Algorithmic complexity of Greenberg's conjecture

Georges Gras

ALGORITHMIC COMPLEXITY OF GREENBERG'S CONJECTURE

GEORGES GRAS

Abstract. Let k be a totally real number field and p a prime. We show that the "complexity" of Greenberg's conjecture ($\lambda = \mu = 0$) is of p-adic nature governed (under Leopoldt's conjecture) by the finite torsion group $\mathscr{T}_k$ of the Galois group of the maximal abelian p-ramified pro-p-extension of k, by means of images in $\mathscr{T}_k$ of ideal norms from the layers k_n of the cyclotomic tower (Theorem 5.2). These images are obtained via the formal algorithm computing, by "unscrewing", the p-class group of k_n. Conjecture 5.4 of equidistribution of these images would show that the number of steps b_n of the algorithms is bounded as $n \to \infty$, so that Greenberg's conjecture, hopeless within the sole framework of Iwasawa's theory, would hold true "with probability 1". No assumption is made on $[k : \mathbb{Q}]$, nor on the decomposition of p in $k/\mathbb{Q}$.

Contents

2020 *Mathematics Subject Classification.* 11R23, 11R29, 11R37, 11Y40.

Key words and phrases. Greenberg's conjecture, p-class groups, class field theory, p-adic regulators, p-ramification theory, Iwasawa's theory.

1. Introduction

Let k be a totally real number field, $p \geq 2$ a prime number and S the set of p-places $\mathfrak{p} \mid p$ of k. Let k_∞ be the cyclotomic $\mathbb{Z}_p$-extension of k and k_n the degree p^n extension of k in k_∞. Let $\mathscr{C}\!\ell_k$ and $\mathscr{C}\!\ell_{k_n}$ be the p-class groups of k and k_n, respectively. We denote by $\mathscr{T}_k$ the torsion group of $\mathscr{A}_k := \mathrm{Gal}(H_k^{\rm pr}/k)$, where $H_k^{\rm pr}$ is the maximal abelian S-ramified pro-p-extension of k (i.e., unramified outside S), assuming the Leopoldt conjecture for p in k_∞. The group $\mathscr{T}_k$ is closely related to the deep Tate–Chafarevich group (same p-rank):

$$Ш_k^2 := \mathrm{Ker}\big[\mathrm{H}^2(\mathscr{G}_{k,S}, \mathbb{F}_p) \to \oplus_{\mathfrak{p}\mid p}\, \mathrm{H}^2(\mathscr{G}_{k_\mathfrak{p}}, \mathbb{F}_p)\big],$$

where $\mathscr{G}_{k,S}$ is the Galois group of the maximal S-ramified pro-p-extension of k (hence $\mathscr{A}_k = \mathscr{G}_{k,S}^{\rm ab}$) and $\mathscr{G}_{k_\mathfrak{p}}$ the local analogue over $k_\mathfrak{p}$; but $\mathscr{T}_k$ is very easily computable and relates the p-class group and the p-adic regulator.

We call *Greenberg's conjecture for k and p*, the nullity of the Iwasawa invariants λ, μ (see the origin of the conjecture in [10, Theorems 1 and 2]). The main effective test for this conjecture is the criterion of Jaulent [14, Théorèmes A, B] proving that the conjecture is equivalent to the capitulation in k_∞ of the logarithmic class group $\widetilde{\mathscr{C}\!\ell}_k$ of k (defined in [12] with PARI/GP pakage in [1]), an invariant also related to S-ramification theory. [1] For specific cases of decomposition of p, as in [10], see [19].

In our opinion, many aesthetic statements, equivalent to Greenberg's conjecture, are translations of standard formalism of class field and Iwasawa's theories. In other words, *some "non-algebraic" p-adic aspects of the "diophantine construction" of the class groups at each layer k_n*, are not taken into account. We show how this construction works and study its arithmetic complexity by means of the number b_n of steps of the algorithms which become oversized in the tower as soon as λ or μ are non-zero, suggesting the triviality of the algorithms for $n \gg 0$ (i.e., $b_n \leq 1$).

Our purpose has nothing to do with computational or theoretical approaches in the area of the "main theorem" on abelian fields (analytic formulas, cyclotomic units, L_p-functions, etc.) as, for instance, the very many contributions (cited in our papers [5, 6]), also giving computations and suggesting that equidistribution results may have striking consequences for the conjecture; our viewpoint is essentially logical and based on the governing group $\mathscr{T}_k$, because we have conjectured that $\mathscr{T}_k = 1$ for all $p \gg 0$, due to

[1] For more information on the main pioneering works about *the practice* of this theory, see "history of abelian p-ramification" in [9, Appendix] (e.g., Gras: "Crelle's Journal" (1982/83), Jaulent: "Ann. Inst. Fourier" (1984), Nguyen Quang Do: "Ann. Inst. Fourier" (1986), Movahhedi "Thèse" (1988) and others). For convenience, we mostly refer to our book (2003/2005), which contains all the needed results in the most general statements. For more broad context about the base field and the set S, see [16] and its bibliography.

properties of p-adic regulators [8] (p-rationality of k, as defined in [17] for such fields), which relativizes Greenberg's conjecture, obvious in that case.

In many papers, as in [10], the decomposition of p in $k/\mathbb{Q}$ plays a specific role, which is not necessary for us. We shall not put any assumption on the degree of k nor on the decomposition of p in $k/\mathbb{Q}$.

Conventions 1.1. *Subject to replace k by a layer $K = k_{n_0}$ of $k_\infty = K_\infty$, one may assume, without any loss of generality, that p is totally ramified in K_∞/K and is such that Iwasawa's formula for $\#\mathscr{C}_{k_n}$ holds true for all layers above K; indeed, we have $\lambda(K) = \lambda(k)$, $\mu(K) = [K : k]\,\mu(k)$ and $\nu(K) = \nu(k) + \lambda(k)\,n_0$.*

2. Main results

The results of the paper may be described as follows in two parts:

(A) From results of [4, 5, 6]. The formal algorithm, determining $\#\mathscr{C}_{k_n}$ (whence giving the Iwasawa invariants), computes inductively the classical filtration $(\mathscr{C}^i_{k_n})_{i\geq 0}$, where $\mathscr{C}^{i+1}_{k_n}/\mathscr{C}^i_{k_n} := (\mathscr{C}_{k_n}/\mathscr{C}^i_{k_n})^{G_n}$, for all $i \geq 0$ ($\mathscr{C}^0_{k_n} = 1$), where $G_n = \mathrm{Gal}(k_n/k)$. We have the decreasing i-sequence:

$$\#\big(\mathscr{C}^{i+1}_{k_n}/\mathscr{C}^i_{k_n}\big) = \frac{\#\mathscr{C}_k}{\#\mathrm{N}_{k_n/k}(\mathscr{C}^i_{k_n})} \cdot \frac{p^{n\cdot(\#S-1)}}{(\Lambda^i_n : \Lambda^i_n \cap \mathrm{N}_{k_n/k}(k_n^\times))}, \tag{2.1}$$

with the increasing i-sequence of groups Λ^i_n, from $\Lambda^0_n = E_k$:

$$\Lambda^i_n := \{x \in k^\times,\ \ (x) = \mathrm{N}_{k_n/k}(\mathfrak{A}),\ \ \mathscr{cl}_{k_n}(\mathfrak{A}) \in \mathscr{C}^i_{k_n}\}. \tag{2.2}$$

Then $\mathscr{C}^{i+1}_{k_n}/\mathscr{C}^i_{k_n}$ in (2.1) becomes trivial for some minimal $i =: b_n \geq 0$ (giving $\mathscr{C}^{b_n}_{k_n} = \mathscr{C}_{k_n}$) as soon as the two factors vanish. Thus the length b_n of the algorithm depends on the decreasing evolution of the "class factor" $\frac{\#\mathscr{C}_k}{\#\mathrm{N}_{k_n/k}(\mathscr{C}^i_k)}$ dividing $\#\mathscr{C}_k$ and that of the "norm factor" $\frac{p^{n\cdot(\#S-1)}}{(\Lambda^i_n : \Lambda^i_n \cap \mathrm{N}_{k_n/k}(k_n^\times))}$ dividing the order of a suitable quotient $\mathscr{R}^{\mathrm{nr}}_k$ of the normalized p-adic regulator $\mathscr{R}_k$ (defined in [7, § 5]), related to the ramification of p in $H^{\mathrm{pr}}_k/k_\infty$ (Theorem 3.4, Corollary 4.2). We prove in Theorem 4.3, under Conventions 1.1, the following inequalities (where v_p is the p-adic valuation):

$$b_n \leq \lambda \cdot n + \mu \cdot p^n + \nu \leq v_p(\#\mathscr{C}_k \cdot \#\mathscr{R}^{\mathrm{nr}}_k) \cdot b_n,$$

giving $\mathscr{C}_k = \mathscr{R}^{\mathrm{nr}}_k = 1 \iff \lambda = \mu = \nu = 0 \iff b_n = 0$ for all n.

Taking k hight enough in the tower, Greenberg's conjecture is equivalent to $b_n \leq 1$ for all n (Corollary 4.4), which constitutes a spectacular algorithmic discontinuity compared to $b_n \to \infty$ if λ or μ are non-zero. In an heuristic point of view, it is "necessary" that the algorithms become limited, because of the unpredictable behavior of the class and norm factors.

