Greenberg's conjecture for totally real number fields in terms of algorithmic complexity

Georges Gras

GREENBERG'S CONJECTURE FOR TOTALLY REAL FIELDS IN TERMS OF ALGORITHMIC COMPLEXITY

GEORGES GRAS

ABSTRACT. Let k be a totally real number field and let k_∞ be its cyclotomic $\mathbb{Z}_p$-extension, $p \geq 2$. Generalizing some viewpoints of Taya and others, we show that Greenberg's conjecture ($\lambda = \mu = 0$) depends on images, of ideal norms along the stages k_n/k of the tower, in the torsion group $\mathcal{T}_k$ of the Galois group of the maximal abelian p-ramified pro-p-extension of k; these images (obtained inductively via a classical algorithm in each k_n) take place both in the p-class group $\mathcal{C}\ell_k$ and in the normalized p-adic regulator $\mathcal{R}_k$ of k (Theorem 6.2). A property of uniform distribution of these images (Conjecture 6.4) would lead to density results needed for a proof of Greenberg's conjecture, which remains hopeless within the sole framework of Iwasawa's theory. Indeed, many "algebraic/class field theory" criteria exist, which hide a broad p-adic arithmetic and algorithmic complexity governed by $\mathcal{T}_k$. No assumption is made on the degree $[k : \mathbb{Q}]$, nor on the decomposition of p in $k/\mathbb{Q}$.

CONTENTS

1. INTRODUCTION

Let k be a totally real number field of degree d and let $p \geq 2$ be a prime number. Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and let $k_\infty := k\,\mathbb{Q}_\infty$ be that of k. We

Date: June 22, 2020.

1991 *Mathematics Subject Classification.* 11R23, 11R29, 11R37, 11Y40.

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

denote by k_n the degree p^n extension of k in k_∞ and put $G_n := \mathrm{Gal}(k_n/k)$. Let $\mathcal{C}\ell_k$ and $\mathcal{C}\ell_{k_n}$ be the ordinary p-class groups of k and k_n, respectively. We denote by $\mathcal{T}_k$ the torsion group of $\mathcal{A}_k := \mathrm{Gal}(H_k^{\rm pr}/k)$, where $H_k^{\rm pr}$ is the maximal abelian p-ramified (i.e., unramified outside p and ∞) pro-p-extension of k.
In the case $p = 2$, all the forthcoming 2-invariants: "$\mathcal{C}\ell$ (class groups), $\mathcal{T}$ (torsion in p-ramification), $\mathcal{R}$ (regulators), $\mathcal{W}$ (local torsion), $\mathcal{G}$ (genus groups), ..." may be also considered in the restricted sense "*res*" instead of the ordinary sense "*ord*". But, to avoid complicated notations, we do not emphasize about this distinction, so that all writings will be identical for all p; indeed, there is a kind of "miracle" since, *under Leopoldt's conjecture*, we have:

$$\#\mathcal{T}_k^{\rm res} = 2^d\,\#\mathcal{T}_k^{\rm ord} \quad [7,\ \text{Theorem III.4.1.5}],$$

knowing that, for totally real number fields k of global unit group E_k:

$$(1)\qquad \#\mathcal{C}\ell_k^{\rm res} = \tfrac{2^d}{(E_k:E_k^{\rm pos})}\cdot\#\mathcal{C}\ell_k^{\rm ord},\quad \#\mathcal{R}_k^{\rm res} = \tfrac{(E_k:E_k^{\rm pos})}{2}\cdot\#\mathcal{R}_k^{\rm ord},\quad \#\mathcal{W}_k^{\rm res} = 2\,\#\mathcal{W}_k^{\rm ord},$$

