \{x \in \mathrm{V},\ \mathcal{B}(x,V) = 0\}$. Of course one always has $\dim \mathcal{B} = \mathrm{rk}(\mathcal{B}) + \dim(\mathcal{R}ad_r) = \mathrm{rk}(\mathcal{B}) + \dim(\mathcal{R}ad_l)$. And, remark moreover that the restriction of $\mathcal{B}$ at $\mathcal{R}ad_r$ (resp. $\mathcal{R}ad_l$) produces a totally isotropic subspace of V.

Let us come back to the bilinear form $\mathcal{B}_{\mathrm{K}}$ on the Kummer radical of $\mathrm{K}^{ur,2}/\mathrm{K}$, and let us give now three types of totally isotropic subspaces W that may appear.

PROPOSITION 3.9. *Let* $\mathrm{W} := \langle \varepsilon_1, \cdots, \varepsilon_r\rangle(\mathrm{K}^\times)^2 \subset \mathrm{V}$ *be an* $\mathbb{F}_2$*-subspace of dimension* r*, generated by some units* $\varepsilon_i \in \mathcal{O}_{\mathrm{K}}^\times$*. Then* $\mathrm{W} \subset \mathcal{R}ad_r$*, and thus* $(\mathrm{V}, \mathcal{B}_{\mathrm{K}})$ *contains* W *as a totally isotropic subspace of dimension* r*.*

Proof. Indeed, here $\mathfrak{a}(\varepsilon_i) = \mathcal{O}_{\mathrm{K}}$ for $i = 1, \cdots, r$. □

PROPOSITION 3.10. *Let* $\mathrm{K} = \mathrm{k}(\sqrt{b})$ *be a quadratic extension. Suppose that there exist* $a_1, \cdots, a_r \in \mathrm{k}$ *such that the extensions* $\mathrm{k}(\sqrt{a_i})/\mathrm{k}$ *are independent and unramified everywhere. Suppose moreover that* $b \notin \langle a_1, \cdots, a_r\rangle(\mathrm{k}^\times)^2$*. Then* $\mathrm{W} := \langle a_1, \cdots, a_r\rangle(\mathrm{K}^\times)^2$ *is a totally isotropic subspace of dimension* r*.*

Proof. Let $\mathfrak{p} \subset \mathcal{O}_{\mathrm{k}}$ be a prime ideal of $\mathcal{O}_{\mathrm{k}}$. It is sufficient to prove that $\left(\frac{\mathrm{K}_{a_i}/\mathrm{K}}{\mathfrak{p}}\right)$ is trivial. Let us study all the possibilities.
• If $\mathfrak{p}$ is inert in K/k, then as $\mathrm{K}(\sqrt{a_i})/\mathrm{K}$ is unramified at $\mathfrak{p}$, $\mathfrak{p}$ must split in $\mathrm{K}(\sqrt{a_i})/\mathrm{K}$ and then $\left(\frac{\mathrm{K}_{a_i}/\mathrm{K}}{\mathfrak{p}}\right)$ is trivial.
• If $\mathfrak{p} = \mathfrak{P}^2$ is ramified in K/k, then $\left(\frac{\mathrm{K}_{a_i}/\mathrm{K}}{\mathfrak{p}}\right) = \left(\frac{\mathrm{K}_{a_i}/\mathrm{K}}{\mathfrak{P}}\right)^2$ is trivial.

• If $\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2$ splits, then obviously $\left(\frac{\mathrm{K}_{a_i}/\mathrm{K}}{\mathfrak{P}_1}\right) = \left(\frac{\mathrm{K}_{a_i}/\mathrm{K}}{\mathfrak{P}_2}\right)$, and then $\left(\frac{\mathrm{K}_{a_i}/\mathrm{K}}{\mathfrak{p}}\right)$ is trivial. □

PROPOSITION 3.11. *Suppose* K *is totally imaginary. Let* $\mathrm{W} := \langle a_1, \cdots, a_r\rangle(\mathrm{K}^\times)^2 \subset \mathrm{V}$ *be a subspace of* V *such that each quadratic extension* $\mathrm{K}(\sqrt{a_i})/\mathrm{K}$, $i = 1, \cdots, r$, *embeds in an unramified degree* 4 *cyclic extension. Then* $W \subset \mathcal{R}ad_l$.

Proof. Denote by x_i a generator of $H^1(\mathrm{Gal}(\mathrm{K}_{a_i}/\mathrm{K}))$. By Proposition 2.2, we get $x_i \cup x_i = 0 \in H^2_{et}(\mathrm{G}^{ur}_{\mathrm{K}}(2))$, and then $\mathcal{B}_{\mathrm{K}}(a_i, V) = 0$ by Remark 3.8. □

It is then natural to define the index of K as follows:

DEFINITION 3.12. *The index* $\nu(\mathrm{K})$ *of* K *is the index of the bilinear form* $\mathcal{B}_{\mathrm{K}}$.

Of course, if the form $\mathcal{B}_{\mathrm{K}}$ is non-degenerate, one has: $\nu(\mathrm{K}) \leq \frac{1}{2}d_2\mathrm{Cl}_{\mathrm{K}}$. Thus one says that Cl_{K} is non-degenerate if the form $\mathcal{B}_{\mathrm{K}}$ is non-degenerate.

To finish this part, let us give the relation with the 4-rank $\mathrm{R}_{\mathrm{K},4}$ of the class group Cl_{K} defined as follows: $\mathrm{R}_{\mathrm{K},4} := \dim_{\mathbb{F}_2} \mathrm{Cl}_{\mathrm{K}}[4]/\mathrm{Cl}_{\mathrm{K}}[2]$, where $\mathrm{Cl}_{\mathrm{K}}[m] = \{c \in \mathrm{Cl}_{\mathrm{K}}, c^m = 1\}$. One has immediately:

PROPOSITION 3.13. *Let* K *be a totally imaginary number field. Then* $\mathrm{R}_{\mathrm{K},4} \leq d_2\mathrm{Cl}_{\mathrm{K}} - \mathrm{rk}(\mathcal{B}_{\mathrm{K}})$.

Proof. Indeed, the subspace of characters of $H^1(\mathrm{G}^{ur}_{\mathrm{K}}(2))$ corresponding to the unramified degree 4 cyclic extensions of K is a subspace of the left-radical of $\mathcal{B}_{\mathrm{K}}$ (see Proposition 3.11), and then $\mathrm{R}_{\mathrm{K},4} \leq \dim \mathcal{R}ad_l$. To conclude, use the fact that $n = d_2\mathrm{Cl}_{\mathrm{K}} = \dim \mathcal{R}ad_l + \mathrm{rk}(\mathcal{B}_{\mathrm{K}})$. □

REMARK 3.14. *Of course, Proposition 3.13 can be made more precise in many cases. Typically, in the quadratic case thanks to the Rédei matrix (see Section 4.3.4). See also the generalization of Yue [36].*

4 On the cohomological dimension

4.1 A first observation

For basic facts concerning the cohomological dimension of a pro-p group we refer for example to [24, Chapter III].

Before developing a general setting, let us start with the following observation. Let $\mathcal{O}^\times_{\mathrm{K}^{ur}(p)}$ be the group generated by the units of the ring of integers of all subextensions F/K of $\mathrm{K}^{ur}(p)/\mathrm{K}$. Let us recall the following result due to Wingberg [35, Theorem 1.1] (see also [24, Chapter VIII, §8, Corollary 8.8.3]):

THEOREM 4.1 (Wingberg). *There are canonical isomorphims:*

$$\hat{H}^i(\mathrm{G}_\mathrm{K}^{ur}(p), \mathcal{O}^\times_{\mathrm{K}^{ur}(p)}) \simeq \hat{H}^{3-i}(\mathrm{G}_\mathrm{K}^{ur}(p), \mathbb{Z})^\vee,$$

for all $i \in \mathbb{Z}$.