(B) One may replace, in (2.2), the ideal norms $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$ by representatives $\mathfrak{t} \in I_{k_n} \otimes \mathbb{Z}_p$ (I_{k_n} is the group of prime-to-p ideals of k_n) whose Artin

symbols are in $\mathscr{T}_k$, *hence finite in number* (main Theorem 5.2); so, each step of the algorithm (i.e., the evolution of the class and norm factors) only depends on at most $\#\mathscr{T}_k$ possibilities, taking the class of the random ideal $\mathfrak{t}$, then computing Hasse's symbols on S of numbers $\tau \in k_n^\times \otimes \mathbb{Z}_p$ when $\mathfrak{t} = (\tau)$ is principal, in other words, for this last case a classical situation involving random $\mathbb{Z}/p^n\mathbb{Z}$-matrices of symbols for which some equidistribution results are proven [20, Section 6].

Then, under the natural Conjecture 5.4 of independence and randomness of the data obtained, inductively, at each step of the algorithm, one would obtain that Greenberg's conjecture holds true with "probability 1", suggesting possible analytic proof of this fact, using the powerful techniques used in [15, 20] for degree p cyclic extensions of $\mathbb{Q}$, but unfortunately, probably not a complete proof of Greenberg's conjecture.

3. Abelian p-ramification and genus theories

3.1. **Abelian p-ramification – The torsion group $\mathscr{T}_k$.** Recall the data needed for the study of the Galois group $\mathscr{A}_k$ of the maximal abelian p-ramified pro-p-extension $H_k^{\rm pr}$ of k and its torsion group $\mathscr{T}_k$ (under Leopoldt's conjecture). Let $k'^\times$ be the subgroup of $k^\times$ of prime-to-p elements:

(**a**) Let E_k be the group of p-principal units $\varepsilon \equiv 1 \,(\mathrm{mod}\ \prod_{\mathfrak{p}\in S}\mathfrak{p})$ of k. Let $U_k := \bigoplus_{\mathfrak{p}\in S} U_\mathfrak{p}$ be the $\mathbb{Z}_p$-module of p-principal local units, where $U_\mathfrak{p}$ is the group of $\mathfrak{p}$-principal units of the $\mathfrak{p}$-completion $k_\mathfrak{p}$ of k. Let μ_k (resp. $\mu_\mathfrak{p}$) be the group of pth roots of unity of k (resp. $k_\mathfrak{p}$). Put $W_k := \bigoplus_{\mathfrak{p}\in S} \mu_\mathfrak{p}$ and $\mathscr{W}_k := W_k/\mu_k$; thus, $\mathscr{W}_k = W_k$ for $p \neq 2$ and $\mathscr{W}_k = W_k/\langle \pm 1 \rangle$ for $p = 2$.

(**b**) Let $\iota : k'^\times \otimes \mathbb{Z}_p \to U_k$ be the canonical surjective diagonal map. Let $\overline{E}_k$ be the closure of ιE_k in U_k and let $H_k^{\rm nr}$ be the p-Hilbert class field of k. By class field theory, $\mathrm{Gal}(H_k^{\rm pr}/k_\infty H_k^{\rm nr}) \simeq \mathrm{tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k) = U_k^*/\overline{E}_k$, where $U_k^* := \{u \in U_k,\ \mathrm{N}_{k/\mathbb{Q}}(u) \in \langle \pm 1 \rangle\}$.

(**c**) Let $\mathscr{C}_k$ be the p-class group of k and let:

$$\mathscr{R}_k := \mathrm{tor}_{\mathbb{Z}_p}(\log(U_k)/\log(\overline{E}_k)) = \log(U_k^*)/\log(\overline{E}_k) \tag{3.1}$$

be the normalized p-adic regulator [7, § 5].

(**d**) The sub-group of $\mathscr{T}_k$ fixing the Bertrandias–Payan field $H_k^{\rm bp}$ is isomorphic to $\mathscr{W}_k$ (the field $H_k^{\rm bp}$ is the compositum of all p-cyclic extensions of k embeddable in p-cyclic extensions of arbitrary large degree).

Recall some classical fundamental results (under Leopoldt's conjecture) that may be found in [3, Corollary III.3.6.3], [7, Lemma 3.1, Corollary 3.2], [13, Définition 2.11, Proposition 2.12], then [18, § 1] or [17], via cohomology:

Proposition 3.1. *We have the exact sequences:*

$$1 \to U_k^*/\overline{E}_k \longrightarrow \mathscr{T}_k \longrightarrow \mathrm{Gal}(k_\infty H_k^{\rm nr}/k_\infty) \simeq \mathscr{C}_k \to 1, \tag{3.2}$$

$$1 \to \mathscr{W}_k \longrightarrow U_k^*/\overline{E}_k \longrightarrow \log(U_k^*)/\log(\overline{E}_k) \simeq \mathscr{R}_k \to 0. \tag{3.3}$$

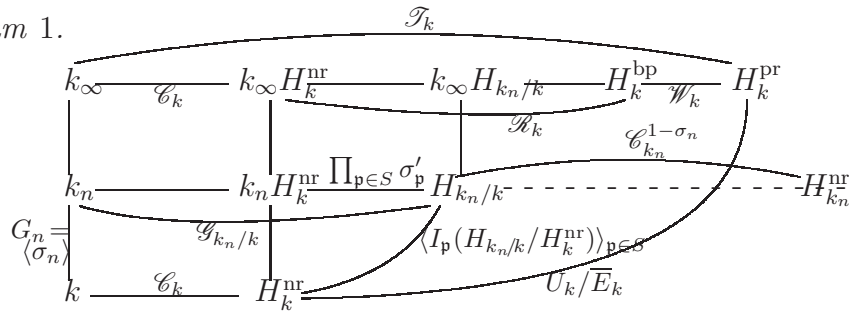
3.2. **Genus theory.** We denote by $H_{k_n}^{\rm nr}$ the p-Hilbert class field of k_n. Since p is totally ramified in k_n/k by convention, the inertia groups $I_{\mathfrak{p}}(k_n/k)$ in k_n/k, $\mathfrak{p} \in S$, are isomorphic to $G_n = {\rm Gal}(k_n/k)$.

Let ω_n be the map which associates with $\varepsilon \in E_k$ the family of Hasse's symbols $\left(\frac{\varepsilon\,,\,k_n/k}{\mathfrak{p}}\right) \in G_n$, $\mathfrak{p} \in S$. This yields the genus exact sequence interpreting the product formula of the Hasse symbols [3, Corollary IV.4.4.1]:

$$1 \to E_k/E_k \cap {\rm N}_{k_n/k}(k_n^\times) \xrightarrow{\omega_n} \Omega(k_n/k) \xrightarrow{\pi_n} {\rm Gal}(H_{k_n/k}/k_n H_k^{\rm nr}) \to 1,$$

where $\Omega(k_n/k) := \left\{(\sigma_{\mathfrak{p}})_{\mathfrak{p}\in S} \in G_n^{\#S},\ \prod_{\mathfrak{p}\in S}\sigma_{\mathfrak{p}} = 1\right\} \simeq G_n^{\#S-1}$, then where $H_{k_n/k}$ is *the p-genus field* of k_n/k defined as the maximal sub-extension of $H_{k_n}^{\rm nr}$, abelian over k. The image of ω_n is contained in $\Omega(k_n/k)$ and the map π_n is defined as follows: with $(\sigma_{\mathfrak{p}})_{\mathfrak{p}\in S} \in G_n^{\#S}$, π_n associates the product of the extensions $\sigma'_{\mathfrak{p}}$ of the $\sigma_{\mathfrak{p}}$ in the inertia groups $I_{\mathfrak{p}}(H_{k_n/k}/H_k^{\rm nr})$ generating ${\rm Gal}(H_{k_n/k}/H_k^{\rm nr})$; from the product formula, if $(\sigma_{\mathfrak{p}})_{\mathfrak{p}\in S} \in \Omega(k_n/k)$, then $\prod_{\mathfrak{p}\in S}\sigma'_{\mathfrak{p}}$ fixes both $H_k^{\rm nr}$ and k_n, whence $k_n H_k^{\rm nr}$. The genus exact sequence shows that the kernel of π_n is $\omega_n(E_k)$.

Diagram 1.



We have, using Chevalley's ambiguous class number formula [2, p. 402]:

$$\#\mathscr{G}_{k_n/k} = \#{\rm Gal}(H_{k_n/k}/k_n) = \frac{\#\mathscr{C}_{k_n}}{\#\mathscr{C}_{k_n}^{1-\sigma_n}} = \#\mathscr{C}_k \cdot \frac{p^{n\cdot(\#S-1)}}{(E_k : E_k \cap {\rm N}_{k_n/k}(k_n^\times))} \tag{3.4}$$

In the Diagram, the genus field $H_{k_n/k}$ is the fixed field of the image of $\mathscr{C}_{k_n}^{1-\sigma_n}$, where $\mathscr{G}_{k_n/k} = {\rm Gal}(H_{k_n/k}/k_n)$ is the genus group in k_n/k.

