MATHEMATICS OF COMPUTATION
Volume 84, Number 291, January 2015, Pages 371–383
S 0025-5718(2014)02838-X
Article electronically published on June 24, 2014

COMPUTING THE TORSION OF THE p-RAMIFIED MODULE OF A NUMBER FIELD

FRÉDÉRIC PITOUN AND FIRMIN VARESCON

ABSTRACT. We fix a prime number p and a number field K, and denote by M the maximal abelian p-extension of K unramified outside p. Our aim is to study the $\mathbb{Z}_p$-module $\mathfrak{X} = \mathrm{Gal}(M/K)$ and to give a method to effectively compute its structure as a $\mathbb{Z}_p$-module. We also give numerical results, for real quadratic fields, cubic fields and quintic fields, together with their interpretations via Cohen-Lenstra heuristics.

1. INTRODUCTION

We fix a prime number p and a number field K. We denote by M the maximal abelian p-extension of K unramified outside p. The aim of this paper is to study the $\mathbb{Z}_p$-module $\mathfrak{X} = \mathrm{Gal}(M/K)$ and give an algorithm to compute its $\mathbb{Z}_p$-structure. This module is described by the exact sequence

$$\overline{U}_K \longrightarrow \textstyle\prod_{v|p} U_v^1 \longrightarrow \mathfrak{X} \longrightarrow \mathrm{Gal}(\mathcal{H}/K) \longrightarrow 1, \tag{1}$$

from class field theory [Gra03, p. 294], where $\overline{U_K}$ is the pro-p-completion of the group of units U_K, U_v^1 is the group of principal units at the place v above p of K, and $\mathcal{H}$ is the maximal p-sub-extension of the Hilbert class field of K. Leopoldt's conjecture for K and p is equivalent to injectivity of $\overline{U}_K \to \prod_{v|p} U_v^1$. Therefore, from this exact sequence, we deduce that the $\mathbb{Z}_p$-rank r of $\mathfrak{X}$ is greater or equal to r_2+1 and is equal r_2+1 if and only if K and p satisfy Leopoldt's conjecture. Hence $\mathfrak{X}$ is the direct product of a free part isomorphic to $\mathbb{Z}_p^r$ and of a torsion part, that we denote by $\mathcal{T}_p$. Our algorithm checks whether K satisfies Leopoldt's conjecture at p and then computes the torsion $\mathcal{T}_p$.

We propose a method which is based on the fact that the $\mathbb{Z}_p$-module $\mathfrak{X}$ is the projective limit of the p-parts of the ray class groups modulo p^n, $\mathcal{A}_{p^n}(K)$. We then study the stabilization of these groups with respect to n and the behaviour of invariants of $\mathcal{A}_{p^n}(K)$, as n is increasing. This approach leads us to our algorithm.

Before addressing the technical part of this article, we recall the definition and some basic properties of the ray class groups modulo p^n. Then, we use our algorithm to compute some cases and propose an heuristic explanation of the statistical data, using the Cohen-Lenstra philosophy [CL84].

Received by the editor April 10, 2012 and, in revised form, February 13, 2013, April 4, 2013 and May 3, 2013.

2010 *Mathematics Subject Classification.* Primary 11R23, 11R37, 11Y40.

2. Background from class field theory

In this section, we recall the basic notions from class field theory that we will need later. We fix v a place of K above p and π_v a local uniformiser of K_v, the completion of K at v. We use [Gra03] and [Ser68] as the main references.

Definition 2.1.

(1) The conductor of an abelian extension of local fields L_v/K_v is the minimum of integers c such that $U_v^c \subset N_{L_v/K_v}(L_v^\times)$ (we recall that $U_v^c = 1 + (\pi_v^c)$ and we use the convention $U_v^0 = U_v$).

(2) (Theorem and Definition 4.1 + Lemma 4.2.1 [Gra03, pp. 126–127]. The conductor of an abelian extension L/K of a global field is the ideal $\mathfrak{m} = \prod_v \mathfrak{p}_v^{c_v}$, where v runs through all finite places of K and where c_v is the conductor of the local extension L_v/K_v.

We start with two lemmas.

Lemma 2.2 ([Ser68, Proposition 9, p. 219])**.** *Let K_v be the completion of K at the valuation v normalized by $v(p) = 1$ and $v(\pi_v) = \frac{1}{e_v}$, where e_v is the ramification index of the extension $K_v/\mathbb{Q}_p$. If $m > \frac{e_v}{p-1}$, then the map $x \mapsto x^p$ is an isomorphism from U_v^m to $U_v^{m+e_v}$.*

Lemma 2.3. *Let $K_v \subset L_v \subset M_v$ be a tower of extensions of $\mathbb{Q}_p$, such that the extension M_v/K_v is abelian and the extension M_v/L_v is of degree p. We denote, respectively, by $c_{M,v}$ and $c_{L,v}$ the conductors of the extensions M_v/K_v and L_v/K_v. If $c_{L,v} > \frac{e_v}{p-1}$, then we have*

$$c_{M,v} \leq c_{L,v} + e_v. \tag{2}$$

Proof. By definition, $c_{L,v}$ is the smallest integer n such that $U_v^n \subset N_{L_v/K_v}(L_v^\times)$. Local class field theory gives the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N_{M_v/K_v}(M_v^\times) & \longrightarrow & K_v^\times & \longrightarrow & \mathrm{Gal}(M_v/K_v) & \longrightarrow & 1 \\ & & \downarrow & & \| & & \downarrow & & \\ 1 & \longrightarrow & N_{L_v/K_v}(L_v^\times) & \longrightarrow & K_v^\times & \longrightarrow & \mathrm{Gal}(L_v/K_v) & \longrightarrow & 1 \end{array}$$

Applying the snake lemma we get the exact sequence

$$1 \longrightarrow N_{M_v/K_v}(M_v^\times) \longrightarrow N_{L_v/K_v}(L_v^\times) \longrightarrow \mathrm{Gal}(M_v/L_v) = \mathbb{Z}/p\mathbb{Z} \longrightarrow 1.$$

Consequently, $N_{M_v/K_v}(M_v^\times)$ is a subgroup of $N_{L_v/K_v}(L_v^\times)$ of index p. Let $n \in \mathbb{N}$, $n \geq c_{L,v} + e_v$, and $x \in U_v^n$. We have to show that $x \in N_{M_v/K_v}(M_v^\times)$. By Lemma 2.2, $x^{\frac{1}{p}}$ is a well-defined element of $U_v^{n-e_v}$. Yet $n - e_v \geq c_{L,v}$, therefore, $x^{\frac{1}{p}} \in N_{L_v/K_v}(L_v^\times)$. Now, as $N_{M_v/K_v}(M_v^\times)$ is of index p in $N_{L_v/K_v}(L_v^\times)$, we deduce that $x \in N_{M_v/K_v}(M_v^\times)$. Therefore, we have that $U_v^n \subset N_{M_v/K_v}(M_v^\times)$ for all integers n such that $n \geq c_{L,v} + e_v$. By the definition of the conductor, this proves (2).