Hence, the exact sequence $0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{p} \mathbb{Q}/\mathbb{Z} \longrightarrow 0$ allows us to obtain:

$$H_3(\mathrm{G}_\mathrm{K}^{ur}(p), \mathbb{F}_p) \longrightarrow \hat{H}^0(\mathrm{G}_\mathrm{K}(p), \mathcal{O}^\times_{\mathrm{K}^{ur}(p)}) \xrightarrow{p} \hat{H}^0(\mathrm{G}_\mathrm{K}(p), \mathcal{O}^\times_{\mathrm{K}^{ur}(p)})$$

By using the isomorphism $\hat{H}^0(\mathrm{G}_\mathrm{K}(p), \mathcal{O}^\times_{\mathrm{K}^{ur}(p)}) \simeq \varprojlim_{\mathrm{F}} \mathcal{O}^\times_\mathrm{K}/\mathrm{N}_{\mathrm{F}/\mathrm{K}}(\mathcal{O}^\times_\mathrm{F})$, where F runs through the finite extensions of K in $\mathrm{K}^{ur}(p)$, we then have

$$H_3(\mathrm{G}_\mathrm{K}(p), \mathbb{F}_p) \twoheadrightarrow \big(\varprojlim_{\mathrm{F}} \mathcal{O}^\times_\mathrm{K}/\mathrm{N}_{\mathrm{F}/\mathrm{K}}(\mathcal{O}^\times_\mathrm{F})\big)[p]. \tag{2}$$

Take now $p = 2$. Thanks to (2), we note that if -1 is not a universal norm (of a unit) in $\mathrm{K}^{ur}(2)/\mathrm{K}$, then $H^3(\mathrm{G}, \mathbb{F}_2) \neq \{0\}$, showing that $cd(\mathrm{G}_\mathrm{K}^{ur}(2)) \neq 2$. This condition about -1 is sometimes not so difficult to test, indeed:

PROPOSITION 4.2. *Let* K *be an imaginary quadratic field such that the discriminant* disc_K *of* K *is divisible by at least three odd primes* p_i*, with* $p_i \equiv 3 (\mathrm{mod}\ 4)$*,* $i = 1, 2, 3$*. Then* $cd(\mathrm{G}_\mathrm{K}^{ur}(2)) \neq 2$.

Proof. Put $\mathrm{L} = \mathrm{K}(\sqrt{p_1 p_2})$ and $\mathrm{K}_1 = \mathbb{Q}(\sqrt{p_1 p_2})$. Then the biquadratic field L is an unramified extension of K. As the extension L/K_1 is ramified at the odd prime p_3, the fundamental unit of K_1 is also the fundamental unit of $\mathcal{O}^\times_\mathrm{L}$. As $\mathrm{N}_{\mathrm{K}_1/\mathbb{Q}}\varepsilon = +1$, one concludes that -1 is not an universel norm in $\mathrm{K}^{ur}(2)/\mathrm{K}$. □

4.2 General statement

The strategy here is more or less the one used in [3] to disprove the existence of unramified embeddings. Here we apply their idea to disprove the apparence of quotients of $\mathrm{G}_\mathrm{K}^{ur}(2)$ of cohomological dimension 2 in a more systematic way, by using the bilinear form $\mathcal{B}_\mathrm{K}$.

From now on we assume that K is totally imaginary (and that $p = 2$).
Suppose given G a quotient of $\mathrm{G}_\mathrm{K}^{ur}(2)$. Then one has $H^1(\mathrm{G}) \hookrightarrow H^1(\mathrm{G}_\mathrm{K}^{ur}(2))$. Now take $x, y \in H^1(\mathrm{G}_\mathrm{K}^{ur}(2))$ coming from $H^1(\mathrm{G})$. Then, the cup-product $x \cup x \cup y \in H^3(\mathrm{G}_\mathrm{K}^{ur}(2))$ comes from $H^3(\mathrm{G})$ by the inflation map. Now, one may use the computation of Carlson-Schlank : if $x \cup x \cup y$ is non-zero in $H^3_{et}(\mathrm{X}_\mathrm{K})$, then $H^3(\mathrm{G}) \neq 0$, and then G is not of cohomological dimension 2.

REMARK 4.3. *If we want* $x \cup x \cup y \neq 0$*, then we need the cup-product* $x \cup x$ *non-trivial in* $H^2_{et}(\mathrm{X}_\mathrm{K})$*, which is equivalent to the condition that* K_x/K *can not be embedded in an unramified degree* 4 *cyclic extension of* K.

Let us recall Theorem 2 (we use the notations of Section 3):

THEOREM 4.4. *Let* $\mathrm{K}/\mathbb{Q}$ *be a totally imaginary number field. Then* $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ *has no quotient* G *of cohomological dimension* 2 *and of* 2*-rank* $d_2\mathrm{G} > \nu(\mathrm{K})$. *In particular,* $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ *has no quotient* G *of cohomological dimension* 2 *and of* 2*-rank* $d_2\mathrm{G} > d_2\mathrm{Cl}_{\mathrm{K}} - \frac{1}{2}\mathrm{rk}(\mathcal{B}_{\mathrm{K}})$.

Proof. Let G be a non-trivial uniform quotient of $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ of dimension $d > 0$. Let W be the Kummer radical of $H^1(\mathrm{G})^\vee$; here W is a subspace of the Kummer radical V of $\mathrm{K}^{ur,2}/\mathrm{K}$. As $d > \nu(\mathrm{K})$, the space W is not totally isotropic. Then, one can find $x, y \in H^1(\mathrm{G}) \subset H^1(\mathrm{X}_{\mathrm{K}})$ such that $x \cup x \cup y \in H^3_{et}(\mathrm{X}_{\mathrm{K}})$ is not zero (by Proposition 2.4). See also Remark 3.8. And thanks to the stategy developed just before, we are done for the first part ot the theorem. For the second part, one has just to note that in this case $\nu(\mathrm{K}) \leq d_2\mathrm{Cl}_{\mathrm{K}} - \frac{1}{2}\mathrm{rk}(\mathcal{B}_{\mathrm{K}})$ by Proposition 3.2. □

COROLLARY 4.5. *If* Cl_{K} *is non-degenerate, then* $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ *has no quotient* G *of cohomological dimension* 2 *and of* 2*-rank* $d_2\mathrm{G} > \frac{1}{2}d_2\mathrm{Cl}_{\mathrm{K}}$.