which makes coherent the formulas $\#\mathcal{T} = \#\mathcal{C}\ell\cdot\#\mathcal{R}\cdot\#\mathcal{W}$ in the two senses (see the definitions of $\mathcal{R}_k$, $\mathcal{W}_k$, in the ordinary sense, in § 3.1).
We call *Greenberg's conjecture for totally real number fields* k, the nullity of the Iwasawa invariants λ, μ of the cyclotomic p-tower k_∞ of k (for all p) (see the origin of the conjecture in [15, Theorems 1 and 2] with the study of two particular cases of decomposition of p in $k/\mathbb{Q}$). This conjecture is, in some sense, a generalization of Vandiver's conjecture for $\mathbb{Q}(\mu_p)^+$ (see [14] for a new approach on Vandiver's conjecture that can be generalized for annihilation aspects in p-ramification theory [37]).
Main recent studies of this conjecture, after the pioneering works of Fukuda–Komatsu, Hiroshi, Ichimura–Sumida, Nishino, Ozaki, Ozaki–Taya, Taya [2, 3, 4, 5, 18, 19, 20, 38, 39, 41, 42, 43], are [10, 12, 24, 26, 27, 30, 33, 34, 35, 36]. In [10, 12] we have given the bases of our method with many numerical experiments and a survey of known results and criteria. In [26, Théorème A] a new criterion is given (capitulation in k_∞ of the logarithmic class group $\widetilde{\mathcal{C}\ell}_k$ of k), in [27] the Greenberg conjecture is stated in terms of "universal norms". In [35] a synthetic view of the criteria of Greenberg, Jaulent, Nguyen Quang Do and others, is given by means of Iwasawa's theory. Then we shall explain in what sense these algebraic criteria hide a tricky arithmetic complexity, materialized by the algorithm given Section 5.1.

Remark 1.1. Subject to replace k by a stage $K := k_{n_0}$ in k_∞, one may assume without any limitation of the generality (under Leopoldt's conjecture in $K_\infty = k_\infty$) that p is totally ramified in K_∞/K; if necessary, K may be such that the corresponding Iwasawa formula for K is fulfilled for all $n \geq 0$. Indeed, K is totally real and the Iwasawa invariants of K (λ', μ') are trivial if and only if that of k (λ, μ) are trivial (in fact, $\lambda' = \lambda$, $\mu' = \mu\, p^{n_0}$). So we shall remember that the number s_p of p-places of k, ramified in any k_n/k, $n \geq 1$, is at least 1. We only assume that k_∞/k is totally ramified at p.
In many papers, the decomposition of p in $k/\mathbb{Q}$ plays an important role and needs different techniques; for instance, two cases are examined after [15]:

(i) The case $s_p = 1$ of a single place over p in k_∞; in this case, the corresponding papers assume that p is totally ramified in k_∞/k, which constitutes a restriction when $p \mid d$ (e.g., $p = 2$ and $k = \mathbb{Q}(\sqrt{m})$, $m \equiv 2 \pmod 8$).
(ii) The case $s_p = d$ (p totally split in $k/\mathbb{Q}$, thus totaly ramified in k_∞/k).

On the contrary, we shall not put any assumption on the degree d nor on the decomposition of p in $k/\mathbb{Q}$; to analyze Greenberg's conjecture, we will show how this

decomposition of p intervenes, especially regarding the inertia groups of the p-places in $H_k^{\rm pr}/k_\infty$ and regarding the "normalized regulator" $\mathcal{R}_k$.

2. Main results.

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

(A) The algorithm, determining $\#\mathcal{C}\ell_{k_n}$ in k_n (whence giving the Iwasawa invariants for $n \gg 0$), computes inductively the classical filtration $(\mathcal{C}\ell^i_{k_n})_{i\geq 0}$, where $\mathcal{C}\ell^{i+1}_{k_n}/\mathcal{C}\ell^i_{k_n} := (\mathcal{C}\ell_{k_n}/\mathcal{C}\ell^i_{k_n})^{G_n}$, with $\mathcal{C}\ell^0_{k_n} = 1$ and $G_n = {\rm Gal}(k_n/k)$. We have the decreasing sequence, where $s_p \geq 1$ is the number of p-places of k:

$$\#\big(\mathcal{C}\ell^{i+1}_{k_n}/\mathcal{C}\ell^i_{k_n}\big) = \frac{\#\mathcal{C}\ell_k}{\#{\rm N}_{k_n/k}(\mathcal{C}\ell^i_{k_n})} \cdot \frac{p^{n\cdot(s_p-1)}}{(\Lambda^i_n : \Lambda^i_n \cap {\rm N}_{k_n/k}(k_n^\times))}, \tag{2}$$

where:

$$\Lambda^i_n := \{x \in k^\times,\ \ (x) = {\rm N}_{k_n/k}(\mathfrak{A}),\ \ \mathcal{C}\ell_{k_n}(\mathfrak{A}) \in \mathcal{C}\ell^i_{k_n}\}, \tag{3}$$

giving the increasing sequence (from $\Lambda^0_n = E_k$):

$$E_k/E_k\cap{\rm N}_{k_n/k}(k_n^\times) \hookrightarrow \cdots \hookrightarrow \Lambda^i_n/\Lambda^i_n\cap{\rm N}_{k_n/k}(k_n^\times) \hookrightarrow \Lambda^{i+1}_n/\Lambda^{i+1}_n\cap{\rm N}_{k_n/k}(k_n^\times) \hookrightarrow \cdots$$

Then $\mathcal{C}\ell^{i+1}_{k_n}/\mathcal{C}\ell^i_{k_n}$ in (2) becomes trivial for some $i = b_n$ (thus $\mathcal{C}\ell_{k_n} = \mathcal{C}\ell^{b_n}_{k_n}$) if and only if the two factors vanish. The length b_n of the algorithm depends on the decreasing evolution of the "class factors" $\dfrac{\#\mathcal{C}\ell_k}{\#{\rm N}_{k_n/k}(\mathcal{C}\ell^i_k)}$ dividing $\#\mathcal{C}\ell_k$ and the "norm factors" $\dfrac{p^{n\cdot(s_p-1)}}{(\Lambda^i_n : \Lambda^i_n \cap {\rm N}_{k_n/k}(k_n^\times))}$ dividing the order of a suitable quotient $\mathcal{R}^{\rm nr}_k$ of the normalized p-adic regulator $\mathcal{R}_k$, related to the decomposition of p in $H_k^{\rm pr}/k_\infty$ (Theorems 3.8, 5.3, § 5.1).

We prove (Theorem 5.4) that $\mathcal{C}\ell_k = \mathcal{R}^{\rm nr}_k = 1 \iff \lambda = \mu = \nu = 0$ and obtain, when $\mathcal{C}\ell_k \cdot \mathcal{R}^{\rm nr}_k \neq 1$, the following bound for b_n (where v_p is the p-adic valuation):

$$b_n \geq \frac{1}{v_p(\#\mathcal{C}\ell_k \#\mathcal{R}^{\rm nr}_k)} \cdot (\lambda \cdot n + \mu \cdot p^n + \nu). \tag{4}$$

These results are in relation with the property (Theorem 5.9) $\lambda = \mu = 0 \iff \lim\limits_{i\to\infty}\lim\limits_{n\to\infty} \#\big(\mathcal{C}\ell^{i+1}_{k_n}/\mathcal{C}\ell^i_{k_n}\big) = 1$.

(B) From Theorem 6.2 one may replace in (3) the ideal norms $\mathfrak{a} = {\rm N}_{k_n/k}(\mathfrak{A})$ by representatives $\mathfrak{t}$ whose Artin symbols are in $\mathcal{T}_k$, *hence finite in number*; but under Greenberg's conjecture, replacing k by k_n, one gets $b_m(k_n) = 1$ for all $m \geq n \gg 0$ (Theorem 4.1 (ii)), which constitutes a spectacular algorithmic discontinuity compared to the other case where, from (4) applied to k_n, $b_m(k_n) \to \infty$ with m if λ or μ is nonzero. So the main question is the algorithmic complexity, analyzed in Section 6, suggesting possible analytic proof in the framework of the powerful techniques used in [29] in the case of degree p cyclic extensions.

Indeed, as we have seen, each step of the algorithm only depends on finite number of possibilities (at most $\#\mathcal{T}_k$) by taking the class of the random ideal $\mathfrak{t}$ and by computing, when $\mathfrak{t} = (\tau)$ is principal, Hasse's symbols at the p-places of the random element τ, in other words a classical situation involving random $\mathbb{Z}/p^n\mathbb{Z}$-matrices. Then the algorithm is based on the of evolution relation (14), only depending on basic arithmetic. So, under the natural Conjecture 6.4 of independence and randomness of the data obtained at each step of

the algorithm, one may obtain that Greenberg's conjecture holds true with probability 1.