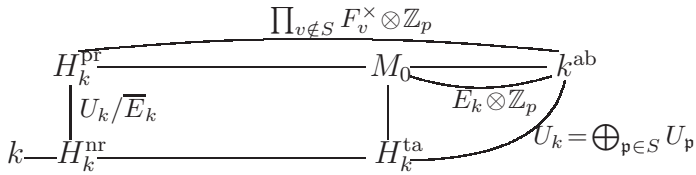
3.3. **Groups $\mathscr{R}_k^{\rm nr}$, $\mathscr{R}_k^{\rm ram}$ – Ramification in $H_k^{\rm pr}/k_\infty$.** The genus group $\mathscr{G}_{k_n/k}$ has, in our context, the following main property that will give Theorem 3.4 when n is large enough:

Lemma 3.2. *For all $n \geq 0$, $k_\infty H_{k_n/k} \subseteq H_k^{\rm bp}$. Then $\#\mathscr{G}_{k_n/k} \,\big|\, \#\mathscr{C}_k \cdot \mathscr{R}_k$, which is equivalent (using formula (3.4)) to $\dfrac{p^{n\cdot(\#S-1)}}{(E_k : E_k \cap {\rm N}_{k_n/k}(k_n^\times))} \,\Big|\, \#\mathscr{R}_k$.*

Proof. Indeed, using the idelic global reciprocity map (under Leopoldt's conjecture), we have the fundamental diagram [3, § III.4.4.1] of the Galois group of the maximal abelian pro-p-extension $k^{\rm ab}$ of k, with our present notations,

where F_v is the residue field of the tame place v (finite or infinite) and where $H_k^{\rm ta}$ is the maximal tame sub-extension of $k^{\rm ab}$. The fixed field of $U_k = \bigoplus_{\mathfrak{p}\in S} U_\mathfrak{p}$ is $H_k^{\rm ta}$ since each $U_\mathfrak{p}$ is the inertia group of $\mathfrak{p}$ in $k^{\rm ab}/k$. Thus, $\mathrm{tor}_{\mathbb{Z}_p}(U_\mathfrak{p}) = \mu_\mathfrak{p}$, restricted to $\mathrm{Gal}(H_k^{\rm pr}/k)$, fixes k_∞ and since $k_\infty H_{k_n/k}/k_\infty$ is unramified, it fixes $k_\infty H_{k_n/k}$ for all $n \geq 0$.

Diagram 2.



In Diagram 1, the restriction of $W_k = \bigoplus_{\mathfrak{p}\in S} \mu_\mathfrak{p}$ to $\mathrm{Gal}(H_k^{\rm pr}/H_k^{\rm nr})$ is isomorphic to $W_k/\mu_k = \mathscr{W}_k$ whose fixed field is $H_k^{\rm bp}$; whence the first claim.

The second one is obvious since non-ramification propagates. Then $\#\mathscr{G}_{k_n/k}$ increases with n and stabilizes at a divisor of $[H_k^{\rm bp} : k_\infty] = \#\mathscr{C}_k \cdot \#\mathscr{R}_k$. □

Put $\mathscr{G}_k \simeq \mathscr{G}_{k_n/k}$ for n large enough. This group is called the genus group of k_∞/k; then the field $H_k^{\rm gen} := \bigcup_m H_{k_m/k}$ (the genus field of k_∞/k) is unramified over k_∞ of Galois group $\mathscr{G}_k$. We can state more precisely:

Theorem 3.3. *Let $n_0 \geq 0$ be such that $\#\mathscr{G}_{k_{n_0}/k}$ stabilizes, definig the genus field $H_k^{\rm gen}$ such that $\mathrm{Gal}(H_k^{\rm gen}/k_\infty) = \mathscr{G}_k$. Then $H_k^{\rm gen}$ is the maximal unramified extension of k_∞ in $H_k^{\rm pr}$ and $\mathrm{Gal}(H_k^{\rm pr}/H_k^{\rm gen}) \simeq \big\langle \mathrm{tor}_{\mathbb{Z}_p}(U_\mathfrak{p}\overline{E}_k/\overline{E}_k) \big\rangle_{\mathfrak{p}\in S}$.*

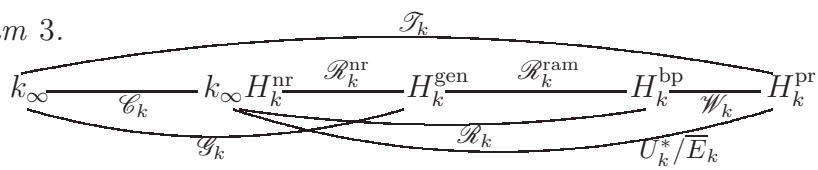
Proof. To simplify, put $L_\infty := H_k^{\rm gen}$. Let L'_∞ be a degree p unramified extension of L_∞ in $H_k^{\rm bp}$; put $L = H_{k_n/k}$, $n \geq n_0$, and consider L' such that $L' \cap L_\infty = L$ and $L'L_\infty = L'_\infty$; thus $\mathrm{Gal}(L_\infty/L) \simeq \mathrm{Gal}(L'_\infty/L') \simeq \mathbb{Z}_p$. Taking $n \gg n_0$, one may assume that L_∞/L and L'_∞/L' are totally ramified at p.

Let $M \neq L'$ be a degree p extension of L in L'_∞ and v a p-place of L; if v was unramified in M/L, the non-ramification would propagate over L' in L'_∞ (a contradiction). Thus, the inertia group of v in L'_∞/L is necessarily $\mathrm{Gal}(L'_\infty/L)$ or $\mathrm{Gal}(L'_\infty/L')$, but this last case for all v gives $L'/L/k_n$ unramified and L'/k abelian (absurd by definition of the genus field $L = H_{k_n/k}$); so there exists v_0 totally ramified in L'_∞/L, hence in L'_∞/L_∞ (absurd).

For $\mathfrak{p} \in S$, the inertia group $I_\mathfrak{p}(H_k^{\rm pr}/k_\infty)$ is isomorphic to the torsion part, $\mathrm{tor}_{\mathbb{Z}_p}(U_\mathfrak{p}\overline{E}_k/\overline{E}_k)$, of the image of $U_\mathfrak{p}$ in $U_k/\overline{E}_k$. □

Let $\mathscr{R}_k^{\rm nr} := \mathrm{Gal}(H_k^{\rm gen}/k_\infty H_k^{\rm nr})$, $\mathscr{R}_k^{\rm ram} := \mathrm{Gal}(H_k^{\rm bp}/H_k^{\rm gen})$. The top of Diagram 1 may be specified as follows (with $H_k^{\rm pr}/H_k^{\rm gen}$ totally ramified at p):

Diagram 3.



From Lemma 3.2, formula (3.4) and the above study, we can state (a generalization of Taya analytic viewpoint [21, Theorem 1.1]):

Theorem 3.4. *Let $n \gg 0$ be such that $\mathscr{G}_{k_n/k} := \mathrm{Gal}(H_{k_n/k}/k_n) \simeq \mathscr{G}_k$. Then $\#\mathscr{G}_k = \#\mathscr{C}_k \cdot \#\mathscr{R}_k^{\mathrm{nr}} = \mathscr{C}_{k_n}^{G_n}$, equivalent to $\dfrac{p^{n\cdot(\#S-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))} = \#\mathscr{R}_k^{\mathrm{nr}}$.*

4. Filtration of $\mathscr{C}_{k_n}$ – Class and Norm factors

Describe now a formal algorithm of computation of $\#\mathscr{C}_{k_n}$, for all $n \geq 0$, by means of "unscrewing" in k_n/k. For this, put $G_n := \mathrm{Gal}(k_n/k) =: \langle\, \sigma_n \,\rangle$. Let I_{k_n} be the group of prime-to-p ideals of k_n.

4.1. **Filtration of the class groups.** One uses the filtration of $M_n := \mathscr{C}_{k_n}$ defined as follows [4, Corollary 3.7]. For $n \geq 0$ fixed, $(M_n^i)_{i\geq 0}$ is the i-sequence of sub-G_n-modules of M_n defined by $M_n^0 := 1$ and $M_n^{i+1}/M_n^i := (M_n/M_n^i)^{G_n}$, for $0 \leq i \leq b_n$, where b_n is the least integer i such that $M_n^i = M_n$ (i.e., such that $M_n^{i+1} = M_n^i$).

If $\mathscr{C}_k = 1$, $M_0 = M_0^0 = 1$, $b_0 = 0$; if $\mathscr{C}_k \neq 1$, $M_0 = M_0^1 = \mathscr{C}_k$, $b_0 = 1$.

We will obtain, inductively, ideal groups $J_n^i \subset I_{k_n}$, with $J_n^0 = 1$, such that:

$$M_n^i =: \mathscr{cl}_{k_n}(J_n^i), \text{ for all } i \geq 0.$$

Proposition 4.1. *This filtration has the following properties:*

(i) From $M_n^0 = 1$, one gets $M_n^1 = M_n^{G_n}$ of order $\#\mathscr{C}_k \cdot \dfrac{p^{n\cdot(\#S-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))}$.

(ii) One has $M_n^i = \{c \in M_n,\ c^{(1-\sigma_n)^i} = 1\}$, for all $i \geq 0$.

(iii) The i-sequence $\#(M_n^{i+1}/M_n^i)$, $0 \leq i \leq b_n$, is decreasing to 1 and is bounded by $\#M_n^1$ since $1 - \sigma_n$ defines the injections $M_n^{i+1}/M_n^i \hookrightarrow M_n^i/M_n^{i-1}$.

(iv) $\#M_n = \#M_n^{b_n} = \prod_{i=0}^{b_n-1} \#(M_n^{i+1}/M_n^i)$.