□

Definition 2.4. Let n be a positive integer. We denote by

- H the maximal abelian unramified extension of K;

- H_{p^n} the compositum of all abelian extensions of K whose conductors divide p^n;
- $\mathcal{H}_{p^n}$ the compositum of all abelian p-extensions of K whose conductors divide p^n;
- M the maximal extension of K which is abelian and unramified outside p.

So the Galois groups $\mathrm{Gal}(\mathcal{H}/K)$ and $\mathrm{Gal}(\mathcal{H}_{p^n}/K)$ are, respectively, isomorphic to the p-parts of $\mathrm{Gal}(H/K)$ and $\mathrm{Gal}(H_{p^n}/K)$.

Proposition 2.5 ([Gra03, Corollary 5.1.1, p. 47]). *We have the exact sequences*

$$1 \longrightarrow K^\times \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v} \longrightarrow \mathcal{I}_K \longrightarrow \mathrm{Gal}(H_{p^n}/K) \longrightarrow 1$$

$$1 \longrightarrow K^\times \prod_v U_v \longrightarrow \mathcal{I}_K \longrightarrow \mathrm{Gal}(H/K) \longrightarrow 1,$$

where $\mathcal{I}_K$ is the group of idèles of K.

We denote the Galois group $\mathrm{Gal}(\mathcal{H}_{p^n}/K)$ by $\mathcal{A}_{p^n}(K)$. It is the p-part of the Galois group $\mathrm{Gal}(H_{p^n}/K)$ which, in turn, is isomorphic to the ray class group modulo p^n of K. By definition, we have a natural inclusion $\mathcal{H}_{p^n} \subset \mathcal{H}_{p^{n+1}}$, the union $\bigcup_n \mathcal{H}_{p^n}$ is equal to M and the projective limit $\varprojlim \mathcal{A}_{p^n}(K)$ is canonically isomorphic to $\mathfrak{X}$.

Proposition 2.6. *For any integer $n > 0$, the Galois groups of the extensions M and H_{p^n} of K are related by the exact sequence*

$$1 \longrightarrow U_K^{(p^n)} \longrightarrow \prod_{v|p} U_v^{ne_v} \longrightarrow \mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(H_{p^n}/K) \longrightarrow 1,$$

where $U_K^{(p^n)} = \{u \in U_K \text{ such that } \forall\ v|p, \quad u \in U_v^{ne_v}\}$ and

$$\overline{U}_K^{(p^n)} \longrightarrow \prod_{v|p} U_v^{ne_v} \longrightarrow \mathfrak{X} \longrightarrow \mathcal{A}_{p^n}(K) \longrightarrow 1,$$

where $\overline{U}_K^{(p^n)}$ is the pro-p-completion of $U_K^{(p^n)}$, i.e., $\varprojlim_m U_K^{(p^n)}/p^m$. If, moreover, K and p satisfy Leopoldt's conjecture, then $\overline{U}_K^{(p^n)} \to \prod_{v|p} U_v^{ne_v}$ is injective.

Proof. To obtain the second exact sequence, we apply the pro-p-completion process to the first. Note that the injectivity of $\overline{U}_K^{(p^n)} \to \prod_{v|p} U_v^{ne_v}$ is equivalent to Leopoldt's conjecture. Now we prove exactness of the first sequence.

From the definition of the extensions M and H_{p^n}, we deduce the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & K^\times \prod_{v\nmid p} U_v \prod_{v|p} 1 \arrow[r] \arrow[d, hook] & \mathcal{I}_K \arrow[r] \arrow[d, equal] & \mathrm{Gal}(M/K) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & K^\times \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v} \arrow[r] & \mathcal{I}_K \arrow[r] & \mathrm{Gal}(H_{p^n}/K) \arrow[r] & 1.
\end{tikzcd}$$

By the snake lemma, we have that

$$\ker(\mathrm{Gal}(M/K) \to \mathrm{Gal}(H_{p^n}/K)) = (K^\times \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v})/(K^\times \prod_{v\nmid p} U_v \prod_{v|p} 1).$$

Now, we define the map

$$\theta : (K^\times \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v}) \to (\prod_{v|p} U_v^{ne_v})/U_K^{(p^n)},$$

by setting for $k(u_v)_v \in K^\times \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v}$, $\theta(k(u_v)_v) = \overline{(u_v)_{v|p}}$, where $\overline{(u_v)_{v|p}}$ is the class of $(u_v)_{v|p}$ in $(\prod_{v|p} U_v^{ne_v})/U_K^{(p^n)}$.

We first check that the map θ is well defined, i.e., that if $k(u_v)_v = k'(u'_v)_v$ in $K^\times \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v}$, then $\theta(k(u_v)_v) = \theta(k'(u'_v)_v)$. By definition, for all v, $k(u_v)_v = k'(u'_v)_v$ if and only if $i_v(k)u_v = i_v(k')u'_v$, where i_v is the embedding of K in K_v. We deduce that for all v, $i_v(k'k^{-1}) \in U_v$ and that for all $v|p$, $i_v(k'k^{-1}) \in U_v^{ne_v}$. So we get $k'k^{-1} \in U_K^{(p^n)}$ and $\overline{(u_v)_{v|p}} = \overline{(u'_v)_{v|p}}$.