3. Abelian p-ramification and genus theories

3.1. **Abelian p-ramification – The torsion group $\mathcal{T}_k$.** Let $s_p \geq 1$ be the number of primes $\mathfrak{p} \mid p$ in k (hence totally ramified in k_∞/k with the convention of Remark 1.1). Under Leopoldt's conjecture for p in k_∞, recall the main data needed for the study of the Galois group $\mathcal{A}_k$ of the maximal abelian p-ramified pro-p-extension $H_k^{\rm pr}$ of k and its torsion group $\mathcal{T}_k$ (see for instance [13, Appendix 1] for a wide story of abelian p-ramification theory in its various aspects):

(a) Let E_k be the group of p-principal global units $\varepsilon \equiv 1 \pmod{\prod_{\mathfrak{p}\mid p}\mathfrak{p}}$ of k. Let $U_k := \bigoplus_{\mathfrak{p}\mid p} U_{k,\mathfrak{p}}$ be the $\mathbb{Z}_p$-module of p-principal local units, where $U_{k,\mathfrak{p}}$ is the group of $\mathfrak{p}$-principal units of the $\mathfrak{p}$-completion $k_\mathfrak{p}$ of k. Denote by $\mu_p(\kappa)$ the group of pth roots of unity of any field κ and put $W_k := {\rm tor}_{\mathbb{Z}_p}(U_k) = \bigoplus_{\mathfrak{p}\mid p} \mu_p(k_\mathfrak{p})$ and $\mathcal{W}_k := W_k/\mu_p(k)$. Since $\mu(k) = \{\pm 1\}$, $\mathcal{W}_k := W_k$ for $p \neq 2$ and $\mathcal{W}_k := W_k/\{\pm 1\}$ for $p = 2$.

(b) Let $\iota : \{x \in k^\times \otimes \mathbb{Z}_p,\ x \text{ prime to } p\} \to U_k$ be the diagonal embedding. Let $\overline{E}_k$ be the closure of ιE_k in U_k and let H_k be the p-Hilbert class field of k; then we have ${\rm Gal}(H_k^{\rm pr}/H_k) \simeq U_k/\overline{E}_k$. One checks that under Leopoldt's conjecture,

$$ {\rm tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k) = U_k^*/\overline{E}_k, \text{ where } U_k^* := \{u \in U_k,\ \ {\rm N}_{k/\mathbb{Q}}(u) \in \{\pm 1\}\}. $$

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

$$ \mathcal{R}_k := {\rm tor}_{\mathbb{Z}_p}(\log(U_k)/\log(\overline{E}_k)) = \log(U_k^*)/\log(\overline{E}_k) \tag{5} $$

be the normalized p-adic regulator [11, § 5]; recall that for $p \neq 2$, $\#\mathcal{R}_k = \frac{R_k}{p^{d-1}}$ and $\#\mathcal{R}_k = \frac{1}{2^{s_2-1}}\frac{R_k}{2^{d-1}}$ for $p = 2$, where R_k is the classical regulator.

(d) The sub-group of $\mathcal{T}_k$ fixing the Bertrandias–Payan field $H_k^{\rm bp}$ is isomorphic to $\mathcal{W}_k$.

For a given base field k, the invariants $\mathcal{C}\ell_k$ and $\mathcal{W}_k$ are trivial for almost all primes p; this is only conjectured for $\mathcal{R}_k$ (see [8] for conjectural p-adic properties of regulators) and constitutes an out of reach question.

Recall some classical results in our context (under the Leopoldt conjecture):

Proposition 3.1. [11, § 4, § 5]. *We have the exact sequences:*

$$ 1 \to {\rm tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k) = U_k^*/\overline{E}_k \longrightarrow \mathcal{T}_k \longrightarrow {\rm Gal}(k_\infty H_k/k_\infty) \simeq \mathcal{C}\ell_k \to 1, $$

$$ 1 \to \mathcal{W}_k \longrightarrow {\rm tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k) \longrightarrow {\rm tor}_{\mathbb{Z}_p}(\log(U_k)/\log(\overline{E}_k)) \simeq \mathcal{R}_k \to 0. \tag{6} $$