In [4, Formula (29), § 3.2], we established a generalization of Chevalley's ambiguous class number formula, by means of the norm groups $\mathrm{N}_{k_n/k}(M_n^i) = \mathscr{cl}_k(\mathrm{N}_{k_n/k}(J_n^i))$ and the subgroups $\Lambda_n^i := \{x \in k^\times,\ (x) \in \mathrm{N}_{k_n/k}(J_n^i)\}$ of $k^\times$, giving $\#\big(M_n^{i+1}/M_n^i\big) = \dfrac{\#\mathscr{C}_k}{\#\mathrm{N}_{k_n/k}(M_n^i)} \cdot \dfrac{p^{n\cdot(\#S-1)}}{(\Lambda_n^i : \Lambda_n^i \cap \mathrm{N}_{k_n/k}(k_n^\times))}$, where:

$$\frac{\#\mathscr{C}_k}{\#\mathrm{N}_{k_n/k}(M_n^i)} \quad \& \quad \frac{p^{n\cdot(\#S-1)}}{(\Lambda_n^i : \Lambda_n^i \cap \mathrm{N}_{k_n/k}(k_n^\times))} \tag{4.1}$$

are integers called *the class factor* and *the norm factor*, respectively, at the step i of the algorithm in the layer k_n. These factors are independent of the choice of the ideals defining J_n^i up to principal ideals of k_n and the groups Λ_n^i are, therefore, defined up to elements of $\mathrm{N}_{k_n/k}(k_n^\times)$.

From Lemma 3.2 and Diagram 3, we can state, for any fixed integer n and for the class and norm factors (4.1):

Corollary 4.2. *The class factors divide $\#\mathscr{C}_k$ and define a decreasing i-sequence since $\mathrm{N}_{k_n/k}(M_n^i) \subseteq \mathrm{N}_{k_n/k}(M_n^{i+1})$ for all $i \geq 0$. The norm factors divide $\#\mathscr{R}_k^{\mathrm{nr}}$ and define a decreasing i-sequence for all $i \geq 0$, due to the injective maps $E_k/E_k \cap \mathrm{N}_{k_n/k}(k_n^\times) \hookrightarrow \cdots \Lambda_n^i/\Lambda_n^i \cap \mathrm{N}_{k_n/k}(k_n^\times) \hookrightarrow \Lambda_n^{i+1}/\Lambda_n^{i+1} \cap \mathrm{N}_{k_n/k}(k_n^\times) \cdots$*

4.2. **Relation of the algorithms with Iwasawa's theory.** The subgroups J_n^i of I_{k_n} are built inductively from $J_n^0 = 1$, hence $\Lambda_n^0 = E_k$. More precisely the algorithm is the following, for n and i fixed [5, § 6.2]:

Let $x \in \Lambda_n^i$, $(x) = \mathrm{N}_{k_n/k}(\mathfrak{A})$, $\mathfrak{A} \in J_n^i$; thus x is local norm on the tame places. Suppose that x is local norm on S, hence global norm and we can write $x = \mathrm{N}_{k_n/k}(y)$, $y \in k_n^\times$. The random aspects occur, from the relation $\mathrm{N}_{k_n/k}(y) = \mathrm{N}_{k_n/k}(\mathfrak{A})$, in the mysterious "evolution relation" giving the existence of an ideal $\mathfrak{B} \in I_{k_n}$ such that $(y) = \mathfrak{A}\,\mathfrak{B}^{1-\sigma_n}$. Remark that for $\mathrm{N}(y) = 1$ and $y = b^{1-\sigma_n}$, b is given by an *additive Hilbert's resolvent*.

A priori there is no algebraic link with the previous data because of the global solution y (Hasse's norm theorem) unique up to $k_n^{\times 1-\sigma_n}$; this gives $\mathfrak{B}$ up to principal ideals. All numbers $x \in \Lambda_n^i \cap \mathrm{N}_{k_n/k}(k_n^\times)$ define the step $i+1$:

$$J_n^{i+1} := J_n^i \cdot \langle \ldots, \mathfrak{B}, \ldots \rangle \text{ and } \Lambda_n^{i+1} := \{x \in k^\times,\ (x) \in \mathrm{N}_{k_n/k}(J_n^{i+1})\}.$$

Therefore, for $i = b_n$ we obtain $M_n^{b_n} = \mathscr{C}_{k_n}$, $\mathrm{N}_{k_n/k}\big(M_n^{b_n}\big) = \mathscr{C}_k$ and $(\Lambda_n^{b_n} : \Lambda_n^{b_n} \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(\#S-1)}$, which explains that $\#\mathscr{C}_{k_n}$ essentially depends on the number of steps b_n of the algorithm; this is expressed in terms of Iwasawa invariants as follows:

Theorem 4.3. *We assume the Conventions 1.1 for the base field k and recall that $\mathscr{R}_k^{\mathrm{nr}} := \mathrm{Gal}(H_k^{\mathrm{gen}}/k_\infty H_k^{\mathrm{nr}})$ (Diagram 3), where H_k^{gen} is the genus field of k_∞/k (Theorem 3.3). Let b_n be the length of the algorithm in the layer k_n. Then (where v_p denotes the p-adic valuation):*

(i) $b_n \leq \lambda \cdot n + \mu \cdot p^n + \nu \leq v_p(\#\mathscr{C}_k \cdot \#\mathscr{R}_k^{\mathrm{nr}}) \cdot b_n$, for all $n \geq 0$. So, $\lambda = \mu = 0 \iff b_n$ bounded.

(ii) $b_m \geq b_n$, for all $m \geq n \geq 0$.

(iii) $b_1 = 0 \iff \lambda = \mu = \nu = 0 \iff b_n = 0$ for all $n \iff \mathscr{C}_k = \mathscr{R}_k^{\mathrm{nr}} = 1$.

Proof. Let $M_n := \mathscr{C}_{k_n}$, for all $n \geq 0$.

(i) As $\#\big(M_n^{i+1}/M_n^i\big) \geq p$, for $0 \leq i \leq b_n - 1$, Proposition 4.1 (iv) implies $\#M_n = \#M_n^{b_n} \geq p^{b_n}$; whence $b_n \leq \lambda \cdot n + \mu \cdot p^n + \nu$.

From the fact that $\#\big(M_n^{i+1}/M_n^i\big) \mid \#\mathscr{C}_k \cdot \#\mathscr{R}_k^{\mathrm{nr}}$ (Corollary 4.2) this yields $\#\big(M_n^{i+1}/M_n^i\big) \leq \#\mathscr{C}_k \cdot \#\mathscr{R}_k^{\mathrm{nr}}$ for $0 \leq i \leq b_n - 1$, whence $\#\mathscr{C}_{k_n} \leq (\#\mathscr{C}_k \cdot \#\mathscr{R}_k^{\mathrm{nr}})^{b_n}$ from Proposition 4.1 (iv); hence the second inequality and the second claim.

(ii) By definition, $M_m^{b_m} = M_m$ with b_m minimal. Since k_m/k_n is totally ramified, $\mathrm{N}_{k_m/k_n}(M_m^{b_m}) = M_n$, but $\mathrm{N}_{k_m/k_n}(M_m^{b_m}) \subseteq M_n^{b_m}$ (Proposition 4.1 (ii)), whence $M_n \subseteq M_n^{b_m}$, thus $M_n^{b_m} = M_n$, proving the claim.

(iii) So $b_1 = 0$ implies $b_0 = 0$, whence $\lambda + \mu p + \nu = \mu + \nu = 0$ yielding $\lambda = \mu = 0$ and $\nu = 0$; then (i) implies $b_n = 0$ for all $n \geq 0$, in other words, $\mathscr{C}_{k_n} = 1$ for all $n \geq 0$; thus, taking $n \gg 0$ to apply Theorem 3.4 yields $\mathscr{G}_{k_n/k} = \mathscr{C}_{k_n}^{G_n} = 1$, whence $\mathscr{C}_k = \mathscr{R}_k^{\rm nr} = 1$ (reciprocals obvious). □

Corollary 4.4. *(a) Under Conventions 1.1, $\lambda = \mu = 0$ (equivalent to b_n bounded) is equivalent to each of the following properties:*

(i) $\mathrm{N}_{k_n/k} : \mathscr{C}_{k_n} \to \mathscr{C}_k$ is an isomorphisms for all $n \geq 0$.

(ii) $\#\mathscr{C}_{k_n}^{G_n} = \#\mathscr{C}_{k_n} = \#\mathscr{C}_k$, for all $n \geq 0$.

(iii) $\mathscr{C}_{k_n}^{G_n} = \mathscr{C}_{k_n}$, for all $n \geq 0$ and $\mathscr{R}_k^{\rm nr} = 1$.

(b) Let k_{n_1}, still denoted k, be such that b_n is constant for all $n \geq n_1$;[2] *for this new base field k and the new b-function, $b_n \leq 1$, for all $n \geq 0$.*

Proof. Proof of (a). (i) Under the condition $\lambda = \mu = 0$, $\#\mathscr{C}_{k_n} = \#\mathscr{C}_k = p^\nu$ for all n, and all the (surjective) norm maps are isomorphisms.

(ii) Chevalley's formula $\#\mathscr{C}_{k_n}^{G_n} = \#\mathscr{C}_k \cdot \frac{p^{n\cdot(\#S-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))} \leq \#\mathscr{C}_{k_n} = \#\mathscr{C}_k$ yields $\#\mathscr{C}_{k_n}^{G_n} = \#\mathscr{C}_{k_n} = \#\mathscr{C}_k$ and $\frac{p^{n\cdot(\#S-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))} = 1$, for all $n \geq 0$.

(iii) From (ii), $\mathscr{R}_k^{\rm nr} = 1$, taking $n \gg 0$ to apply Theorem 3.4.

In the three cases, the reciprocals are obvious.