Proof. In this case, $\mathrm{rk}(\mathcal{B}_{\mathrm{K}}) = \mathrm{d}_2\mathrm{Cl}_{\mathrm{K}}$ □

4.3 THE IMAGINARY QUADRATIC CASE - DENSITY ESTIMATIONS

4.3.1 A FIRST DENSITY ESTIMATE

Let us give now a density estimate for imaginary quadratic fields. Recall that we denote by $\mathcal{F}^-$ the set of imaginary quadratic fields and by $\mathcal{F}_X^- := \{\mathrm{K} \in \mathcal{F}^-,\ |\mathrm{disc}_{\mathrm{K}}| \leq X\}$. Put also

$$\mathcal{D}_X^- = \{\mathrm{K} \in \mathcal{F}_X^-, \mathrm{G}_{\mathrm{K}}^{ur}(2) \text{ has no quotient G s.t. } d_2\mathrm{G} = d_2\mathrm{G}_{\mathrm{K}}^{ur}(2)\ \&\ cd(\mathrm{G}) = 2\}.$$

THEOREM 4.6 (Theorem 1). *One has:*

$$0 \leq 1 - \frac{\#\mathcal{D}_X^-}{\#\mathcal{F}_X^-} \leq C\frac{\log\log X}{\sqrt{\log X}},$$

where C *is an absolute constant.*

Proof. The proof is based on the two following things: (i) on an analytic estimate; (ii) on our strategy and on a computation of [3]. Let us start the analytic tools. For $X \geq 2$, denote by

$$\mathcal{T}_X^- = \{\mathrm{K} \in \mathcal{F}_X^-,\ \exists \text{ odd primes } p \neq q,\ pq|\mathrm{disc}_{\mathrm{K}},\ \left(\frac{p^*}{q}\right) = -1\}.$$

Remark at this point that

$$\{\mathrm{K} \in \mathcal{F}_X^-,\ \exists \text{ odd primes } p \neq q,\ p \equiv q \equiv 3 \pmod 4, pq|\mathrm{disc}_{\mathrm{K}}\} \subset \mathcal{T}_X^-;$$

indeed, by Legendre formula, $\left(\frac{p^*}{q}\right)\left(\frac{q^*}{p}\right) = -1$. Denote by $\mathcal{E}_X^-$ the complement of $\mathcal{T}_X^-$ in $\mathcal{F}_X^-$.

PROPOSITION 4.7. *The set $\mathcal{E}_X^-$ is of zero density. More precisely, one has*

$$\#\mathcal{E}_X^- = O\Big(X\frac{\log\log X}{\sqrt{\log X}}\Big).$$

Proof. Note by $\mathcal{E}_{i,X}$ the set of square-free integers $n \leq X$, having exactly i prime factors $\equiv 3 \pmod 4$, and put $\mathcal{E}_X = \mathcal{E}_{0,X} \cup \mathcal{E}_{1,X}$. Clearly, $\#\mathcal{E}_X^- = O(\#\mathcal{E}_X)$. We will use the following:

LEMMA 4.8. *Uniformly for $X \geq 2$, one has*

$$\#\mathcal{E}_{0,X} = O\Big(\frac{X}{\sqrt{\log X}}\Big).$$

Proof. Indeed, every integer $n \in \mathcal{E}_{0,X}$ is a sum of two squares. A famous result of Landau (see for example [21, Chapter 7, Theorem 7.28]) states that the number of integers $n \leq X$ which are sum of two squares is asymptotic to $C'\dfrac{X}{\sqrt{\log X}}$, for some absolute positive C'. □

We want to prove the bound

$$\mathcal{E}_{1,X} = O\Big(X\frac{\log\log X}{\sqrt{\log X}}\Big) \tag{3}$$

uniformly for $X \geq 2$, as a consequence of Lemma 4.8. Since we are searching an upper bound, we may suppose that $X = 2^\kappa$, where $\kappa > 1$ is an integer. We start from the decomposion formula

$$\#\mathcal{E}_{1,X} = \sum_{\substack{p \equiv 3 \pmod 4 \\ p \leq X/2}} \#\mathcal{E}_{0,X/p} + O(\pi(X)).$$

Put $Y = 2^t$ with $t = 1, 2, \cdots, \kappa - 1$ and split the above formula as

$$\#\mathcal{E}_{1,X} = \sum_t \sum_{Y/2 < p \leq Y} \#\mathcal{E}_{0,X/p} + O\big(\frac{X}{\log X}\big). \tag{4}$$

We deduce from Lemma 4.8 that, uniformly for $Y/2 < p \leq Y$ and $Y = 2^t$, and $0 \leq t \leq \kappa - 1$, we have the bound

$$\#\mathcal{E}_{0,X/p} = O\big(\frac{X}{Y\sqrt{\kappa - t}}\big),$$

and by Tchebychev's bound we deduce

$$\sum_{Y/2 < p \leq Y} \#\mathcal{E}_{0,X/p} = O\big(\frac{X}{t\sqrt{\kappa - t}}\big).$$

Inserting this into (4), we obtain

$$\#\mathcal{E}_{1,X} = O\big(X \sum_{1\le t\le \kappa-1} \frac{1}{t\sqrt{\kappa-t}}\big).$$

To evaluate the sum over t, we split it according to $1 \le t < \kappa/\log\kappa$ and $\kappa/\log\kappa \le t \le \kappa - 1$ leading to

$$\sum_{1\le t\le \kappa-1} \frac{1}{t\sqrt{\kappa-t}} = O\big(\frac{1}{\sqrt{\kappa}} \sum_{1\le t\le \kappa} \frac{1}{t} + \frac{\log\kappa}{\kappa} \sum_{1\le u\le \kappa} \frac{1}{\sqrt{u}}\big),$$

which gives (3), since $\kappa = O(\log X)$. This completes the proof of Proposition 4.7. □

Now let us give the tool from étale cohomology.

LEMMA 4.9. *Let* $\mathrm{K}/\mathbb{Q}$ *be an imaginary quadratic field. Suppose that there exist two distinct odd prime numbers* p *and* q *such that* $pq|\mathrm{disc_K}$ *and* $\left(\frac{p^*}{q}\right) = -1$. *Then there exist* $x, y \in H^1(\mathrm{G}_\mathrm{K}^{ur}(2))$ *such that* $x \cup x \cup y \neq 0 \in H^3(\mathrm{G}_\mathrm{K}^{ur}(2))$.

Proof. Take $\mathrm{K}_x = \mathrm{K}(\sqrt{p^*})$ and $\mathrm{K}_y = \mathrm{K}(\sqrt{q^*})$. Then, by Proposition 2.4, the cup-product $x \cup x \cup y \in H^3_{et}(X)$ is not trivial, and then non-trivial in $H^3(\mathrm{G}_\mathrm{K}^{ur}(2))$. □

We now finish the proof of Theorem 4.6. Take $\mathrm{K} \in \mathcal{T}_\mathrm{K}^-$, and let us consider a quotient $\mathrm{G}_\mathrm{K}^{ur}(2) \twoheadrightarrow \mathrm{G}$ such that $H^1(\mathrm{G}_\mathrm{K}^{ur}(2)) \simeq H^1(\mathrm{G})$. But by Lemma 4.9, there exists $x, y \in H^1(\mathrm{G}_\mathrm{K}(2))$ such that $x \cup x \cup y \neq 0 \in H^3_{et}(\mathrm{X_K})$, and then not trivial in $H^3(\mathrm{G}_\mathrm{K}^{ur}(2))$ and finally not trivial in $H^3(\mathrm{G})$. Hence, $\mathcal{T}_X^- \subset \mathcal{D}_X^-$, and $\#\mathcal{F}_X^- - \#\mathcal{D}_X^- \le \mathcal{E}_X^-$; to conclude, let us recall the well-known estimate: $\#\mathcal{F}_X^- = \frac{3}{\pi^2}X + O(\sqrt{X})$. □

Now, we would like to extend this density estimate.