It is clear that $(K^\times \prod_{v\nmid p} U_v \prod_{v|p} 1) \subset \ker(\theta)$ and that the map θ is surjective. We will show that $(K^\times \prod_{v\nmid p} U_v \prod_{v|p} 1) = \ker(\theta)$. Let $k(u_v) \in \ker(\theta)$. Then there exists $x \in U_K^{(p^n)}$ such that for all $v|p$, $u_v = i_v(x)$. We consider the element $x(u'_v)_v$, where $u'_v = 1$ if $v|p$ and $u'_v = i_v(x)^{-1}u_v$ if $v \nmid p$. We have $(u_v)_v = x(u'_v)_v \Rightarrow k(u_v)_v = kx(u'_v)_v$ and as $kx(u'_v)_v \in (K^\times \prod_{v\nmid p} U_v \prod_{v|p} 1)$, we have $\ker(\theta) \subset (K^\times \prod_{v\nmid p} U_v \prod_{v|p} 1)$, and, finally

$$(K^\times \prod_{v\nmid p} U_v \prod_{v|p} U_v^{ne_v})/(K^\times \prod_{v\nmid p} U_v \prod_{v|p} 1) \simeq (\prod_{v|p} U_v^{ne_v})/U_K^{(p^n)}.$$

We deduce the first exact sequence. □

3. Explicit Computation of $\mathcal{T}_p$

In this section, we present our method to check that K satisfies Leopoldt's conjecture at p and then to compute $\mathcal{T}_p$. The main point is that, for n large enough, $\mathcal{A}_{p^n}(K)$ determines $\mathfrak{X}$.

3.1. **Stabilization of $\mathcal{A}_{p^n}(K)$.** For simplicity we denote $Y_n = \ker(\mathcal{A}_{p^{n+1}}(K) \to \mathcal{A}_{p^n}(K))$. Let $\tilde{K}$ be the compositum of all the $\mathbb{Z}_p$-extensions of K. We denote by r the $\mathbb{Z}_p$-rank of $\mathfrak{X}$, so that $r \geq r_2 + 1$.

Proposition 3.1. *There exists an n_0 such that $\tilde{K} \cap \mathcal{H}_{p^{n_0}}/\tilde{K} \cap \mathcal{H}_p$ is ramified at all places above p. Also, for all $n \geqslant n_0$, Y_n surjects onto $(\mathbb{Z}/p\mathbb{Z})^r$.*

Before proving the proposition, we need a lemma.

Lemma 3.2. *If the extension $\tilde{K} \cap \mathcal{H}_{p^n}/\tilde{K} \cap \mathcal{H}_p$ is ramified at a place v above p, then $c_{n,v} > \frac{e_v}{p-1}$, where $c_{n,v}$ is the conductor of the local extension $(\tilde{K} \cap \mathcal{H}_{p^n})_w/K_v$ and w is a place above v.*

Proof of Lemma 3.2. As M contains the cyclotomic $\mathbb{Z}_p$-extension, there exists an n_0 such that $\tilde{K} \cap \mathcal{H}_{p^{n_0}}/\tilde{K} \cap \mathcal{H}_p$ is ramified at all places v above p. As $\tilde{K} \cap \mathcal{H}_{p^{n_0}}/\tilde{K} \cap \mathcal{H}_p$ is ramified at v, then, for $n \geq n_0$, $\tilde{K} \cap \mathcal{H}_{p^n}/\tilde{K} \cap \mathcal{H}_p$ is ramified at v, so that there exists an m such that $n \geq m \geq 2$ and that $\tilde{K} \cap \mathcal{H}_{p^{m-1}}/\tilde{K} \cap \mathcal{H}_p$ is unramified at v and such that $\tilde{K} \cap \mathcal{H}_{p^m}/\tilde{K} \cap \mathcal{H}_p$ is ramified at v. Then the local conductor $c_{m,v}$ is greater than $(m-1)e_v$, yet $m \geq 2$ so $c_{m,v} > (m-1)e_v \geqslant e_v \geqslant \frac{e_v}{p-1}$. As the conductor of the extension $\tilde{K} \cap \mathcal{H}_{p^m}/K$ divides the conductor of $\tilde{K} \cap \mathcal{H}_{p^n}/K$, we have $c_{n,v} \geqslant c_{m,v} > \frac{e_v}{p-1}$. □

Proof of the Proposition 3.1. We consider the diagram

$$
\begin{tikzcd}[arrows=dash]
\tilde{K}\cap\mathcal{H}_{p^n} \arrow[r] \arrow[d] & (\tilde{K}\cap\mathcal{H}_{p^n})\mathcal{H}_p \arrow[rr] \arrow[d] & & \mathcal{H}_{p^n} \\
\tilde{K}\cap\mathcal{H}_{p^{n-1}} \arrow[r] \arrow[d] & (\tilde{K}\cap\mathcal{H}_{p^{n-1}})\mathcal{H}_p \arrow[r] \arrow[d] & \mathcal{H}_{p^{n-1}} \arrow[ur] \arrow[ur, bend right, "Y_{n-1}"'] & \\
\tilde{K}\cap\mathcal{H}_p \arrow[r] \arrow[d] & \mathcal{H}_p \arrow[ur] & & \\
K. & & &
\end{tikzcd}
\tag{3}
$$

We have $\mathrm{Gal}(\tilde{K}/K) = \mathbb{Z}_p^r$. It is clear that $Y_n \twoheadrightarrow \mathrm{Gal}(\tilde{K}\cap\mathcal{H}_{p^{n+1}}/\tilde{K}\cap\mathcal{H}_{p^n})$. Yet $\mathrm{Gal}(\tilde{K}/\tilde{K}\cap\mathcal{H}_{p^n})$ is a $\mathbb{Z}_p$-submodule of $\mathrm{Gal}(\tilde{K}/K) = \mathbb{Z}_p^r$ of finite index, so it is isomorphic to $\mathbb{Z}_p^r$. Hence there exist r extensions, say $M_1, M_2, \cdots, M_r$ of $\tilde{K}\cap\mathcal{H}_{p^n}$, contained in $\tilde{K}$ such that $\mathrm{Gal}(M_i/\tilde{K}\cap\mathcal{H}_{p^n}) \simeq \mathbb{Z}/p\mathbb{Z}$ and $\mathrm{Gal}(M_1\cdots M_r/\tilde{K}\cap\mathcal{H}_{p^n}) \simeq (\mathbb{Z}/p\mathbb{Z})^r$. Yet the conductor of the extension $\tilde{K}\cap\mathcal{H}_{p^n}/K$ divides $p^n = \prod_{v|p}\mathfrak{p}_v^{ne_v}$. Moreover, the hypothesis on $\tilde{K}\cap\mathcal{H}_{p^n}/\tilde{K}\cap\mathcal{H}_p$ ensures that we can use Lemma 2.3 and consequently the conductor of the extension M_i/K divides $\prod_{v|p}\mathfrak{p}_v^{ne_v+e_v} = p^{n+1}$, i.e., $M_i \subset \mathcal{H}_{p^{n+1}}$ for all $i \in \{1, \cdots, r\}$. Hence the map is surjective. $\square$

We deduce immediately the corollary.