3.2. **Genus theory in k_n/k.** We denote by H_{k_n} the p-Hilbert class field of k_n. Since p is totally ramified in k_n/k, the inertia groups $I_\mathfrak{p}(k_n/k)$ in k_n/k, $\mathfrak{p} \mid p$, 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 $\left(\frac{\varepsilon\,,\,k_n/k}{\mathfrak{p}}\right) \in G_n$, $\mathfrak{p} \mid p$. This yields the genus exact sequence interpreting the product formula of the Hasse symbols of a unit (see, e.g., [7, Corollary IV.4.4.1]):

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

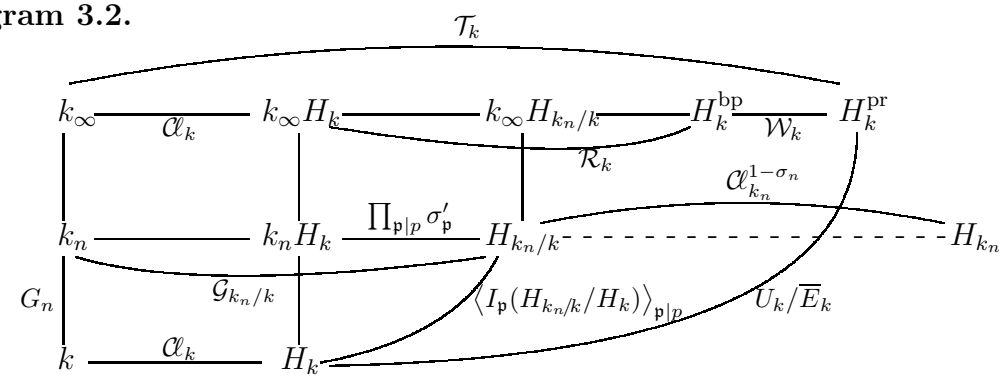
where $\Omega(k_n/k) := \left\{(\sigma_\mathfrak{p})_{\mathfrak{p}\mid p} \in G_n^{s_p},\ \prod_{\mathfrak{p}\mid p}\sigma_\mathfrak{p} = 1\right\} \simeq G_n^{s_p-1}$, then where $H_{k_n/k}$ is *the p-genus field* of k_n/k defined as the maximal sub-extension of H_{k_n}, abelian over k.

The image of ω_n is contained in $\Omega(k_n/k)$ and the map π_n is defined as follows: with $(\sigma_\mathfrak{p})_{\mathfrak{p}\mid p} \in G_n^{s_p}$, π_n associates the product of the extensions $\sigma'_\mathfrak{p}$ of the $\sigma_\mathfrak{p}$ in the inertia

groups $I_{\mathfrak{p}}(H_{k_n/k}/H_k)$ generating $\mathrm{Gal}(H_{k_n/k}/H_k)$; from the product formula, if $(\sigma_{\mathfrak{p}})_{\mathfrak{p}|p} \in \Omega(k_n/k)$, then $\prod_{\mathfrak{p}|p} \sigma'_{\mathfrak{p}}$ fixes both H_k and k_n, whence $k_n H_k$.
The genus exact sequence shows that the kernel of π_n is $\omega_n(E_k)$. We have as expected, using Chevalley's ambiguous class number formula [1],

$$\#\mathcal{G}_{k_n/k} := \#\mathrm{Gal}(H_{k_n/k}/k_n) = \frac{\#\mathcal{C}\ell_{k_n}}{\#\mathcal{C}\ell_{k_n}^{1-\sigma_n}} = \#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{C}\ell_k \cdot \frac{p^{n\cdot(s_p-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))}.$$

Diagram 3.2.