4.3.2 THE CONTEXT

Let us consider an imaginary quadratic field $\mathrm{K} = \mathbb{Q}(\sqrt{D})$, $D \in \mathbb{Z}_{<0}$ square-free. Let $p_1, \cdots, p_{k+1}$ be the *odd* prime numbers dividing D (we assume $D \neq -1, -2$). Let us write the discriminant $\mathrm{disc_K}$ of K as: $\mathrm{disc_K} = p_0^* \cdot p_1^* \cdots p_{k+1}^*$, where $p_0^* \in \{1, -4, \pm 8\}$. Denote by n the 2-rank of $\mathrm{Cl_K}$:

- if 2 is unramified in $\mathrm{K}/\mathbb{Q}$, *i.e.* $p_0^* = 1$, then $n = k$ and $V =< p_1^*, \cdots, p_k^* > (\mathrm{K}^\times)^2 \subset \mathrm{K}^\times$ is the Kummer radical of $\mathrm{K}^{ur,2}/\mathrm{K}$;
- is 2 is ramified in $\mathrm{K}/\mathbb{Q}$, *i.e.* $p_0^* = -4$ or ± 8, then $n = k + 1$ and $V =< p_1^*, \cdots, p_{k+1}^* > (\mathrm{K}^\times)^2 \subset \mathrm{K}^\times$ is the Kummer radical of $\mathrm{K}^{ur,2}/\mathrm{K}$.

We denote by $\mathcal{F} = \{p_1^*, \cdots, p_n^*\}$ the $\mathbb{F}_2$-basis of V, where here $n = k$ or $k+1$.

LEMMA 4.10. *(i) For $p^* \neq q^* \in \mathcal{F}$, one has: $\mathcal{B}_{\mathrm{K}}(p^*, q^*) = 0$ if and only if, $\left(\frac{p^*}{q}\right) = 1$.*
(ii) For $p|D$, put $D_p := D/p^*$. Then for $p^* \in \mathcal{F}$, one has: $\mathcal{B}_{\mathrm{K}}(p^*, p^*) := \left(\frac{D_p}{p}\right)$.

Proof. Obvious. □

Hence the matrix of the bilinear form $\mathcal{B}_{\mathrm{K}}$ in the basis $\mathcal{F}$ is a square $n \times n$ Rédei-matrix type $\mathrm{M}_{\mathrm{K}} = (m_{i,j})_{i,j}$, where

$$m_{i,j} = \begin{cases} \left(\frac{p_i^*}{p_j}\right) & \text{if } i \neq j, \\ \left(\frac{D_{p_i}}{p_i}\right) & \text{if } i = j. \end{cases}$$

Here as usual, one uses the additive notation (the 1's are replaced by 0's and the -1's by 1's).

EXAMPLE 4.11. *Take $\mathrm{K} = \mathbb{Q}(\sqrt{-4 \cdot 3 \cdot 5 \cdot 7 \cdot 13})$. This quadratic field has a root discriminant $|\mathrm{disc}_{\mathrm{K}}|^{1/2} \approx 73.89$, and the 2-rank of $\mathrm{G}_{\mathrm{K}}(2)$ is actually 4 but we don't know if $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ is finite or not; see the recent works of Boston and Wang [2]. Take $\mathcal{F} = \{-3, -5, -7, -13\}$. Then the Gram matrix of $\mathcal{B}_{\mathrm{K}}$ in $\mathcal{F}$ is:*

$$\mathrm{M}_{\mathrm{K}} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Hence $\mathrm{rk}(\mathcal{B}_{\mathrm{K}}) = 3$ and $\nu(\mathrm{K}) \leq 4 - \frac{3}{2} = 2.5$. By Theorem 5.1, one concludes that $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ has no quotient G of cohomological dimension 2 and 2-rank $d_2\mathrm{G} \geq 3$. By Corollay 3.5, remark that here one has $\nu(\mathrm{K}) = 2$.

4.3.3 SYMMETRIC BILINEAR FORMS. EXAMPLES

Let us conserve the context of the previous section 4.3.2. Then, thanks to the quadratic reciprocity law, one gets:

PROPOSITION 4.12. *The bilinear form $\mathcal{B}_{\mathrm{K}} : V \times V \to \mathbb{F}_2$ is symmetric, if and only if, there is at most one prime $p \equiv 3(\mod 4)$ dividing D.*

Proof. Obvious. □

Let us give some examples.

EXAMPLE 4.13. *Take $k+1$ prime numbers $p_1, \cdots, p_{k+1}$, such that*

- $p_1 \equiv \cdots p_k \equiv 1 (\mathrm{mod}\ 4)$ *and* $p_{k+1} \equiv 3 (\mathrm{mod}\ 4)$*;*
- *for* $1 \leq i < j \leq k$, $\left(\dfrac{p_i}{p_j}\right) = 1$*;*
- *for* $i = 1, \cdots, k$, $\left(\dfrac{p_i}{p_{k+1}}\right) = -1$

Put $\mathrm{K} = \mathbb{Q}(\sqrt{-p_1 \cdots p_{k+1}})$*. In this case the matrix of the bilinear form* $\mathcal{B}_\mathrm{K}$ *in the basis* $(p_i)_{1 \leq k}$ *is the identity matrix of dimension* $k \times k$ *and,* $\nu(\mathrm{K}) = \lfloor \frac{k}{2} \rfloor$*. Hence,* $\mathrm{G}_\mathrm{K}^{ur}(2)$ *has no quotient* G *of cohomological dimension* 2 *and of* 2*-rank* $d_2\mathrm{G} \geq \lfloor \frac{k}{2} \rfloor + 1$*.*

EXAMPLE 4.14. *Take* $2m+1$ *prime numbers* $p_1, \cdots, p_{2m+1}$*, such that*

- $p_1 \equiv \cdots p_{2m} \equiv 1 (\mathrm{mod}\ 4)$ *and* $p_{2m+1} \equiv 3 (\mathrm{mod}\ 4)$*;*
- $\left(\dfrac{p_1}{p_2}\right) = \left(\dfrac{p_3}{p_4}\right) = \cdots = \left(\dfrac{p_{2m-1}}{p_{2m}}\right) = -1$*;*
- *for the other indices* $1 \leq i < j \leq 2m$, $\left(\dfrac{p_i}{p_j}\right) = 1$*;*
- *for* $i = 1, \cdots, 2m$, $\left(\dfrac{p_i}{p_{2m+1}}\right) = -1$

Put $\mathrm{K} = \mathbb{Q}(\sqrt{-p_1 \cdots p_{2m+1}})$*. In this case the bilinear form* $\mathcal{B}_\mathrm{K}$ *is non-degenerate and alternating, then isometric to* $\overbrace{\mathcal{H}(0) \perp \cdots \perp \mathcal{H}(0)}^{m}$*. Hence,* $\nu(\mathrm{K}) = m$*, and* $\mathrm{G}_\mathrm{K}^{ur}(2)$ *has no quotient of cohomological dimension* 2 *and of* 2*-rank at least* $m+1$*.*

4.3.4 RELATION WITH THE 4-RANK OF THE CLASS GROUP

The study of the 4-rank of the class group of quadratic number fields started with the work of Rédei [26] (see also [27]). Since, then many authors have contribued to its extensions, generalizations and applications. Let us cite an article of Lemmermeyer [20] where one can find a large literature about the question. See also a paper of Stevenhagen [32], and the work of Gerth [10] and Fouvry-Klüners [8] concerning the density question.
Let us conserve the context and the notations of the section 4.3.2: here $\mathrm{K} = \mathbb{Q}(\sqrt{D})$ is an imaginary quadratic field of discrimant disc_K, $D \in \mathbb{Z}_{<0}$ square-free. Denote by $\{q_1, \cdots q_{n+1}\}$ the set of prime numbers that ramify in $\mathrm{K}/\mathbb{Q}$; $d_2\mathrm{Cl}_\mathrm{K} = n$. Here we can take $q_i = p_i$ for $1 \leq i \leq n$, and $q_n = p_{k+1}$ or $q_n = 2$ following the ramification at 2. Then, consider the Rédei matrix $\mathrm{M}'_\mathrm{K} = (m_{i,j})_{i,j}$ of size $(n+1) \times (n+1)$ with coefficients in $\mathbb{F}_2$, where

$$m_{i,j} = \begin{cases} \left(\dfrac{q_i^*}{q_j}\right) & \text{if } i \neq j, \\ \left(\dfrac{D_{q_i}}{q_i}\right) & \text{if } i = j. \end{cases}$$

It is not difficult to see that the sum of the rows is zero, hence the rank of M'_{K} is smaller than n.