Corollary 3.3. *Let n be a positive integer such that the extension $\tilde{K}\cap\mathcal{H}_{p^n}/\tilde{K}\cap\mathcal{H}_p$ is ramified at all places above p, and that the cardinality of Y_n is exactly p^{r_2+1}. Then $Y_n \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$ and K satisfies Leopoldt's conjecture at p.*

From now on, as we can numerically check that K satisfies Leopoldt's conjecture at p, we assume it does so, in order to compute $\mathcal{T}_p$. Note that if Leopoldt's conjecture is false, then $r > r_2 + 1$ and our algorithm never stops.

Corollary 3.4. *We assume that, for some integer n such that the extension $\tilde{K}\cap\mathcal{H}_{p^n}/\tilde{K}\cap\mathcal{H}_p$ is ramified at all places above of p, the cardinal of Y_n is exactly p^{r_2+1}. Then $Y_n \simeq \mathrm{Gal}(\tilde{K}\cap\mathcal{H}_{p^{n+1}}/\tilde{K}\cap\mathcal{H}_{p^n})$.*

It remains to check that if $Y_{n_0} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$ for some n_0, then $Y_n \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$ for all integers $n \geq n_0$. For this purpose, we consider the exact sequence defining the p-part of the ray class group

$$1 \longrightarrow \overline{U}_K^{(p^n)} \longrightarrow \prod_{v|p} U_v^{ne_v} \longrightarrow \mathfrak{X} \longrightarrow \mathcal{A}_{p^n}(K) \longrightarrow 1,$$

and we denote $\mathcal{Q}_n = \prod_{v|p} U_v^{ne_v}/\overline{U}_K^{(p^n)}$. We have $\mathcal{Q}_n = \mathrm{Gal}(M/\mathcal{H}_{p^n})$ and consequently $\mathcal{Q}_n/\mathcal{Q}_{n+1} = Y_n \simeq \mathrm{Gal}(\mathcal{H}_{p^{n+1}}/\mathcal{H}_{p^n})$.

Proposition 3.5. *For $n \geq 2$, raising to the p^{th} power induces, via the Artin map, a surjection from Y_n to Y_{n+1}.*

Proof. Recall that $\mathcal{Q}_n = \prod_{v|p} U_v^{ne_v}/\overline{U}_K^{(p^n)} = \ker(\mathfrak{X} \to \mathcal{A}_{p^n}(K))$. We have that $n > \frac{1}{p-1}$. Raising to the p^{th} power realizes an isomorphism of $\prod_{v|p} U_v^{ne_v}$ onto

$\prod_{v|p} U_v^{ne_v+e_v}$. This isomorphism induces a surjection from $\mathcal{Q}_n$ onto $\mathcal{Q}_{n+1}$. We consider the diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{Q}_{n+1} \arrow[r] \arrow[d, "(.)^p"] & \mathcal{Q}_n \arrow[r] \arrow[d, "(.)^p"] & \mathcal{Q}_n/\mathcal{Q}_{n+1} \arrow[r] \arrow[d, "(.)^p"] & 1 \\
1 \arrow[r] & \mathcal{Q}_{n+2} \arrow[r] & \mathcal{Q}_{n+1} \arrow[r] & \mathcal{Q}_{n+1}/\mathcal{Q}_{n+2} \arrow[r] & 1.
\end{tikzcd}$$

We deduce from the snake lemma that the vertical arrow on the right-hand side is a surjection from $\mathcal{Q}_n/\mathcal{Q}_{n+1}$ onto $\mathcal{Q}_{n+1}/\mathcal{Q}_{n+2}$, i.e., from Y_n onto Y_{n+1}. □

Corollary 3.6. *We denote $q_n = \#(Y_n)$. For all $n \geqslant 2$, $q_n \geqslant q_{n+1}$. Therefore the sequence $(q_n)_{n\geq 1}$ is ultimately constant.*

We recall that Y_n is $\ker(\mathcal{A}_{p^{n+1}}(K) \to \mathcal{A}_{p^n}(K))$.

Theorem 3.7. *As we assume Leopoldt's conjecture, there exists an integer n_0 such that $Y_{n_0} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$. Moreover, for all integers $n \geq n_0$, the modules $\mathcal{Q}_n = \mathrm{Gal}(M/\mathcal{H}_{p^n})$ are $\mathbb{Z}_p$-free of rank r_2+1 and*

$$Y_n \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}.$$

Proof. The $\mathbb{Z}_p$-module $\mathfrak{X}$ is isomorphic to the direct product of its torsion part and of $\mathbb{Z}_p^{r_2+1}$. An isomorphism being chosen, we can identify $\mathbb{Z}_p^{r_2+1}$ with a subgroup of $\mathfrak{X}$ and therefore define, via Galois theory, an extension M' of K such that $\mathrm{Gal}(M'/K) \simeq \mathcal{T}_p$ and $\tilde{K}M' = M$.

Since this extension is unramified outside p, there exists an integer n_1 such that $M' \subset \mathcal{H}_{p^{n_1}}$ and consequently $\mathcal{H}_{p^{n_1}}\tilde{K} = M$. Moreover, for all integers $n \geq n_1$, $\mathrm{Gal}(M/\mathcal{H}_{p^n})$ is a submodule of finite index of $\mathrm{Gal}(M/M') = \mathbb{Z}_p^{r_2+1}$, and consequently $\mathcal{Q}_n = \mathrm{Gal}(M/\mathcal{H}_{p^n}) \simeq \mathbb{Z}_p^{r_2+1}$. The $\mathbb{Z}_p$-module $\mathcal{Q}_n$ is therefore free of rank r_2+1.