Proof of (b). Consider the second step of the algorithm in k_n (we exclude the case $b_n = 0$ where all class groups are trivial); the class factor for $\mathscr{C}_{k_n}^2/\mathscr{C}_{k_n}^1$ is trivial since $\mathrm{N}_{k_n/k}(\mathscr{C}_{k_n}^{G_n}) = \mathscr{C}_k$ (from (i), (ii)) and the norm factor, as divisor of $\mathscr{R}_k^{\rm nr}$, is also trivial (from (iii)); whence $b_n = 1$ for all $n \geq 0$. □

Note that under Greenberg's conjecture, in $\frac{p^{n\cdot(\#S-1)}}{(\Lambda_n^1 : \Lambda_n^1 \cap \mathrm{N}_{k_n/k}(k_n^\times))}$, we have $\Lambda_n^1 = \{x \in k^\times,\ (x) = \mathrm{N}_{k_n/k}(\mathfrak{A}), \mathfrak{A} \in J_n^1\}$ where $\mathscr{A}_{k_n}(J_n^1) = \mathscr{C}_{k_n}^{G_n}$; thus, norms being isomorphisms, $(x) = \mathrm{N}_{k_n/k}(\mathfrak{A})$ implies that $\mathfrak{A} = (\alpha)$, $\alpha \in k_n^\times$, so that $\Lambda_n^1 = E_k\, \mathrm{N}_{k_n/k}(k_n^\times)$, showing that the algorithm becomes trivial.

4.3. **The n-sequences $(\mathscr{C}_{k_n}/\mathscr{C}_{k_n}^i)^{G_n}$.** We fix the step i of the algorithms. For now, we do not assume the Conventions 1.1. For all $m \geq n \geq 0$, the norm maps N_{k_m/k_n} on M_m and $M_m^{(1-\sigma_m)^i}$ are surjective (they are, a priori, not injective nor surjective on the kernels M_m^i of the maps $M_m \to M_m^{(1-\sigma_m)^i}$). This leads to the following result (see [5, Lemmas 7.1, 7.2] for the details), giving another approach of the conjecture:

Theorem 4.5. *For all $i \geq 0$ fixed, $\left\{\#\left(M_n^{i+1}/M_n^i\right)\right\}_n$ defines an increasing n-sequence of divisors of $\#\mathscr{C}_k \cdot \#\mathscr{R}_k^{\rm nr}$. Thus $\lim_{n\to\infty} \#\left(M_n^{i+1}/M_n^i\right) =: p^{c^i} p^{\rho^i}$. The*

[2] On must note that for each change of base field in the tower, the Iwasawa invariants are given by Conventions 1.1, and the algorithms are distinct; for instance the parameter b_n defines a new function of the nth layer of the new k (in the meaning $[k_n : k] = p^n$).

i-sequences p^{c^i} and p^{ρ^i} are decreasing, stationary at a divisor p^c of $\#\mathscr{C}\!\ell_k$ and p^ρ of $\#\mathscr{R}_k^{\rm nr}$, respectively. Greenberg's conjecture is equivalent to $c=\rho=0$.

5. $\mathscr{T}_k$ as governing invariant of the algorithms

The ideals $\mathfrak{A}\in J_n^i$ may be arbitrarily modified up to principal ideals of k_n, whence $\mathrm{N}_{k_n/k}(\mathfrak{A})$ defined up to elements of $\mathrm{N}_{k_n/k}(k_n^\times)$, as well as Λ_n^i. We intend to obtain suitable *finite sets* of representatives of these ideal norms, independently of n, more precisely of cardinality $\leq \#\mathscr{T}_k$.

5.1. **Decomposition of $\mathrm{N}_{k_n/k}(\mathfrak{A})$ – The fundamental ideals $\mathfrak{t}$.** Let $H_k^{\rm pr}$ and $H_{k_n}^{\rm pr}$ be the maximal abelian p-ramified pro-p-extensions of k and k_n, respectively. Let F be an extension of $H_k^{\rm nr}$ such that $H_k^{\rm pr}$ be the direct compositum of F and $k_\infty H_k^{\rm nr}$ over $H_k^{\rm nr}$ (possible because $k_\infty\cap H_k^{\rm nr}=k$ due to the total ramification of p in k_∞/k); we put $\Gamma=\mathrm{Gal}(H_k^{\rm pr}/F)\simeq\mathbb{Z}_p$.

In the same way, we fix an extension F_n of F such that $H_{k_n}^{\rm pr}$ be the direct compositum of F_n and $H_k^{\rm pr}$ over k_nF; we put $\Gamma_n=\mathrm{Gal}(H_{k_n}^{\rm pr}/F_n)\simeq\Gamma^{p^n}$. We have $F=F_0\subset F_1\subset\cdots\subset F_n\subset F_{n+1}\subset\cdots$ (see Diagram 4 hereafter).

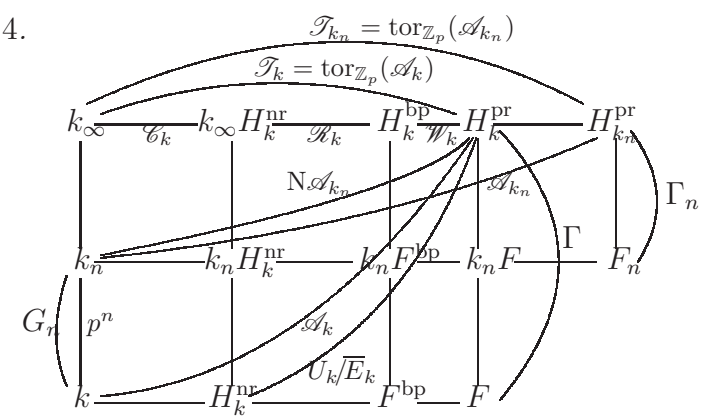
In what follows, we systematically use the flatness of $\mathbb{Z}_p$.

Consider the Artin symbols $\left(\frac{H_k^{\rm pr}/k}{\cdot}\right)$ and $\left(\frac{H_{k_n}^{\rm pr}/k_n}{\cdot}\right)$, defined on $I_k\otimes\mathbb{Z}_p$ and $I_{k_n}\otimes\mathbb{Z}_p$, respectively. Their images are the Galois groups $\mathscr{A}_k$ (resp. $\mathscr{A}_{k_n}$); their kernels are the groups of infinitesimal principal ideals $\mathscr{P}_{k,\infty}$ (resp. $\mathscr{P}_{k_n,\infty}$), where $\mathscr{P}_{k,\infty}$ is the set of ideals (x_∞), $x_\infty\in k'^\times\otimes\mathbb{Z}_p$, such that $\iota x_\infty=1$ in U_k (idem for $\mathscr{P}_{k_n,\infty}$) [3, Theorem III.2.4, Proposition III.2.4.1].

The arithmetic norm (or restriction of automorphisms), in k_n/k, leads to $\mathrm{N}_{k_n/k}(\mathscr{A}_{k_n})=\mathrm{Gal}(H_k^{\rm pr}/k_n)$ and $\mathrm{N}_{k_n/k}(\mathscr{T}_{k_n})=\mathscr{T}_k$ since $k_{n\infty}=k_\infty$. The fixed points formula $\mathscr{T}_{k_n}^{G_n}\simeq\mathscr{T}_k$ ([3, Theorem IV.3.3], [11, Section 2 (c)]), implies $\mathrm{Ker}(\mathrm{N}_{k_n/k})=\mathscr{T}_{k_n}^{1-\sigma_n}=\mathrm{Gal}(H_{k_n}^{\rm pr}/H_k^{\rm pr})$.

We denote by $\mathscr{K}_\infty^\times\subset k'^\times\otimes\mathbb{Z}_p$ the subgroup of infinitesimal elements of k (idem for $\mathscr{K}_{n,\infty}^\times\subset k_n'^\times\otimes\mathbb{Z}_p$). In the sequel, the notations x_∞, $y_\infty,\ldots$ always denote such infinitesimal elements.

Diagram 4.



Lemma 5.1. *If* $(x_\infty) \in \mathscr{P}_{k,\infty} \cap \mathrm{N}_{k_n/k}(I_{k_n} \otimes \mathbb{Z}_p)$, *then* $x_\infty \in \mathrm{N}_{k_n/k}(\mathscr{K}_{n,\infty}^\times)$.

Proof. The assumption implies that x_∞ is everywhere local norm in k_n/k, whence $x_\infty = \mathrm{N}_{k_n/k}(y)$, $y \in k_n'^\times \otimes \mathbb{Z}_p$ (Hasse norm theorem). Thus, we get $\iota \mathrm{N}_{k_n/k}(y) = \mathrm{N}_{k_n/k}(\iota_n y) = 1$ and $\iota_n y = t^{1-\sigma_n}$, $t \in \prod_{\mathfrak{p}_n \in S_n} k_{n,\mathfrak{p}_n}^\times$ (Hilbert's Theorem 90, $\mathrm{H}^1(G_n, \prod_{\mathfrak{p}_n \in S_n} k_{n,\mathfrak{p}_n}^\times) = 1$). Consider t in the profinite completion $\prod_{\mathfrak{p}_n \in S_n} \widehat{k}_{n,\mathfrak{p}_n}^\times$; then one has the exact sequence [11, Chap. 1, § a)]:

$$1 \to \mathscr{K}_{n,\infty}^\times \longrightarrow k_n^\times \otimes \mathbb{Z}_p \xrightarrow{\widehat{\iota}_n} \prod_{\mathfrak{p}_n \in S_n} \widehat{k}_{n,\mathfrak{p}_n}^\times \simeq \mathbb{Z}_p^{\#S} \oplus U_k \to 1.$$

Put $t = \widehat{\iota}_n z$, $z \in k_n^\times \otimes \mathbb{Z}_p$; then $\widehat{\iota}_n y = \widehat{\iota}_n(z^{1-\sigma_n})$, $y = z^{1-\sigma_n}\, y_\infty$, $y_\infty \in \mathscr{K}_{n,\infty}^\times$, then $x_\infty = \mathrm{N}_{k_n/k}(y_\infty)$. We also have $\mathrm{H}^1(G_n, \mathscr{K}_{n,\infty}^\times) = 1$ [11, Lemme 5]. □

The fundamental link between ideal norms in k_n/k and the torsion group $\mathscr{T}_k$ is given, for n large enough, by the following result where the "uniqueness" are relative to the choices of the F_n; we say that some numbers $a \in k'^\times \otimes \mathbb{Z}_p$ (depending on n) are "close to 1" if $\iota a \to 1$ in U_k when $n \to \infty$.