THEOREM 4.15 (Rédei). *Let* K *be an imaginary quadratic number field. Then* $\mathrm{R}_{\mathrm{K},4} = d_2\mathrm{Cl}_{\mathrm{K}} - \mathrm{rk}(\mathrm{M}'_{\mathrm{K}})$.

REMARK 4.16. *The strategy of Rédei is to construct for every couple* (D_1, D_2) *"of second kind", a degree* 4 *cyclic unramified extension of* K. *Here to be of second kind means that* $\mathrm{disc}_{\mathrm{K}} = D_1D_2$, *where* D_i *are fundamental discriminants such that* $\left(\frac{D_1}{p_2}\right) = \left(\frac{D_2}{p_1}\right) = 1$, *for every prime* $p_i|D_i$, $i = 1, 2$. *And clearly, this condition corresponds exactly to the existence of orthogonal subspaces* W_i *of the Kummer radical* V, $i = 1, 2$, *generated by the* p_i^*, *for all* $p_i|D_i$: $\mathcal{B}_{\mathrm{K}}(W_1, W_2) = \mathcal{B}_{\mathrm{K}}(W_2, W_1) = \{0\}$. *Such orthogonal subspaces allow us to construct totally isotropic subspaces. And then, the larger the* 4*-rank of* Cl_{K}, *the larger* $\nu(\mathrm{K})$ *must be (as noted by Proposition 3.2 and 3.13).*

Consider now the matrix $\mathrm{M}''_{\mathrm{K}}$ obtained from M'_{K} after deleting the last row. Remark here that M_{K} (which is the Gram matrix of $\mathcal{B}_{\mathrm{K}}$) is a submatrix of the Rédei matrix $\mathrm{M}''_{\mathrm{K}}$:

$$\mathrm{M}''_{\mathrm{K}} = \left(\begin{array}{|c|c} \hline \mathrm{M}_{\mathrm{K}} & \begin{array}{c} * \\ \vdots \\ * \end{array} \\ \hline \end{array} \right)$$

Hence,

$$\mathrm{rk}(\mathcal{B}_{\mathrm{K}}) + 1 \geq \mathrm{rk}(\mathrm{M}'_{\mathrm{K}}) = \mathrm{rk}(\mathrm{M}''_{\mathrm{K}}) \geq \mathrm{rk}(\mathcal{B}_{\mathrm{K}}).$$

Remark that in example 4.11, $\mathrm{rk}(\mathcal{B}_{\mathrm{K}}) = 3$ and $\mathrm{rk}(\mathrm{M}'_{\mathrm{K}}) = 4$. But sometimes one has $\mathrm{rk}(\mathrm{M}'_{\mathrm{K}}) = \mathrm{rk}(\mathcal{B}_{\mathrm{k}})$, as for example:

(A): when: $p_0 = 1$ (the set of primes $p_i \equiv 3 (\mathrm{mod}\ 4)$ is odd);

(B): or, when $\mathcal{B}_{\mathrm{K}}$ is non-degenerate.

For situation (A), it suffices to note that the sum of the columns is zero (thanks to the properties of the Legendre symbol).

4.3.5

From now on we follow the work of Gerth [10]. Recall that we denote by $\mathcal{F}^-$ the set of imaginary quadratic number fields, and for $0 \leq r \leq n$ and $X \geq 0$,

$$\mathcal{F}^-_X = \big\{\mathrm{K} \in \mathcal{F}^-,\ |\mathrm{disc}_{\mathrm{K}}| \leq X\big\},$$

$$\mathcal{F}_{n,X} = \big\{\mathrm{K} \in \mathcal{F}^-_X,\ d_2\mathrm{Cl}_{\mathrm{K}} = n\big\},\quad \mathcal{F}_{n,r,X} = \big\{\mathrm{K} \in \mathcal{F}_{n,X},\ \mathrm{R}_{\mathrm{K},4} = r\big\}.$$

Denote also

$$\mathrm{A}_X = \big\{\mathrm{K} \in \mathcal{F}^-_X,\ \text{satisfying } (A)\big\},$$

$$\mathrm{A}_{n,X} = \big\{\mathrm{K} \in \mathrm{A}_X,\ d_2\mathrm{Cl}_{\mathrm{K}} = n\big\},\quad \mathrm{A}_{n,r,X} = \big\{\mathrm{K} \in \mathrm{A}_{n,X},\ \mathrm{R}_{\mathrm{K},4} = r\big\}.$$

One has the following density theorem due to Gerth:

THEOREM 4.17 (Gerth [10]). *The limits* $\lim_{X\to\infty} \frac{|\mathrm{A}_{n,r,X}|}{|\mathrm{A}_{n,X}|}$ *and* $\lim_{X\to\infty} \frac{|\mathcal{F}_{n,r,X}|}{|\mathcal{F}_{n,X}|}$ *exist and are equal. Denote by* $d_{n,r}$ *this quantity. Then* $d_{n,r}$ *can be estimated and,*

$$d_{\infty,r} := \lim_{n\to\infty} d_{n,r} = \frac{2^{-r^2}\prod_{k=1}^{\infty}(1-2^{-k})}{\prod_{k=1}^{r}(1-2^{-k})}.$$

Recall also the following quantities introduced at the beginning of our work:

$$\mathcal{D}_{n,X}^{(d)} := \{\mathrm{K}\in\mathcal{F}_{n,X},\ \mathrm{G}_{\mathrm{K}}^{ur}(2) \text{ has no quotient G s.t. } cd(\mathrm{G})=2 \ \&\ d_2(\mathrm{G})\geq d\},$$

and consider the limit:

$$\mathcal{D}_n^{(d)} := \liminf_{X\to+\infty} \frac{\#\mathcal{D}_{n,X}^{(d)}}{\#\mathcal{F}_{n,X}}.$$

After combining all our observations, we obtain (see also Corollary *i*):

COROLLARY 4.18. *For* $\frac{n+1}{2}\leq d\leq n$*, one has*

$$\mathcal{D}_n^{(d)} \geq d_{n,0}+d_{n,1}+\cdots+d_{n,2d-n-1}.$$

In particular:

(*i*) $\mathcal{D}_5^{(3)}\geq .33129$, $\mathcal{D}_5^{(4)}\geq .99062$, $\mathcal{D}_5^{(5)}\geq .99999$;

(*ii*) $\mathcal{D}_6^{(4)}\geq .86718$, $\mathcal{D}_6^{(5)}\geq .99925$, $\mathcal{D}_6^{(6)}\geq 1-5.2\cdot 10^{-8}$;

Moreover, for large n, $\mathcal{D}_n^{(2+n/2)}\geq .99995$.