About the other kernel Y_n we saw that there exists an integer n_2 such that Y_n maps surjectively onto $(\mathbb{Z}/p\mathbb{Z})^{r_2+1}$ for all integer $n \geq n_2$ (we can choose n_2 to be the minimum of all integers n such that for all p-places v the conductors of $(\tilde{K} \cap \mathcal{H}_{p^n})_w/K_v$ are at least $\frac{e}{p-1}$). Then we note that mapping $x \in U_v^{ne_v}$ to $x \in U_v^{ne_v+e_v}$ realizes an isomorphism between $U_v^{ne_v}$ and $U_v^{ne_v+e_v}$, so that the quotient $\mathcal{Q}_n/\mathcal{Q}_{n+1}$, which is isomorphic to Y_n, is killed by p. Define $n_0 = \mathrm{Max}(n_1, n_2)$ and let $n \geqslant n_0$ be an integer. The kernel Y_n is therefore a quotient of $\mathbb{Z}_p^{r_2+1}$, which maps surjectively onto $(\mathbb{Z}/p\mathbb{Z})^{r_2+1}$ and is killed by p. Hence we get $Y_n \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$. □

3.2. **Computing the invariants of $\mathcal{T}_p$.** We start by recalling the definition of the invariant factors of an abelian group G.

Definition 3.8. Let G be a finite abelian group, there exists a unique sequence $a_1, \cdots, a_t$ such that $a_i | a_{i+1}$ for $i \in \{1, \cdots, t-1\}$ and $G \simeq \prod_{i=1}^{t} \mathbb{Z}/a_i\mathbb{Z}$.
These a_i are the invariant factors of the group G.

In what follows we will denote these invariants by $\mathcal{FI}(G) = [a_1, \cdots, a_t]$. If G is a p-group, these invariant factors are all powers of p. In practice, we are able to determine the invariant factors of $\mathcal{A}_{p^n}(K)$. We will see in this section that the knowledge of invariant factors of $\mathcal{A}_{p^n}(K)$, for n large enough, combined with the stabilizing properties of $\mathcal{A}_{p^n}(K)$, does determine explicitly the invariant factors of $\mathcal{T}_p$, and thus $\mathcal{T}_p$ itself. We recall that for n large enough, $\mathcal{A}_{p^n}(K)$ is isomorphic to the direct product of $\mathrm{Gal}(\tilde{K}\cap\mathcal{H}_{p^n}/K)$ and of $\mathrm{Gal}(\mathcal{H}_{p^n}/\tilde{K}\cap\mathcal{H}_{p^n})=\mathcal{T}_p$. So we will first explore the structure of $\mathrm{Gal}(\tilde{K}\cap\mathcal{H}_{p^n}/K)$.

Proposition 3.9. *Let n_0 be such that $\tilde{K}\cap\mathcal{H}_{p^{n_0}}/\tilde{K}\cap\mathcal{H}_p$ is ramified at all places above p and*

$$Y_{n_0}\simeq(\mathbb{Z}/p\mathbb{Z})^{r_2+1}.$$

Then for all integers $n\geq n_0$, we have

$$\mathrm{Gal}(\tilde{K}/\tilde{K}\cap\mathcal{H}_{p^{n+1}})=p\,\mathrm{Gal}(\tilde{K}/\tilde{K}\cap\mathcal{H}_{p^n}).$$

Proof. By Theorem 3.7, on the one hand, $\mathcal{Q}_n$ is $\mathbb{Z}_p$-free of rank r_2+1 and, on the other hand, $Y_n=\mathcal{Q}_n/\mathcal{Q}_{n+1}\simeq(\mathbb{Z}/p\mathbb{Z})^{r_2+1}$. This gives $\mathcal{Q}_{n+1}=p\mathcal{Q}_n$. As $\tilde{K}\cap\mathcal{H}_{p^{n_0}}/\tilde{K}\cap\mathcal{H}_p$ is ramified at all places above p and $Y_{n_0}\simeq(\mathbb{Z}/p\mathbb{Z})^{r_2+1}$, we have $\mathcal{T}_p\subset\mathcal{A}_{p^{n_0}}(K)$, so $\tilde{K}\mathcal{H}_{p^{n_0}}=M$. Then, considering the diagram

$$\begin{tikzcd}
\tilde{K} \arrow[r, dash] \arrow[d, dash] & M \arrow[d, dash] \arrow[d, bend right, dash, "\mathcal{Q}_{n+1}"'] \arrow[dd, bend left, dash, "\mathcal{Q}_n"] \\
\tilde{K}\cap\mathcal{H}_{p^{n+1}} \arrow[r, dash] \arrow[d, dash] & \mathcal{H}_{p^{n+1}} \arrow[d, dash] \\
\tilde{K}\cap\mathcal{H}_{p^n} \arrow[r, dash] \arrow[d, dash] & \mathcal{H}_{p^n} \\
K &
\end{tikzcd}$$

we get the required isomorphism. □

Corollary 3.10. *Let n_0 be an integer such that $\tilde{K}\cap\mathcal{H}_{p^{n_0}}/\tilde{K}\cap\mathcal{H}_p$ is ramified at all places above p and such that $Y_{n_0}\simeq(\mathbb{Z}/p\mathbb{Z})^{r_2+1}$. Then for all integers $n\geq n_0$ the invariant factors of $\mathrm{Gal}(\tilde{K}\cap\mathcal{H}_{p^{n+1}}/K)$ are obtained by multiplying by p each invariant factor of $\mathrm{Gal}(\tilde{K}\cap\mathcal{H}_{p^n}/K)$.*

From the fact that $\mathfrak{X}\simeq\mathbb{Z}_p^{r_2+1}\times\mathcal{T}_p$, the ray class group, $\mathrm{Gal}(\mathcal{H}_{p^n}/K)$, is isomorphic to the direct product of $\mathrm{Gal}(\tilde{K}\cap\mathcal{H}_{p^n}/K)$ and $\mathrm{Gal}(\mathcal{H}_{p^n}/\tilde{K}\cap\mathcal{H}_{p^n})$. The invariant factors of $\mathrm{Gal}(\mathcal{H}_{p^n}/K)$ are then simply obtained by concatenating the two groups forming the direct product. We now state the result that explicitly determines $\mathcal{T}_p$.