Theorem 5.2. *Let* $n \gg 0$ *fixed and let* $\mathfrak{A} \in I_{k_n} \otimes \mathbb{Z}_p$ *(prime-to-p ideal of* k_n*).*

(i) There exists $\alpha \in k_n'^\times \otimes \mathbb{Z}_p$ *such that* $\mathrm{N}_{k_n/k}(\mathfrak{A}\,(\alpha)) = \mathrm{N}_{k_n/k}(\mathfrak{T}) =: \mathfrak{t}$, *with* $\left(\frac{H_{k_n}^{\mathrm{pr}}/k_n}{\mathfrak{T}}\right) \in \mathscr{T}_{k_n}$, $\left(\frac{H_k^{\mathrm{pr}}/k}{\mathfrak{t}}\right) \in \mathscr{T}_k$ *and* $\iota \mathrm{N}_{k_n/k}(\alpha)$ *close to* 1.

(ii) The representative $\mathfrak{t}$ *of the class* $\mathrm{N}_{k_n/k}(\mathfrak{A}) \cdot \mathrm{N}_{k_n/k}(k_n'^\times \otimes \mathbb{Z}_p)$, *does not depend, modulo* $\mathrm{N}_{k_n/k}(\mathscr{P}_{k_n,\infty})$, *on the tower* $\bigcup_j F_j$.

Proof. (i) From Diagram 4 and the properties of Artin symbols, there exist unique ideals $\mathfrak{T}, \mathfrak{C} \in I_{k_n} \otimes \mathbb{Z}_p$, modulo $\mathscr{P}_{k_n,\infty}$, such that:

$$\mathfrak{A} = \mathfrak{T} \cdot \mathfrak{C} \cdot (y_\infty), \text{ with } \left(\frac{H_{k_n}^{\mathrm{pr}}/k_n}{\mathfrak{T}}\right) \in \mathscr{T}_{k_n},\ \left(\frac{H_{k_n}^{\mathrm{pr}}/k_n}{\mathfrak{C}}\right) \in \Gamma_n,\ y_\infty \in \mathscr{K}_{n,\infty}^\times \tag{5.1}$$

By restriction, the image of Γ_n in Γ is Γ^{p^n}; thus $\mathrm{N}_{k_n/k}(\mathfrak{C}) = \mathfrak{c}^{p^n} \cdot (x_\infty)$ for $\mathfrak{c} \in I_k \otimes \mathbb{Z}_p$ such that $\left(\frac{H_k^{\mathrm{pr}}/k}{\mathfrak{c}}\right) \in \Gamma$ and $x_\infty \in \mathscr{K}_\infty^\times$; but since $H_k^{\mathrm{nr}} \subseteq F$, the ideal $\mathfrak{c}$ is p-principal, thus $\mathfrak{c} = (c)$, $c \in k'^\times \otimes \mathbb{Z}_p$, and then, $\mathrm{N}_{k_n/k}(\mathfrak{C}) = (c^{p^n}) \cdot (x_\infty)$. We have from (5.1):

$$\mathrm{N}_{k_n/k}(\mathfrak{A}) = \mathrm{N}_{k_n/k}(\mathfrak{T}) \cdot (c^{p^n}) \cdot (x_\infty) \cdot \mathrm{N}_{k_n/k}(y_\infty) =: \mathfrak{t} \cdot (c^{p^n}) \cdot (x'_\infty),$$

with $\left(\frac{H_k^{\mathrm{pr}}/k}{\mathfrak{t}}\right) \in \mathscr{T}_k$, $x'_\infty \in \mathscr{K}_\infty^\times$. From Lemma 5.1, since (x'_∞) is norm of ideal in k_n/k, $x'_\infty = \mathrm{N}_{k_n/k}(y'_\infty)$, whence $\mathrm{N}_{k_n/k}\big(\mathfrak{A}\,(c)^{-1}\,(y'_\infty)^{-1}\big) = \mathfrak{t}$.

Let $\alpha = c^{-1}\, y_\infty'^{-1}$; then $\iota \mathrm{N}_{k_n/k}(\alpha) = \iota(c^{-p^n})$ is close to 1.

(ii) Let $\bigcup_j F'_j$ be another tower for Diagram 4; with obvious notations (which depend on n), put $u := \mathrm{N}_{k_n/k}(\alpha)$, $u' := \mathrm{N}_{k_n/k}(\alpha')$, ιu, $\iota u'$ close to 1, we get $\mathrm{N}_{k_n/k}(\mathfrak{A}) \cdot (u) = \mathfrak{t}$, $\mathrm{N}_{k_n/k}(\mathfrak{A}) \cdot (u') = \mathfrak{t}'$. Whence $\mathfrak{t}'\,\mathfrak{t}^{-1} = (a)$, with a close to 1. So, if p^e is the exponent of $\mathscr{T}_k$, we obtain $(a)^{p^e} = (a_\infty) \in \mathscr{P}_{k,\infty}$,

which gives $a^{p^e} = \varepsilon\, a_\infty$, $\varepsilon \in E_k \otimes \mathbb{Z}_p$ with $\iota\varepsilon$ close to 1, hence (for $n \gg 0$) of the form $\varepsilon = \eta^{p^e}$, $\eta \in E_k \otimes \mathbb{Z}_p$, with $\iota\eta$ close to 1 (from Leopoldt's conjecture [3, Theorem III.3.6.2 (iv)]). This yields $(a\,\eta^{-1})^{p^e} = a_\infty$ and we get $\iota(a\,\eta^{-1}) = \xi \in W_k = \mathrm{tor}_{\mathbb{Z}_p}(U_k)$; both ιa and $\iota\eta$ are close to 1, thus $\xi = 1$ and $a\,\eta^{-1} = a'_\infty$ giving $\mathfrak{t}'\,\mathfrak{t}^{-1} = (a'_\infty) \in \mathrm{N}_{k_n/k}(\mathscr{P}_{k_n,\infty})$, using Lemma 5.1 □

5.2. **Images in $\mathscr{C}_k$ and $\mathscr{R}_k$ of the ideals $\mathfrak{t}$ – Conjecture.** We choose, once for all, a set $\mathbf{T}_k = \left\{ \mathfrak{t}_\ell \right\}_{1 \le \ell \le \#\mathscr{T}_k}$, of ideals $\mathfrak{t}_\ell \in I_k \otimes \mathbb{Z}_p$ whose Artin symbols describe $\mathscr{T}_k$ isomorphic to $\mathbf{T}_k \cdot \mathscr{P}_{k,\infty}/\mathscr{P}_{k,\infty}$.

The ideals $\mathrm{N}_{k_n/k}(\mathfrak{A}(\alpha)) = \mathfrak{t} \in \mathbf{T}_k$, well-defined modulo $\mathrm{N}_{k_n/k}(\mathscr{P}_{k_n,\infty})$, play the following roles in the evolution of the class and norm factors:

(i) *Class factors and* $\mathbf{T}_k$. The ideal groups $\mathrm{N}_{k_n/k}(J_n^i)$, representing the class groups $\mathrm{N}_{k_n/k}(M_n^i)$ as denominator of the class factors, are generated, modulo principal ideals (a), $a \in \mathrm{N}_{k_n/k}(k_n'^{\times} \otimes \mathbb{Z}_p)$, by ideals $\mathfrak{t}^i \in \mathbf{T}_k$.

(ii) *Norm factors and* $\mathbf{T}_k$. The groups $\Lambda_n^i = \{x \in k^\times, (x) \in \mathrm{N}_{k_n/k}(J_n^i)\}$, giving the norm factors, are obtained, modulo elements of $\mathrm{N}_{k_n/k}(k_n'^{\times} \otimes \mathbb{Z}_p)$, via principal ideals $(\tau) \in \mathbf{T}_k$ (hence τ is local norm at the tame places in k_n/k and its norm properties only depend on S).

Put $\mathbf{T}_k^{\mathrm{ppl}} := \{\mathfrak{t} \in \mathbf{T}_k,\ \mathfrak{t} = (\tau)\}$; the subgroup $\mathbf{T}_k^{\mathrm{ppl}} \cdot \mathscr{P}_{k,\infty}/\mathscr{P}_{k,\infty}$, is isomorphic to $\mathrm{Gal}(H_k^{\mathrm{pr}}/k_\infty H_k^{\mathrm{nr}})$. Let $\mathfrak{t} = (\tau) \in \mathbf{T}_k^{\mathrm{ppl}}$; so we have $\left(\frac{H_k^{\mathrm{pr}}/k}{\mathfrak{t}}\right) \in \mathrm{Gal}(H_k^{\mathrm{pr}}/k_\infty H_k^{\mathrm{nr}}) \simeq U_k^*/\overline{E}_k$. This yields $\tau^{p^e} = \varepsilon\, x_\infty$, $\varepsilon \in E_k \otimes \mathbb{Z}_p$; whence $\iota \mathrm{N}_{k/\mathbb{Q}}(\tau) = \pm 1$ and the image of $\iota\tau$ modulo $\overline{E}_k$ is defined in $U_k^*/\overline{E}_k$. We consider the image of $\log(\iota\tau)$ in $\log(U_k^*)/\log(\overline{E}_k) = \mathscr{R}_k$, which defines $\log(\mathfrak{t}) := \log(\iota\tau) \pmod{\log(\overline{E}_k)}$. We have $W_k = \mathrm{Ker}(\log)$, and this gives again the exact sequence (3.3).