In the above Diagram, $H_{k_n/k}$ is the fixed field [1] of the image of $\mathcal{C}\ell_{k_n}^{1-\sigma_n}$, where σ_n is a generator of G_n, and $\mathcal{G}_{k_n/k} = \mathrm{Gal}(H_{k_n/k}/k_n)$ is the genus group in k_n/k.
The genus group $\mathcal{G}_{k_n/k}$ has, in our context, the following main property that we will analyze in more details in § 3.3 to obtain Theorem 3.8 when n is large enough:

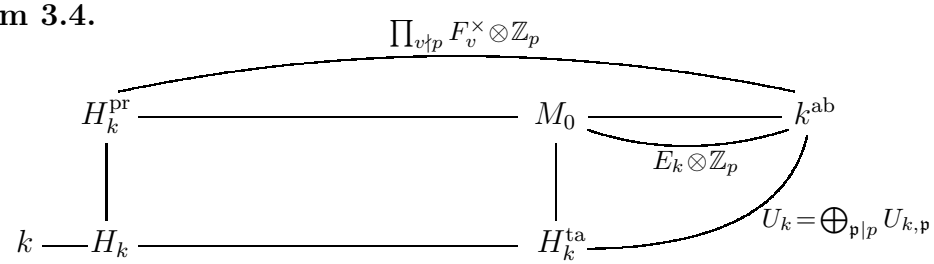
Proposition 3.3. (i) *For all $n \geq 0$, $k_\infty H_{k_n/k} \subseteq H_k^{\mathrm{bp}}$ and $\#\mathcal{G}_{k_n/k} \,\big|\, \#\mathcal{C}\ell_k \cdot \mathcal{R}_k$, which is equivalent to $\dfrac{p^{n\cdot(s_p-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))} \,\Big|\, \#\mathcal{R}_k$.*

(ii) *The n-sequence $\#\mathcal{G}_{k_n/k}$ is increasing and stabilizes at a divisor of $\#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k$.*

(iii) *Let $\mathrm{J}_{k_n/k}$ be the transfer map $\mathcal{C}\ell_k \to \mathcal{C}\ell_{k_n}$, let S_{k_n} be the set of p-places of k_n. Then the orders of $\mathrm{J}_{k_n/k}(\mathcal{C}\ell_k)\cdot c\ell_{k_n}(S_{k_n})$ are bounded by $\#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k$ for all $n \geq 0$.*

Proof. Using the idelic global reciprocity map (under Leopoldt's conjecture), we have the fundamental diagram [7, § III.4.4.1] of the Galois group of the maximal abelian pro-p-extension k^{ab} of k, with our present notations:

Diagram 3.4.



where F_v is the residue field of the tame place v (finite or infinite). We know that the fixed field of $U_k = \bigoplus_{\mathfrak{p}|p} U_{k,\mathfrak{p}}$ is the maximal tame sub-extension H_k^{ta}, since each $U_{k,\mathfrak{p}}$ is the inertia group of $\mathfrak{p}$ in k^{ab}/k. Thus its torsion part, $\mu_p(k_{\mathfrak{p}})$, restricted to $\mathrm{Gal}(H_k^{\mathrm{pr}}/k)$, fixes k_∞ and since $k_\infty H_{k_n/k}/k_\infty$ is unramified, it fixes $k_\infty H_{k_n/k}$ for all $n \geq 0$. From the diagram, the restriction of U_k to $\mathrm{Gal}(H_k^{\mathrm{pr}}/k)$ is $\mathrm{Gal}(H_k^{\mathrm{pr}}/H_k) \simeq U_k/\overline{E}_k$ as usual, and the restriction of $W_k = \bigoplus_{\mathfrak{p}|p} \mu_p(k_{\mathfrak{p}})$ to $\mathrm{Gal}(H_k^{\mathrm{pr}}/H_k)$ is isomorphic to $W_k/\mu_p(k) = \mathcal{W}_k$

[1] If L/K is a Galois extension of Galois group G, we say that K is the fixed field of G but we say that G fixes k when k is only a subfield of K.

whose fixed field is $H_k^{\rm bp}$; whence the first claim (i). Point (ii) is obvious since non-ramification propagates so that $H_{k_n/k}\,k_{n+h} \subseteq H_{k_{n+h}/k}$ for all $h \geq 1$ (use Diagram 3.2). Point (iii) results of the inclusion $\mathrm{J}_{k_n/k}(\mathcal{C}\ell_k)\cdot c\ell_{k_n}(S_{k_n}) \subseteq \mathcal{C}\ell_{k_n}^{G_n}$ with the relation $\#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{G}_{k_n/k}$ and (i). □

Remark 3.5. (i) Since $\mathcal{G}_{k_n/k}$ is "constant" for all $n \gg 0$, which only depends on k, we put $\mathcal{G}_k \simeq \mathcal{G}_{k_n/k}$ for n large enough. This group will be called, by abuse, the genus group of k_∞/k; then the field (called the genus field of k_∞/k):

$$H_k^{\rm gen} := \bigcup_m H_{k_m/k}$$

is unramified over k_∞ of Galois group $\mathcal{G}_k$ (cf. Proposition 3.6 and Diagram 3.7).