Theorem 3.11. *Let n be such that $Y_n=(\mathbb{Z}/p\mathbb{Z})^{r_2+1}$ and $\tilde{K}\cap\mathcal{H}_{p^n}/\tilde{K}\cap\mathcal{H}_p$ is ramified at all places above p. We assume that*

$$\mathcal{FI}(\mathcal{A}_{p^n}(K))=[b_1,\cdots,b_t,a_1,\cdots,a_{r_2+1}]$$

with $(v_p(a_1))>(v_p(b_t))+1$, and that

$$\mathcal{FI}(\mathcal{A}_{p^{n+1}}(K))=[b_1,\cdots,b_t,pa_1,\cdots,pa_{r_2+1}].$$

Then we have

$$\mathcal{FI}(\mathcal{T}_p)=[b_1,\cdots,b_t].$$

Proof. Indeed, as $Y_n \simeq (\mathbb{Z}/p\mathbb{Z})^{r_2+1}$, we have $\mathcal{A}_{p^i}(K) \simeq \mathcal{T}_p \times \mathrm{Gal}(\tilde{K} \cap \mathcal{H}_{p^i}/K)$ for $i \in \{n, n+1\}$. We saw that the invariant factors of $\mathrm{Gal}(\tilde{K} \cap \mathcal{H}_{p^{n+1}}/K)$ are exactly equal to p times those of $\mathrm{Gal}(\tilde{K} \cap \mathcal{H}_{p^n}/K)$. Consequently, if a is an invariant factor of $\mathrm{Gal}(\tilde{K} \cap \mathcal{H}_{p^{n+1}}/K)$, we have necessarily that $a = pa_i$ or $a = pb_i$. But as $\mathrm{Min}(v_p(a_i)) > \mathrm{Max}(v_p(b_i)) + 1$, none of the invariant factors of $\mathrm{Gal}(\tilde{K} \cap \mathcal{H}_{p^{n+1}}/K)$ are of the form pb_i. The invariant factors of $\mathrm{Gal}(\tilde{K} \cap \mathcal{H}_{p^{n+1}}/K)$ are therefore exactly $pa_1, \cdots, pa_{r_2+1}$. The result follows from the fact that $\mathcal{A}_{p^{n+1}}(K)$ is isomorphic to the direct product of $\mathcal{T}_p$ and $\mathrm{Gal}(\tilde{K} \cap \mathcal{H}_{p^{n+1}}/K)$. $\square$

4. Explicit computation of bounds

More generally, if we denote by $e = \max_{v|p} \{e_v\}$ the ramification index of $K/\mathbb{Q}$ and by s the p-adic valuation of e, then we can start to check whether $\mathcal{A}_{p^n}(K)$ stabilizes from rank $n = 2 + s$. To show that $n = 2 + s$ is the proper starting point we consider the diagram

$$\begin{tikzcd}
& \tilde{K}\cap\mathcal{H}_{p^{s+2}} \arrow[dl, dash] \arrow[dd, dash] \arrow[rrr, dash] & & & \mathcal{H}_{p^{s+2}} \arrow[dl, dash] \\
K_{s+1} \arrow[ddr, dash] & & & \mathcal{H}_{p^{s+1}} \arrow[dl, dash] & \\
& \tilde{K}\cap\mathcal{H}_p \arrow[r, dash] \arrow[d, dash] & \mathcal{H}_p & & \\
& K & & &
\end{tikzcd}$$

where K_j is the j^{th} field of the $\mathbb{Z}_p$-extension of K.

We prove below that the places above p are totally ramified in K_{s+1}/K_s. Therefore, $\tilde{K}\cap\mathcal{H}_{p^s}/\tilde{K}\cap\mathcal{H}_p$ is ramified at all places above p and we start the computation by checking whether $\mathcal{A}_{p^n}(K)$ stabilizes from $n = s + 2$, and until it stabilizes. We first prove that all places above p are totally ramified in K_{s+1}/K_s.

We consider the diagram

$$\begin{tikzcd}
& & K_{s+1} \arrow[dl, dash] \arrow[dr, dash] & \\
& K_s \arrow[dl, dash] \arrow[dr, dash] & & \mathbb{Q}_{s+1} \arrow[dl, dash] \\
K \arrow[dr, dash] & & \mathbb{Q}_s \arrow[dl, dash] & \\
& \mathbb{Q} & &
\end{tikzcd}$$

The ramification index of p in $\mathbb{Q}_{s+1}/\mathbb{Q}$ is p^{s+1}, while the one in $K/\mathbb{Q}$ is $p^s a$ with $p \nmid a$. Therefore the extension K_{s+1}/K is ramified and K_{s+1}/K_s is totally ramified at all places above p.

Corollary 4.1. *Let e be the ramification index of p in $K/\mathbb{Q}$ and let s be the p-adic valuation of e. Let $n \geq 2+s$, we assume that*

$$\mathcal{FI}(\mathcal{A}_{p^n}(K)) = [b_1, \cdots, b_t, a_1, \cdots, a_{r_2+1}],$$

with $\mathrm{Min}(v_p(a_i)) > \mathrm{Max}(v_p(b_i)) + 1$ *and, moreover, that*

$$\mathcal{FI}(\mathcal{A}_{p^{n+1}}(K)) = [b_1, \cdots, b_t, pa_1, \cdots, pa_{r_2+1}].$$

Then we have

$$\mathcal{FI}(\mathcal{T}_p) = [b_1, \cdots, b_t].$$

All the computations have been done using the PARI/GPsystem [PAR13].

Example 4.2. We consider the field $K = \mathbb{Q}(\sqrt{-129})$ and $p = 3$. We have $\mathcal{FI}(\mathcal{A}_{p^2}(K)) = [3,3,9]$, $\mathcal{FI}(\mathcal{A}_{p^3}(K)) = [3,9,27]$ and $\mathcal{FI}(\mathcal{A}_{p^4}(K)) = [3,27,81]$. We deduce that $\mathcal{T}_p = (\mathbb{Z}/3\mathbb{Z})$.

5. Numerical results

In the section, we present some of our numerical results and give an explanation of these computations.

5.1. **Heuristic approach.** We first recall some results on Cohen-Lenstra Heuristics. The main reference on the subject is the seminal paper of Cohen-Lenstra [CL84]; see also [Del07]. These heuristics leads us to compare the proportion of fields with non-trivial $\mathcal{T}_p$ with the proportion of groups with non-trivial p-part inside all finite abelian groups. If we assume that the extension $K/\mathbb{Q}$ is Galois with $\Delta = \mathrm{Gal}(K/\mathbb{Q})$, then the module $\mathcal{T}_p$ is a $\mathbb{Z}[\Delta]$-module. In this section, we assume that Δ is cyclic of cardinality l, for some prime number l. Then, as the p-part of the class group, $\mathcal{T}_p$ itself is a finite O_l-module, where O_l is the ring of integers of $\mathbb{Q}(\zeta_l)$. This module $\mathcal{T}_p$ is known in Iwasawa theory as the proper p-adic analogue of the class group. Hence it is a natural question to compute it, to examine the distribution of fields with non-trivial $\mathcal{T}_p$, and to compare this distribution with the Cohen-Lenstra heuristics about the distribution of groups with non-trivial p-part inside all finite abelian groups.