Remark 5.3. Let $(\tau) \in \mathbf{T}_k^{\mathrm{ppl}}$; choosing a representative of τ modulo $\mathscr{K}_\infty^\times$ one may always assume that $(\tau) = \mathrm{N}_{k_n/k}(\mathfrak{T})$, $\mathfrak{T} \in I_{k_n} \otimes \mathbb{Z}_p$, since $\mathrm{N}(\mathscr{T}_{k_n}) = \mathscr{T}_k$ (whence τ local norm at the tame places). Suppose that the image of $\iota\tau$ in $\mathrm{tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k)$ is in the subgroup $\mathrm{Gal}(H_k^{\mathrm{pr}}/H_k^{\mathrm{gen}})$ generated by the inertia groups $\mathrm{tor}_{\mathbb{Z}_p}(U_{\mathfrak{p}}\overline{E}_k/\overline{E}_k)$, $\mathfrak{p} \in S$; then τ is local norm on S. Indeed, let $\iota\tau = u = (u_{\mathfrak{p}}, 1, \ldots, 1)$; u is local norm at each $\mathfrak{p}' \ne \mathfrak{p}$, whence a global norm (product formula). This explains that generators τ of ideals $\mathfrak{t} \in \mathbf{T}_k^{\mathrm{ppl}}$, whose images are in $\mathrm{Gal}(H_k^{\mathrm{pr}}/H_k^{\mathrm{gen}})$, do not modify any norm factor, only depending on the image in $\mathscr{R}_k^{\mathrm{nr}} = \mathrm{Gal}(H_k^{\mathrm{gen}}/k_\infty H_k^{\mathrm{nr}})$.

5.3. **The algorithm in terms of fundamental ideals $\mathfrak{t}$.** We still assume Conventions 1.1 to the base field k. In this subsection, we consider the layer $K = k_n$ (with $p^n \gg p^e$, the exponent of $\mathscr{T}_k$) and, to simplify, we delete indices n (e.g., $M_n^i \to M^i$, $\Lambda_n^i \to \Lambda^i$, $\mathrm{N}_{k_n/k} \to \mathrm{N}$, $b_n \to b$ (number of steps in K)); then uppercase (respectively lowercase) letters for ideals are reserved to K (respectively k).

From Theorem 5.2 (i) and for any prime-to-p ideals $\mathfrak{A} \in J^i$, defining M^i, there exist $\alpha \in K'^{\times} \otimes \mathbb{Z}_p$ and $\mathfrak{T}$ of finite order modulo $\mathscr{P}_{K,\infty}$, such that $\mathrm{N}(\mathfrak{A}\,(\alpha)) = \mathrm{N}(\mathfrak{T}) =: \mathfrak{t} \in \mathbf{T}_k$ with $\mathrm{N}(\alpha)$ close to 1. Denote by $\mathbf{\Sigma}^i_K$, the set of such representatives $\mathfrak{T}^i$ and let $\mathbf{\Sigma}^i_k$ be the set of $\mathfrak{t}^i := \mathrm{N}(\mathfrak{T}^i)$; so:

$$\mathrm{N}(\mathbf{\Sigma}^i_K) = \mathbf{\Sigma}^i_k, \quad \mathrm{N}(M^i) = \mathscr{cl}_k\langle \mathbf{\Sigma}^i_k\rangle, \quad \mathbf{\Sigma}^i_k \subseteq \mathbf{T}_k. \tag{5.2}$$

Replacing $\mathfrak{A}$ by $\mathfrak{A}\,(\alpha)$ does not modify the class and norm factors (4.1) since $\mathscr{cl}_k(\mathrm{N}(\mathfrak{A})) = \mathscr{cl}_k(\mathfrak{t})$ and, if $\mathrm{N}(\mathfrak{A})$ is principal, then $\mathfrak{t} = (\tau)$ is equal to $\mathrm{N}(\mathfrak{A})$ up to $\mathrm{N}(K^{\times} \otimes \mathbb{Z}_p)$, which does not modify the norm properties in Λ^i. Then, in $\Lambda^i = \{\tau \in k'^{\times} \otimes \mathbb{Z}_p,\ (\tau) \in \langle \mathbf{\Sigma}^i_k\rangle\}$, one must find all elements τ^i (by definition of the form $\mathrm{N}(\mathfrak{T}^i)$, $\mathfrak{T}^i \in \langle \mathbf{\Sigma}^i_K\rangle$), such that τ^i is local norm on S in K/k, thus of the form $\mathrm{N}(y^i)$, $y^i \in K'^{\times} \otimes \mathbb{Z}_p$; so the algorithm continues, from $\mathrm{N}(y^i) = \mathrm{N}(\mathfrak{T}^i)$, with the following evolution using Theorem 5.2 (i)):

$$(y^i) = \mathfrak{T}^i \cdot \mathfrak{B}^{1-\sigma}, \text{ with } \mathrm{N}(\mathfrak{B}\,(\beta)) = \mathrm{N}(\mathfrak{T}') = \mathfrak{t}' \in \mathbf{T}_k, \tag{5.3}$$

for a suitable β such that $\mathrm{N}(\beta)$ is close to 1, and one obtains a new $\mathfrak{t}'$ to build $\mathbf{\Sigma}^{i+1}_k$, and so on. If λ or μ do not vanish, there exist, when $[K : k] \to \infty$, arbitrary large i-sequences of sets $\mathbf{\Sigma}^i_k$ such that the class and norm factors are constant, which seems incredible, each new $\mathfrak{t}'$ being a priori random in $\mathbf{T}_k$.

A philosophy should be that it is the $\mathfrak{t}'$ which govern (numerically) the G-structure of the class groups in K/k and not the inverse (see also [6, Remarques 11, § 6]).

Let's give a more precise description of the numerical possibilities, assuming to simplify the comments that $1 \to \mathscr{R}_k \to \mathscr{T}_k \to \mathscr{C}_k \to 1$ is an exact sequence of $\mathbb{F}_p$-vector spaces; we compute the filtration $\{M^i\}_{i\geq 0}$ for $M = \mathscr{C}_K$ ($K = k_n$ fixed) with the following exact sequence at the step i (see (5.2)):

$$1 \longrightarrow \Lambda^i/E_k \xrightarrow{(\,.\,)} \langle \mathbf{\Sigma}^i_k\rangle \xrightarrow{\mathscr{cl}_k} \mathscr{cl}_k\langle \mathbf{\Sigma}^i_k\rangle = \mathrm{N}(M^i) \longrightarrow 1,$$

where $\Lambda^i = \{\tau \in k'^{\times} \otimes \mathbb{Z}_p,\ (\tau) \in \langle \mathbf{\Sigma}^i_k\rangle\}$, and let $\mathfrak{t}^{i+1}$ (obtained as above). Various cases may arrive to get the $(i+1)$th exact sequence

$$1 \to \Lambda^{i+1}/E_k \xrightarrow{(\,.\,)} \langle \mathbf{\Sigma}^{i+1}_k\rangle \xrightarrow{\mathscr{cl}_k} \mathscr{cl}_k\langle \mathbf{\Sigma}^{i+1}_k\rangle = \mathrm{N}(M^{i+1}) \to 1 :$$

(**a**) $\mathscr{cl}_k(\mathfrak{t}^{i+1}) \notin \mathscr{cl}_k\langle \mathbf{\Sigma}^i_k\rangle$. Thus $\mathrm{N}(M^{i+1}) \supsetneq \mathrm{N}(M^i)$ and this decreases the class factor; but there is no new relation of principality between ideals, so $\Lambda^{i+1} = \Lambda^i$ (norm factor unchanged).

(**b**) $\mathscr{cl}_k(\mathfrak{t}^{i+1}) \in \mathscr{cl}_k\langle \mathbf{\Sigma}^i_k\rangle$. Thus $\mathrm{N}(M^{i+1}) = \mathrm{N}(M^i)$ (class factor unchanged); but $\mathfrak{t}^{i+1} = (\tau) \cdot \prod_j \mathfrak{t}_j^{i\,a_j}$ gives, possibly, some $\tau \notin \Lambda^i$. Then two cases arise:

(**i**) $\tau \notin \Lambda^i\,\mathrm{N}(K^{\times})$, therefore $(\Lambda^{i+1} : \Lambda^{i+1} \cap \mathrm{N}(K^{\times})) > (\Lambda^i : \Lambda^i \cap \mathrm{N}(K^{\times}))$, which decreases the norm factor.

(**ii**) $\tau \in \Lambda^i\,\mathrm{N}(K^\times)$ (class and norm factors unchanged). This is the "bad case" occurring, roughly, $O(\lambda n + \mu p^n)$ times if Greenberg's conjecture falls (see Remark 5.3 for more enlightenment).