Proof. As noted by Gerth in [10], the dominating set in the density computation is the set $\mathrm{A}_{n,X}$ of imaginary quadratic number fields $\mathrm{K}=\mathbb{Q}(\sqrt{D})$ satisfying (A). But for K in $\mathrm{A}_{n,X}$, one has $\mathrm{rk}(\mathcal{B}_{\mathrm{K}})=\mathrm{rk}(\mathrm{M}_{\mathrm{K}})=n-\mathrm{R}_{\mathrm{K},4}$. Hence for $\mathrm{K}\in\mathrm{A}_{n,X,r}$, by Proposition 3.2

$$\nu(\mathrm{K})\leq n-\frac{1}{2}\big(n-\mathrm{R}_{\mathrm{K},4}\big)=\frac{1}{2}\big(n+\mathrm{R}_{\mathrm{K},4}\big).$$

Hence $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ has no quotient G of cohomological dimension 2 and 2-rank d when $\mathrm{R}_{\mathrm{K},4}<2d-n$. In particular, when $2d-n\geq 1$, one has

$$\mathcal{D}_n^{(d)} \geq d_{n,0}+d_{n,1}+\cdots+d_{n,2d-n-1}.$$

Now one uses the estimates of Gerth in [10], to obtain:

(*i*) $\mathcal{D}_5^{(3)}\geq d_{5,0}\approx .33129$, $\mathcal{D}_5^{(4)}\geq d_{5,0}+d_{5,1}+d_{5,2}\approx .99062$, $\mathcal{D}_5^{(5)}\geq d_{5,0}+d_{5,1}+d_{5,2}+d_{5,3}+d_{5,4}\approx .99999$,

(*ii*) $\mathcal{D}_6^{(4)}\geq d_{6,0}+d_{6,1}\approx .86718$, $\mathcal{D}_6^{(5)}\geq d_{6,0}+d_{6,1}+d_{6,2}+d_{6,3}\approx .99925$, $\mathcal{D}_6^{(6)}\geq 1-d_{6,6}\approx 1-5.2\cdot 10^{-8}$,

For the last point, remark that $\mathcal{D}_n^{(2+n/2)} \geq d_{n,0} + d_{n,1} + d_{n,2}$, and use the fact that $\lim_{n\to\infty} d_{n,r} = d_{\infty,r}$. □

In the spirit of the Cohen-Lenstra heuristics, the work of Gerth has been improved by Fouvry-Klüners [7], [8]. This work allows us to give a more general density estimation as announced in the Introduction. Recall

$$\mathcal{D}_X^{[i]} := \{\mathrm{K} \in \mathcal{F}_X,\ \mathrm{G}_\mathrm{K}^{ur}(2) \text{ has no quotient G s.t. } cd(\mathrm{G}) = 2 \ \&\ d_2\mathrm{G} \geq i + \frac{d_2\mathrm{Cl}_\mathrm{K}}{2}\}$$

and

$$\mathcal{D}^{[i]} := \liminf_{X\to+\infty} \frac{\#\mathcal{D}_X^{[i]}}{\#\mathcal{F}_X^-}.$$

Our work allows us to obtain (see Corollary ii):

COROLLARY 4.19. *For $i \geq 1$, one has:*

$$\mathcal{D}^{[i]} \geq d_{\infty,0} + d_{\infty,1} + \cdots + d_{\infty,2i-2}.$$

In particular,

$$\mathcal{D}^{[1]} \geq .28878, \quad \mathcal{D}^{[2]} \geq .99471, \text{ and } \mathcal{D}^{[3]} \geq 1 - 9.7 \cdot 10^{-8}.$$

Proof. By Fouvry-Klüners [8], the density of imaginary quadratic fields for which $\mathrm{R}_{\mathrm{K},4} = r$, is equal to $d_{\infty,r}$. Recall that for $\mathrm{K} \in \mathcal{F}^-$, one has $\mathrm{rk}(\mathcal{B}_\mathrm{K}) \geq \mathrm{rk}(\mathrm{M}'_\mathrm{K}) - 1$. Then thanks to Proposition 3.2 and Theorem 4.15, we get

$$\nu(\mathrm{K}) \leq \frac{1}{2} d_2\mathrm{Cl}_\mathrm{K} + \frac{1}{2} + \frac{1}{2}\mathrm{R}_{\mathrm{K},4}.$$

Putting this fact together with Theorem 4.4, we obtain that $\mathrm{G}_\mathrm{K}^{ur}(2)$ has no quotient G of cohomological dimension 2 and 2-rank $d_2\mathrm{G} > \frac{1}{2}d_2\mathrm{Cl}_\mathrm{K} + \frac{1}{2} + \frac{1}{2}\mathrm{R}_{\mathrm{K},4}$. Then for $i \geq 1$, the proportion of the fields K in $\mathcal{D}^{[i]}$ is at least the proportion of $\mathrm{K} \in \mathcal{F}^-$ for which $\mathrm{R}_{\mathrm{K},4} < 2i - 1$, hence at least $d_{\infty,0} + d_{\infty,1} + \cdots + d_{\infty,2i-2}$ by [8]. To conclude:

$$\mathcal{D}^{[1]} \geq d_{\infty,0} \approx .28878$$

$$\mathcal{D}^{[2]} \geq d_{\infty,0} + d_{\infty,1} + d_{\infty,2} \approx .99471$$

$$\mathcal{D}^{[3]} \geq d_{\infty,0} + d_{\infty,1} + d_{\infty,2} + d_{\infty,3} + d_{\infty,4} \approx 1 - 9.7 \cdot 10^{-8}.$$

□

5 On unramified 2-adic analytic extensions

5.1 General result

The unramified Fontaine-Mazur at $p = 2$ has a first evidence just by looking at the 2-part of the class group and the matrix of the bilinear form $\mathcal{B}_\mathrm{K}$. Indeed, one has very easily:

THEOREM 5.1 (Theorem 3). *Let* $\mathrm{K}/\mathbb{Q}$ *be a number field.*

(*i*) *Suppose that the* 4*-rank of the class group of* K *is at most* 2*. Then Conjecture 1.1 holds for* K *(at* $p = 2$*).*

(*ii*) *Suppose* K *is totally imaginary. Then* $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ *has no uniform quotient of dimension* $d > d_2\mathrm{Cl}_{\mathrm{K}} - \mathrm{rk}(\mathcal{B}_{\mathrm{K}})$*. In particular, Conjecture 1.1 holds for* K *(and* $p = 2$*) when* $\mathrm{rk}(\mathcal{B}_{\mathrm{K}}) \geq \mathrm{d}_2\mathrm{Cl}_{\mathrm{K}} - 2$*.*

Proof. (*i*) Let G be a non-trivial uniform quotient of $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ of dimension d. By class field theory, the group G is FAb, and then by Corollary 2.12 the dimension of G must verify $d \geq 3$. Then by Proposition 2.15, $\mathrm{G}^{ab} \twoheadrightarrow (\mathbb{Z}/4\mathbb{Z})^3$, which implies $\mathrm{R}_{\mathrm{K},4} \geq 3$.
(*ii*) If G is a uniform quotient of $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ of dimension d then $\mathrm{R}_{\mathrm{K},4} \geq d$, but by Proposition 3.13, $\mathrm{R}_{\mathrm{K},4} \leq d_2\mathrm{Cl}_{\mathrm{K}} - \mathrm{rk}(\mathcal{B}_{\mathrm{K}})$. For the second part, recall that as G must be FAb then $d \geq 3$. □

REMARK 5.2. *One of the main draw backs of the bilinear form* $\mathcal{B}_{\mathrm{K}}$ *is the appearance of totally isotropic subspaces (following Proposition 3.9 and Proposition 3.10). Here is a situation where such phenomena do not occur. Take a CM-extension* K/k *such that*

(*i*) *the* 2*-rank of the class group of* k *in the narrow sense is odd and* $\mu_{\mathrm{K},2} = \{\pm 1\}$*,*

(*ii*) *the extension* K/k *is unramified at every prime* $\mathfrak{p}|2$*.*

Then there is no totally isotropic subspaces coming from units (see Proposition 3.9).