In what follows, O_F will be the ring of integers of a number field and G will be a finite O_F-module. In general, we know that all O_F-modules G can be written in a non-canonical way as $\bigoplus_{i=1}^q O_F/\mathfrak{a}_i$, where the $\mathfrak{a}_i$ are ideals of O_F. Yet the Fitting ideal $\mathfrak{a} = \prod_{i=1}^q \mathfrak{a}_i$ depends only on the isomorphism class of G, considered as a O_F-module. This invariant, denoted by $\mathfrak{a}(G)$, can be considered as a generalization of the order of G. We also have $N(\mathfrak{a}(G)) = \#G$.

We consider a function g, defined on the set of the isomorphism classes of O_F-modules (typically g is a characteristic function). We follow [CL84] for the next definition, using the same notations.

Definition 5.1. The average of g, if it exists, is the limit when $N \to \infty$ of the quotient

$$\frac{\displaystyle\sum_{G, N(\mathfrak{a}(G)) \leq N} \frac{g(G)}{\# \mathrm{Aut}_{O_F}(G)}}{\displaystyle\sum_{G, N(\mathfrak{a}(G)) \leq N} \frac{1}{\# \mathrm{Aut}_{O_F}(G)}}.$$

where $\sum_{G,N(\mathfrak{a}(G))\leq N}$ is the sum is over all isomorphism classes of O_F-modules G. This average is denoted by $M_{l,0}(g)$.

We denote by $w(\mathfrak{a}) = \sum_{G,\mathfrak{a}(G)=\mathfrak{a}} \frac{1}{\#\operatorname{Aut}_{O_F}(G)}$, where $\mathfrak{a}$ is an ideal of O_F (using the same notation as [CL84]).

Proposition 5.2 ([CL84, Corollary 3.8, p. 40])**.** *Let $n \in \mathbb{N}$. Then*

$$w(\mathfrak{a}) = \frac{1}{N(\mathfrak{a})}\left(\prod_{\mathfrak{p}^\alpha||\mathfrak{a}}\prod_{k=1}^{\alpha}(1-\frac{1}{N_{O_K}(\mathfrak{p})^k})\right)^{-1}.$$

The notation $\mathfrak{p}^\alpha||\mathfrak{a}$ means that $\mathfrak{p}^\alpha|\mathfrak{a}$ and that $\mathfrak{p}^{\alpha+1}\nmid\mathfrak{a}$. Consequently, the function w, defined on the set of ideals of O_F, is multiplicative.

Notation. We denote by Π_p the characteristic function of the set of isomorphism classes of groups whose p-part is non-trivial.

Proposition 5.3 ([CL84, Example 5.10, p. 47])**.** *We denote by $\mathfrak{p}_1,\cdots,\mathfrak{p}_g$ the p-places of O_F, the average of Π_p exists and we have*

$$M_{l,0}(\Pi_p) = 1-\prod_{i=1}^{g}\prod_{k\geq 1}\left(1-\frac{1}{p^{kf_i}}\right), \tag{4}$$

where f_i is the degree of the residual extensions $O_F/\mathfrak{p}_i$ over $\mathbb{F}_p$.

Corollary 5.4. *If the extension F is a Galois extension, all residual degrees are equal to f and in this case*

$$M_{l,0}(\Pi_p) = 1-\prod_{k\geq 1}\left(1-\frac{1}{p^{kf}}\right)^g.$$

Remark. The real number $M_{l,0}(\Pi_p)$ is called the 0-average. This notion can be generalized to the u-average. The expression to compute the u-average is obtained by replacing k by $k+u$ in the expression (4) of the 0-average.

Let $\mathcal{K}$ be a set of number fields, cyclic of degree l, let K run through $\mathcal{K}$ and let G be the p-part of the class group of F. We assume $l \neq p$. If we denote by $A = \mathbb{Z}[\Delta]/\sum_{g\in\Delta} g$, where $\Delta = \operatorname{Gal}(K/\mathbb{Q})$, it is easy to see that G is a finite A-module. As Δ is cyclic of order l, then G is an O_l-module. Following the Cohen-Lenstra Heuristics we give the assumptions.

Assumptions 1 ([CL84, Assumptions, p. 54])**.** *Recall that $l = [K:\mathbb{Q}]$, then we have:*

1. *(Complexe quadratic case) If $r_1 = 0$, $r_2 = 1$, then the proportion of G which are non-trivial is the 0-average of Π_p, restricted to O_l-modules of order prime to l.*
2. *(Totally real case) If $r_1 = n$, $r_2 = 0$, then the proportion of G which are non-trivial is the 1-average of Π_p, restricted to O_l-modules of order prime to l.*

5.2. **Somes numerical results.**

5.2.1. *Case of the quadratic fields.* We observed that in the case of real quadratic fields the proportion of fields with non-trivial $\mathbb{Z}_p$-torsion of $\mathfrak{X}$ was a 0-average, and a 1-average for the imaginary quatratic fields. We will explain why this phenomenon is consistent with Cohen-Lenstra Heuristics in Section 5.2.2.

We consider all quadratic fields $\mathbb{Q}(\sqrt{d})$ with d square-free and $0 < d \leq 10^9$. Then we compute the proportion of fields with non-trivial $\mathcal{T}_p$. We denote this proportion by $f_{\exp}$. The relative error $|f_{\exp} - M_{2,0}(\Pi_p)|/M_{2,0}(\Pi_p)$ is denoted by δ. We remark that δ tends to 0 if we increase the numbers of fields whose torsion we compute, except for the cases p=2 and 3. We explain this discrepancy with 2 and 3 in Section 5.2.2.

p	$M_{2,0}(\Pi_p)$	$f_{\exp}$	δ
2	0,71118	0,93650	0,31683
3	0,43987	0,50120	0,13942
5	0,23967	0,23854	0,00470
7	0,16320	0,16280	0,00247
11	0,09916	0,09893	0,00243
13	0,08284	0,08266	0,00212
17	0,06228	0,06214	0,00233
19	0,05540	0,05526	0,00260
23	0,04537	0,04527	0,00207
29	0,03375	0,03560	0,00193
31	0,03330	0,03323	0,00219
37	0,02776	0,02770	0,00198
41	0,02499	0,02493	0,00207
43	0,02380	0,02376	0,00152
47	0,02173	0,02168	0,00207