We have given, in [6, Section 6], some heuristics about the "equation $(y) = \mathfrak{A}\,\mathfrak{B}^{1-\sigma}$" in cyclic extensions L/K when $\mathrm{N}_{L/K}(y) = \mathrm{N}_{L/K}(\mathfrak{A})$ and its "additive aspects", which applies to $(\tau) = \mathrm{N}(\mathfrak{T}) = \mathrm{N}(y)$ and $(y) = \mathfrak{T}\,\mathfrak{B}^{1-\sigma}$.

Assuming that the ideals $\mathfrak{t}$, given by the algorithm, are random, $cl_k(\mathfrak{t})$ (resp. $\log(\iota\tau)$ (mod $\log(\overline{E}_k)$) are random in $\mathscr{C}_k$ (resp. $\mathscr{R}_k$). This is likely to avoid unbounded algorithms and suggests the following conjecture:

Conjecture 5.4. *For $n \gg 0$ fixed, let $\mathfrak{t}_j$ (or τ_j, when $\mathfrak{t}_j = (\tau_j)$ is principal), be the fundamental ideals encountered by the algorithm computing inductively the successive class and norm factors, in b_n steps; then:*

(i) The classes $cl_k(\mathfrak{t}_j)$ are uniformly distributed in $\mathscr{C}_k$.

(ii) When $\mathfrak{t}_j = (\tau_j)$, the images $\log(\mathfrak{t}_j) := \log(\iota\tau_j)$ (mod $\log(\overline{E}_k)$) are uniformly distributed in the normalized regulator $\mathscr{R}_k = \log(U_k^*)/\log(\overline{E}_k)$.

5.4. **Conclusion and possible methods.** Recall that b_n is the length of the algorithm for the layer n. We observe the huge discontinuity between the case b_n bounded, which characterizes Greenberg's conjecture (Theorem 4.3 and Corollary 4.4) and the case where λ or μ are non-zero, giving $b_n \to \infty$. In other words, there is a conflict between the "random aspect" of the algorithm, when λ or μ are non-zero, and the smooth algebraic form given by Iwasawa's theory. We indeed have, under Conventions 1.1, $\#\mathscr{C}_{k_n} = p^{\lambda\, n+\mu\, p^n+\nu}$ for all $n \geq 0$, so that the algorithm must obtain rigorously these formulas, *for all* n, which seems to be an excessive requirement in contradiction with Conjecture 5.4.

To give a logical way, the sole "solution", where b_n does not tend to infinity, is b_n constant for all $n \geq n_1$, giving, from the new base field k_{n_1}, that we still denote k, the well-known properties when Greenberg's conjecture holds. In that case, $\mathscr{C}^2_{k_n}/\mathscr{C}^1_{k_n} = 1$ and $b_n \leq 1$ for all n. In other words, in this situation, the "unpredictable" evolution relation (5.3) is not needed. The quotient $\mathscr{C}^2_{k_n}/\mathscr{C}^1_{k_n}$ does appear (written instead $(1-\sigma)\mathscr{C}_{k_n}[(1-\sigma)]$) in works of Koymans–Pagano–Smith [15, 20], where deep distribution results are proved for the degree p cyclic case.

We believe that these techniques can be successful for Greenberg's conjecture since the general algorithm of "unscrewing" in k_n/k is identical and is essentially based on random values of classical norm symbols. In other words, Greenberg's conjecture would be, for k_∞/k (k taken hight enough in the cyclotomic tower), an extreme version (of the degree p cyclic case) giving the non-existence of "exceptional p-classes" (i.e., non-invariant p-classes) in the tower, that is to say, $b_n \leq 1$ for all $n \geq 0$ (to be compared with $b_n \to \infty$ if λ or μ do not vanish).

Remark 5.5. For a base field which does not fulfill the previous conditions, the algorithms may need several steps and (under Greenberg's conjecture) they regularize at some layer such that the above trivialization holds; for instance, the case of $k = \mathbb{Q}(\sqrt{6559})$, $p = 3$, computed in [6, § 7.2], yields $\mathscr{C}\ell_k \simeq \mathbb{Z}/9\mathbb{Z}$, $\mathscr{R}_k \simeq \mathbb{Z}/27\mathbb{Z}$, $\mathscr{C}\ell_{k_1} \simeq \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (whence $b_1 = 2$) and $\mathscr{C}\ell_{k_2} \simeq \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$; we compute with [1] that $\widetilde{\mathscr{C}\ell}_k \simeq \mathbb{Z}/3\mathbb{Z}$, $\widetilde{\mathscr{C}\ell}_{k_1} \simeq \widetilde{\mathscr{C}\ell}_{k_2} \simeq \mathbb{Z}/9\mathbb{Z}$.

All this shows how classical arguments of *algebraic number theory* seem insufficient to prove unconditionally Greenberg's conjecture (among others), but that density results may be accessible, giving that the conjecture holds except, possibly, for pathological families of zero density (probably none).

References

[1] K. Belabas and J-F. Jaulent, *The logarithmic class group package in PARI/GP*, Pub. Math. Besançon, Théorie des Nombres (2016), 5–18. http://pmb.univ-fcomte.fr/2016/Belabas_Jaulent.pdf 2, 15

[2] C. Chevalley, *Sur la théorie du corps de classes dans les corps finis et les corps locaux* (Thèse), Jour. of the Faculty of Sciences Tokyo **2** (1933), 365–476. http://eudml.org/doc/192833 5

[3] G. Gras, *Class Field Theory: from theory to practice*, corr. 2nd ed. Springer Monographs in Mathematics, Springer, xiii+507 pages (2005). 4, 5, 10, 12

[4] G. Gras, *Invariant generalized ideal classes–Structure theorems for p-class groups in p-extensions*, Proc. Math. Sci. **127**(1) (2017), 1–34. http://doi.org/10.1007/s12044-016-0324-1 3, 7

[5] G. Gras, *Approche p-adique de la conjecture de Greenberg pour les corps totalement réels*, Ann. Math. Blaise Pascal **24**(2) (2017), 235–291. https://doi.org/10.5802/ambp.370 2, 3, 8, 9

[6] G. Gras, *Normes d'idéaux dans la tour cyclotomique et conjecture de Greenberg*, Ann. math. du Québec **43** (2019), 249–280. https://doi.org/10.1007/s40316-018-0108-3 2, 3, 13, 14, 15

[7] G. Gras, *The p-adic Kummer–Leopoldt Constant: Normalized p-adic Regulator*, Int. J. of Number Theory, **14**(2) (2018), 329–337.3, 4 https://doi.org/10.1142/S1793042118500203

[8] G. Gras, *Heuristics and conjectures in the direction of a p-adic Brauer–Siegel theorem*, Math. Comp. **88**(318) (2019), 1929–1965. https://doi.org/10.1090/mcom/3395 3

[9] G. Gras, *Practice of the Incomplete p-Ramification Over a Number Field – History of Abelian p-Ramification*, Communications in Advanced Mathematical Sciences **2**(4) (2019), 251–280. https://doi.org/10.33434/cams.573729 2

[10] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98**(1) (1976), 263–284. https://doi.org/10.2307/2373625 2, 3

[11] J-F. Jaulent, *S-classes infinitésimales d'un corps de nombres algébriques*, Ann. Sci. Inst. Fourier **34**(2) (1984), 1–27. https://doi.org/10.5802/aif.960 10, 11

[12] J-F. Jaulent, *Classes logarithmiques des corps de nombres*, J. Théorie des Nombres de Bordeaux **6** (1994), 301–325. https://doi.org/10.5802/jtnb.117 2

[13] J-F. Jaulent, *Théorie ℓ-adique globale du corps de classes*, J. Théorie des Nombres de Bordeaux **10**(2) (1998), 355–397. http://www.numdam.org/article/JTNB_1998__10_2_355_0.pdf 4

[14] J-F. Jaulent, *Note sur la conjecture de Greenberg*, J. Ramanujan Math. Soc. **34** (2019), 59–80. http://www.mathjournals.org/jrms/2019-034-001/2019-034-001-005.html 2

[15] P. Koymans, C. Pagano, *On the distribution of $\mathscr{C}(K)[\ell^\infty]$ for degree ℓ cyclic fields* (2018). https://arxiv.org/pdf/1812.06884 4, 14

[16] C. Maire, *Sur la dimension cohomologique des pro-p-extensions des corps de nombres*, J. Théor. Nombres Bordeaux, **17**(2) (2005), 575–606. http://www.numdam.org/item/JTNB_2005__17_2_575_0/ 2

[17] A. Movahhedi, *Sur les p-extensions des corps p-rationnels*, Thèse, Univ. Paris VII, 1988. http://www.unilim.fr/pages_perso/chazad.movahhedi/These_1988.pdf 3, 4

[18] T. Nguyen Quang Do, *Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens*, Ann. Inst. Fourier, **36**(2) (1986), 27–46. https://doi.org/10.5802/aif.1045 4

[19] T. Nguyen Quang Do, *Formules de genres et conjecture de Greenberg*, Ann. Math. Québec, **42**(2) (2018), 267–280. https://doi.org/10.1007/s40316-017-0093-y 2

[20] A. Smith, *2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture* (2017). https://arxiv.org/abs/1702.02325 4, 14

[21] H. Taya, *On p-adic zêta functions and $\mathbb{Z}_p$-extensions of certain totally real number fields*, Tohoku Math. J. **51**(1) (1999), 21–33. https://doi.org/10.2748/tmj/1178224850 7

Chemin de Château Gagnière, Villa la Gardette, 38520 Le Bourg d'Oisans
Email address: g.mn.gras@wanadoo.fr