As consequence of Theorem 5.1, one can give some density estimates following the work of Fouvry-Klueners. Recall also the following quantities introduced at the beginning of our work: for $n, d, X \geq 0$, denote by

$$\mathcal{F}_X^{\pm} := \{\mathrm{K} \in \mathcal{F}^{\pm},\ |\mathrm{disc}_{\mathrm{K}}| \leq X\},$$

$$\mathrm{FM}_X^{\pm} := \{\mathrm{K} \in \mathcal{F}_X^{\pm}, \text{Conjecture 1.1 holds for K}\},$$

and put

$$\mathrm{FM}^{\pm} := \liminf_{X \to +\infty} \frac{\#\mathrm{FM}_X^{\pm}}{\#\mathcal{F}_X^{\pm}}.$$

This work allows us to give a more general density estimation as announced in the Introduction.

COROLLARY 5.3. *One has*

$$\mathrm{FM}^{-} \geq d_{\infty,0} + d_{\infty,1} + d_{\infty,2} \approx .99471, \text{ and } \mathrm{FM}^{+} \geq .99929.$$

Proof. It is a consequence of Theorem 5.1, and the work of Fouvry-Klueners [8]. See also [10] for the computation of the densities. □

5.2 CLIMBING IN $\mathrm{G}_{\mathrm{K}}^{ur}(2)$

Suppose that $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ has a non-trivial uniform quotient G of dimension $d > 1$. Let L/K be the subextension of $\mathrm{K}^{ur}(2)/\mathrm{K}$ with Galois group G. Consider the p-central decending series $(\mathrm{G}_i)_i$ of G, and for $i \geq 1$, denote by K_i the fixed field by the group G_i. Hence, $\mathrm{K}_2 \subset \mathrm{K}^{2,el}$. By Proposition 2.15,

LEMMA 5.4. *One has:* $\mathrm{Cl}_{\mathrm{K}_2} \twoheadrightarrow (\mathbb{Z}/8\mathbb{Z})^d$.

In particular, the 8-rank $\mathrm{R}_{\mathrm{K}_2,8}$ of $\mathrm{Cl}_{\mathrm{K}_2}$ should be at least d. In fact, one can say a little bit more. Indeed, by Chebotarev's density theorem there exist prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_d$ of $\mathcal{O}_{\mathrm{K}}$ such that the Frobenius g_i of $\mathfrak{p}_i$ (with an obvious abuse of notation) in L/K generate G. As G is uniform, the elements $g_1^{2^{i-1}}, \ldots, g_d^{2^{i-1}}$ generate the subgroups G_i, for all $i \geq 1$. For $i = 1, \cdots, d$, let us choose now $\mathfrak{P}_i \subset \mathcal{O}_{\mathrm{K}_2}$ a prime ideal of K_2 above $\mathfrak{p}_i$. Then, as $\mathfrak{p}_i$ does not totally split in K_2/K, and thanks to the property of the global Frobenius, we get that the Frobenius of the primes $\mathfrak{P}_i$ in L/K_2 (or a $\mathrm{Gal}(\mathrm{K}_2/\mathrm{K})$-conjugate of it) is equal to g_i^2. These Frobenius elements generate the Galois group $\mathrm{Gal}(\mathrm{L}/\mathrm{K}_2)$ which is of p-rank d, and in particular, the class of $\mathfrak{P}_i$ in $\mathrm{Cl}_{\mathrm{K}_2}$ is of order at least 8 by Lemma 5.4. This observation is then a new obstruction to test Conjecture 1.1. Let us explain it with an example.

EXAMPLE 5.5. *Take* $\mathrm{K} = \mathbb{Q}(\sqrt{-2 \cdot 31 \cdot 41 \cdot 113})$. *Here* $\mathrm{Cl}_{\mathrm{K}} \simeq (\mathbb{Z}/4\mathbb{Z})^3$. *The* 2*-class group* Cl_{K} *of* K *is generated by the classes of the prime ideals* $\mathfrak{p}_{29}$, $\mathfrak{p}_{823}$, *and* $\mathfrak{p}_{211}$*: by Burnside's lemma the Frobenius of these elements generate* $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ *(and then every* 2*-adic analytic quotient of* $\mathrm{G}_{\mathrm{K}}^{ur}(2)$*). Note that here* $\mathrm{K}_2 = \mathrm{K}(\sqrt{-31}, \sqrt{41}, \sqrt{113})$, *and* $\mathrm{Cl}_{\mathrm{K}_2} \simeq (\mathbb{Z}/16\mathbb{Z})^3 \times (\mathbb{Z}/8\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^4$. *One can also verify that, in* $\mathrm{Cl}_{\mathrm{K}_2}$, *the class of* $\mathfrak{P}_{29}$ *is of order* 16, *the class of* $\mathfrak{P}_{823}$ *is of order* 16, *and the class of* $\mathfrak{P}_{211}$ *is of order* 4. *Hence, thanks to the prime number* 211, *Conjecture 1.1 holds for* K.

To finish, let us look at the family of imaginary quadratic fields K for which $\mathrm{Cl}_{\mathrm{K}} \simeq (\mathbb{Z}/4\mathbb{Z})^3$. For $X \geq 0$, denote by

$$\mathcal{N}_X = \{\mathrm{K} \in \mathcal{F}_X^-, \mathrm{Cl}_{\mathrm{K}} \simeq (\mathbb{Z}/4\mathbb{Z})^3\}.$$

By a result of Koch (see Hajir [13]), one knows that for each $\mathrm{K} \in \mathcal{N}_X$, the pro-2 group $\mathrm{G}_{\mathrm{K}}^{ur}(2)$ is infinite. Let us see the different tests for Conjecture 1.1. Denote by F the unramified 2-elementary maximal extension of K.

(*i*) First, let us see the criteria concerning the 8-rank of Cl_{F}. When $X = 25 \cdot 10^6$, we find $\#\mathcal{N}_X = 459$, and 7 number fields in $\mathcal{N}_X$ are such that $\mathrm{R}_{\mathrm{F},8} \leq 2$ (in fact $= 2$), where $\mathrm{R}_{\mathrm{F},8}$ denotes the 8-rank of the class group of F. Here is the list of these fields: $|\mathrm{disc}_{\mathrm{K}}| \in \{9384952, 11577476, 13478584, 14524408, 17765944, 20167563, 21799304\}$.
Then, for these number fields, Conjecture 1.1 holds.

(*ii*) Now we will test the condition implying the Frobenius. First, remark that one should exclude quickly some number fields. Let us be more precise. Take a

set of generators $\{H_1, \cdots, H_r\}$ of $\mathrm{Cl}_\mathrm{F}[4]$. One can assume that for $i = 1, \cdots, s$, the elements H_i are not in $(\mathrm{Cl}_\mathrm{F})^2$, and for $i = s+1, \cdots, r$, the elements H_i are in $(\mathrm{Cl}_\mathrm{F})^2$. For $i = 1, \cdots, r$, put $h_i = \mathrm{N}_{\mathrm{F}/\mathrm{K}} H_i$. Let us make an easy observation:

Proposition 5.6. *Suppose that there exists a prime ideal $\mathfrak{p} \in \mathcal{O}_\mathrm{K}$ such that $cl_\mathrm{K}(\mathfrak{p}) \in \mathrm{Cl}_\mathrm{K} - (\mathrm{Cl}_\mathrm{K})^2$ and $cl_\mathrm{F}(\mathfrak{P}) \in \mathrm{Cl}_\mathrm{F}[4]$, where $\mathfrak{P}|\mathfrak{p}$, $\mathfrak{P} \subset \mathcal{O}_\mathrm{F}$. Then there exists $i_0 \in \{1, \cdots, s\}$ such that $h_{i_0} \neq 1$.*

Proof. It is a consequence of the fact that $\mathrm{N}_{\mathrm{F}/\mathrm{K}}\mathrm{Cl}_\mathrm{F} = (\mathrm{Cl}_\mathrm{K})^2$. □

Hence, the criteria above the Frobenius will give nothing when the elements $h_1, \cdots, h_s$ are all trivial in Cl_K. And this condition is very easy to test thanks to GP-Pari. As before, take $X = 25 \cdot 10^6$; in $\mathcal{N}_X$, we find 37 number fields (out of 459), for which we are guaranteed that the criteria with the Frobenius will give nothing at the stage F.