We consider now the quadratic field $\mathbb{Q}(\sqrt{d})$ with $-10^9 \leqslant d \leqslant 0$. One uses the 1-average denoted by $M_{2,1}(\Pi_p)$.

p	$M_{2,1}(\Pi_p)$	$f_{\exp}$	δ
2	0,42235	0,93650	1.12734
3	0,15981	0,25718	0,60926
5	0,04958	0,04909	0,00989
7	0,02374	0,02365	0,00374
11	0,00908	0,00905	0,00416
13	0,00641	0,00638	0,00360
17	0,00368	0,00365	0,00445
19	0,00292	0,00291	0,00589
23	0,00198	0,00197	0,00510
29	0,00123	0,00122	0,00916
31	0,00108	0,00107	0,00929
37	0,00075	0,00074	0,00813
41	0,00061	0,00060	0,00982
43	0,00055	0,00055	0,00998
47	0,00046	0,00046	0,01626

We have also computed the proportions for cubic fields, with the program of K. Belabas [Bel97], and for quintic fields using the tables which are available on the website dedicated to PARI/GPsystem [PAR13]. Then we consider the distribution of torsion modules with respect to invariant factors that will not be presented here, for the sake of brevity. To compute $\#\operatorname{Aut}_{O_K}(G)$ we use [Hal38].

5.2.2. *Explanation of numerical results.* In this section we explain our numerical results. Looking at the two tables in §5.2.1 we remark that the proportion $f_{\exp}$ for real quadratic fields seems to be a 0-average, and a 1-average for the imaginary quadratic. We remark also that the default δ for $p = 2, 3$ increases with the number of fields computed. To explain these phenomena we recall a computation of Gras [Gra82, pp. 94–97]. Let k be a number field, we denote by $K = k(\zeta_p)$ and ω the idempotent associated with the action of $\mathrm{Gal}(K/k)$ on μ_p.

Theorem 5.5 ([Gra82, Corollaire 1, p. 96]). *Let p be a prime, $p \neq 2$. If $\mu_p \not\subset k$, then the torsion of $\mathfrak{X}$ is trivial if and only if any prime ideal of k dividing p is totally split in K/k and $(Cl_K)^\omega$ is trivial, where Cl_K is the p-part of the class group of K.*

In the case of quadratic fields, if $p > 3$, then $\mu_p \not\subset k$ and the ramification index of p in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is $p-1$; then all prime ideals of k dividing p ramify in K. Therefore they are not totally split, and so the torsion is trivial if and only if $(Cl_K)^\omega$ is trivial. So when k is a real quadratic field the computation of $\mathcal{T}_p$ reduces to the computation of a class group of imaginary quadratic field and we use the 0-average following Cohen-Lenstra Heuristics. In the case of imaginary quadratic the remark [Gra82, pp. 96–97] explains the 1-average. In the case $p = 3$, if $d \equiv 6 \bmod 9$, then the ideal of k above p is totally split in K, so the torsion is non-trivial. It explains why the frequency obtained is greater. If we consider the other average $M_2'(\Pi_3) = M_{2,0}(\Pi_3) \times \frac{7}{8} + \frac{1}{8}$, then in the real case we obtain

N	$M_2'(\Pi_3)$	$f_{\exp}$	δ
10^6	0,50989	0,48094	0,05678
10^7	0,50989	0,49054	0,03794
10^8	0,50989	0,49697	0,02533
10^9	0,50809	0,50120	0,01704

We now make the computation without the case $d \equiv 6 \bmod 9$.

N	$M_{2,0}(\Pi_3)$	$f_{\exp}$	δ
10^6	0,43987	0,40679	0,07521
10^7	0,43987	0,41776	0,05027
10^8	0,43987	0,42511	0,03356
10^9	0,43987	0,42995	0,02257

It remains to study the 9-rank in the case where $d \equiv 6 \bmod 9$, and to try and find density formulas for the 9-rank. Finally, the discrepancy in the case $p = 2$ is explained by genus theory. Indeed, if the discriminant is divided by enough primes, then the torsion is not trivial. This explains why the frequency tends to 1.

Acknowledgements

It is the authors pleasure to thank Bill Allombert for his help with PARI/GP computations, Christophe Delaunay for his relevant suggestions and the anonymous referees who have devoted their time to study the previous versions of this article and suggested many improvements.

References

[Bel97] K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), no. 219, 1213–1237, DOI 10.1090/S0025-5718-97-00846-6. MR1415795 (97m:11159)

[CL84] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62, DOI 10.1007/BFb0099440. MR756082 (85j:11144)

[Del07] Christophe Delaunay, *Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics*, Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., vol. 341, Cambridge Univ. Press, Cambridge, 2007, pp. 323–340, DOI 10.1017/CBO9780511735158.021. MR2322355 (2008i:11089)

[Gra82] Georges Gras, *Groupe de Galois de la p-extension abélienne p-ramifiée maximale d'un corps de nombres* (French), J. Reine Angew. Math. **333** (1982), 86–132, DOI 10.1515/crll.1982.333.86. MR660786 (84j:12008)

[Gra03] Georges Gras, *Class Field Theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003. From theory to practice; Translated from the French manuscript by Henri Cohen. MR1941965 (2003j:11138)

[Hal38] P. Hall, *A partition formula connected with Abelian groups*, Comment. Math. Helv. **11** (1938), no. 1, 126–129, DOI 10.1007/BF01199694. MR1509594

[PAR13] The PARI Group – Bordeaux, *Pari/gp, version* `2.6.0`, 2013, available from `http://pari.math.u-bordeaux.fr/`.

[Ser68] Jean-Pierre Serre, *Corps Locaux* (French), Hermann, Paris, 1968. Deuxième édition; Publications de l'Université de Nancago, No. VIII. MR0354618 (50 #7096)

27 Avenue du 8 mai 1945, 11400 Castelnaudary, France
E-mail address: `frederic.pitoun@free.fr`

Laboratoire de mathématiques de Besançon, CNRS UMR 6623, Université de Franche Comté, 16 Route de Gray, 25020 Besançon Cédex, France
E-mail address: `firmin.varescon@univ-fcomte.fr`