For the rest, take $X = 10^7$; one has $|\mathcal{N}_X| = 120$. Now, we use the strategy developped before. For every class h of $\mathrm{Cl}_\mathrm{K}/\mathrm{Cl}_\mathrm{K}^2$, take a prime ideal $\mathfrak{p} \subset \mathcal{O}_\mathrm{K}$ that corresponds to h (typically the prime having the smallest norm). Then, we look at the order the Frobenius of $\mathfrak{P}|\mathfrak{p}$ in Cl_F. If this order is less than 4, then Conjecture 1.1 holds. For 86 of these number fields, the computations finish, and for 10 of these fields, the strategy concerning the Frobenius holds; here is the list of these fields (with the prime):

$$(1148984, \mathfrak{p}_{211}), (1316755, \mathfrak{p}_{109}), (1466643, \mathfrak{p}_{1721}), (1934859, \mathfrak{p}_{127}),$$

$$(1972191, \mathfrak{p}_{197}), (2585464, \mathfrak{p}_{43}), (3388855, \mathfrak{p}_{151}), (4200655, \mathfrak{p}_{1303}),$$

$$(7089476, \mathfrak{p}_{953}), (8139027, \mathfrak{p}_{1181}).$$

Remark 5.7. *It woud be interesting to develop in a systematic way the test implying the Frobenius elements. For example, by studying the action of* $\mathrm{Gal}(\mathrm{F}/\mathrm{K})$ *on* Cl_F.

References

[1] F. M. Bleher, T. Chinburg, R. Greenberg, M. Kakde, G. Pappas, M. J. Taylor, *Unramified arithmetic Chern-Simons invariants*, arxiv 2017, https://arxiv.org/abs/1705.07110.

[2] N. Boston and J. Wang, *The 2-class tower of* $\mathbb{Q}(\sqrt{-5460})$, arxiv 2017, https://arxiv.org/pdf/1710.10681.pdf.

[3] M. Carlson and T.M. Schlank, *The unramified inverse Galois problem and cohomology rings of totally imaginary number fields*, arxiv 2016, http://front.math.ucdavis.edu/1612.01766.

[4] J.D. Dixon, M.P.F. Du Sautoy, A. Mann and D. Segal, *Analytic pro-p-groups*, Cambridge studies in advances mathematics 61, Cambridge University Press, 1999.

[5] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, In Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995.

[6] P. Forré, *Strongly free sequences and pro-p-groups of cohomological dimension* 2, J. reine u. angew. Math. 658 (2011), 173-192.

[7] E. Fouvry and J. Klüners, *Cohen-Lenstra heuristics of quadratic number fields*, Algorithmic number theory, 40–55, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 2006.

[8] E. Fouvry and J. Klüners, *On the* 4*-rank of the class groups of quadratic number fields*, Invent. Math. 167 (3) (2007), 455-513.

[9] J. Gärtner, Mild pro-p-groups with trivial cup-product, Ph.D. thesis, Heidelberg, 2011.

[10] F. Gerth III, *The* 4*-class ranks of quadratic number fields*, Invent. Math. 77 (1984), 489-515.

[11] G. Gras, *Class Field Theory*, SMM, Springer, 2003.

[12] Haberland, Galois cohomology of algebraic number fields, Deutscher Verl. der Wiss., Berlin, 1978.

[13] F. Hajir, *On a theorem of Koch*, Pacific J. of Math. 176, 1 (1996), 15-18.

[14] F. Hajir and C. Maire, *On the invariant factors of class groups in towers of number fields*, Canadian J. Math. 70 (2018), 142-172.

[15] M. Knebusch, Specialization of Quadratic and Symmetric Bilinear Forms, Algebra and Applications 11, Springer, 2010.

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

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

[18] J. Labute and J. Mináč, *Mild pro-*2*-groups and* 2*-extensions of* $\mathbb{Q}$ *with restricted ramification*, J. Algebra 332 (2011), 136-158.

[19] M. Lazard, *Groupes analytiques p-adiques*, IHES, Publ. Math. 26 (1965), 389-603.

[20] F. Lemmermeyer, *Higher Descent on Pell Conics I. From Legendre to Selmer*, 2003, https://arxiv.org/pdf/math/0311309.pdf

[21] W.J. LeVeque, Topics in Number Theory, Volume II, Addison-Wesley Publishing Company, Inc, 1956.

[22] A. Lubotzky and A. Mann, *Powerful p-groups II. p-adic Analytic Groups*, J. of Algebra 105 (1987), 506-515.

[23] B. Mazur, *Notes on étale cohomology of number fields*, Annales Sci. Ecole Normale Supérieure 6, série 4 (1973), 521-553.

[24] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of Number Fields, Seconde Edition, GMW 323, Springer-Verlag Berlin Heidelberg, 2008.

[25] The PARI Group, PARI/GP version 2.6.1.,http://pari.math.u-bordeaux.fr/.

[26] L. Rédei, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, Math. Anz. Ungar. Akad. d. Wiss. 49 (1932), 338-363.

[27] L. Rédei and H. Reichardt, *Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers (German)*, J. reine u. angew. Math. 170 (1934), 69-74.

[28] A. Schmidt, *Rings of integer of type* $K(\pi, 1)$, Documenta Mathematica 12 (2007), 441-471.

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

[30] A. Schmidt, *On the relation between* 2 *and* ∞ *in Galois cohomology of number fields*, Compositio Math. 133 (2002), no. 3, 267-288.

[31] J.-P. Serre, Topics in Galois Theory, Research Notes in Mathematics, CRC Press, Taylor & Francis Groups, 1992.

[32] P. Stevenhagen, *Rédei-matrices and applications*, Number theory (Paris, 1992–1993), 245–259, London Math. Soc. Lecture Note Ser., 215, Cambridge Univ. Press, Cambridge, 1995.

[33] P. Symonds and T. Weigel, Cohomology of p-adic analytic groups, in "New horizons on pro-p-groups", M. du Sautoy, D. Segal, A. Shalev, Progress in Math. 184, 2000.

[34] D. Vogel, On the Galois group of 2-extensions with restricted ramification, *J. reine u. angew. Math.* 581 (2005), 117-150.

[35] K. Wingberg, *On the Fontaine-Mazur conjecture for CM-fields*, Compositio Math. 131 (2002), 341-354.

[36] Q. Yue, *The generalized Rédei-matrix*, Math. Zeit. 261 (2009), 23-37.

Christian Maire
Laboratoire de Mathématiques
de Besançon (UMR 6623)
Université Bourgogne Franche-Comté
et CNRS
16 route de Gray
25030 Besançon cédex, France
christian.maire@univ-fcomte.fr