(ii) Let k_0 be a totally real number field in which p totally splits (thus totally ramifies in $k_{0,\infty}/k_0$, i.e., $s_p = d$). We have $\mathcal{W}_{k_0} = 1$ for $p \neq 2$ since $k_{0,\mathfrak{p}} = \mathbb{Q}_p$ for all $\mathfrak{p} \mid p$; then we shall have $\#\mathcal{G}_{k_0} = \#\mathcal{C}\ell_{k_0}\cdot\#\mathcal{R}_{k_0}$ (see Corollary 3.9). This classical case is due to Taya [42, Theorem 1.1]; see analogous recent approaches in [10, Théorème 4.8], [26, § 2.1, § 2.2, Corollaire 11], [35, Théorème C]. For $p = 2$, $\mathcal{W}_{k_0} \simeq \mathbb{F}_2^{d-1}$.

(iii) The case of a single place in k_∞ with p totally ramified in k_∞/k (i.e., $s_p = 1$ giving $\frac{p^{n\cdot(s_p-1)}}{(E_k:E_k\cap \mathrm{N}_{k_n/k}(k_n^\times))} = 1$) is also considered; we have $\#\mathcal{G}_k = \#\mathcal{C}\ell_k$ and the norm factors that we shall define later as divisors of $\#\mathcal{R}_k$ (see (7)) will be trivial.

We shall, now, emphasize on the influence, for the arithmetic of $H_k^{\rm pr}/k_\infty$, of the decomposition of p in $k/\mathbb{Q}$ in the following subsection in which we characterize a subgroup $\mathcal{R}_k^{\rm ram}$ and the quotient $\mathcal{R}_k^{\rm nr} = \mathcal{R}_k/\mathcal{R}_k^{\rm ram}$, of $\mathcal{R}_k$, such that $\#\mathcal{G}_k = \#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr}$.

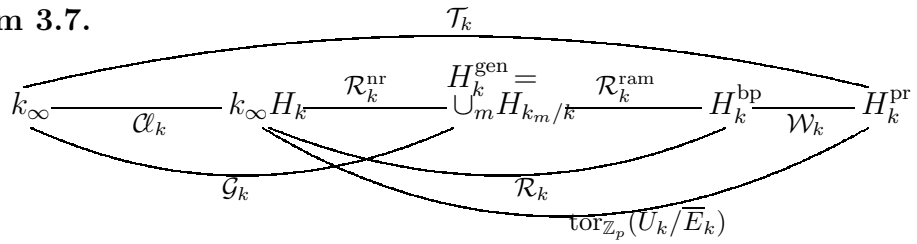
3.3. **Ramification in $H_k^{\rm pr}/k_\infty$.** Recall, once for all, that the tame places totally split in $H_k^{\rm pr}/k_\infty$ [7, Remark III.4.8.2]. From Remark 3.5 (i), we can state:

Proposition 3.6. *Let $n_0 \gg 0$ be such that $\#\mathcal{G}_{k_n/k}$ stabilizes for all $n \geq n_0$, defining the genus field $H_k^{\rm gen}$ such that $\mathrm{Gal}(H_k^{\rm gen}/k_\infty) = \mathcal{G}_k$. Then $H_k^{\rm gen}$ is the maximal unramified extension of k_∞ in $H_k^{\rm pr}$ and $\mathrm{Gal}(H_k^{\rm pr}/H_k^{\rm gen}) \simeq \big\langle\, \mathrm{tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}}\overline{E}_k/\overline{E}_k)\,\big\rangle_{\mathfrak{p}\mid p}$.*

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 $\mathrm{Gal}(L'_\infty/L') \simeq \mathrm{Gal}(L_\infty/L) \simeq \mathbb{Z}_p$. Replacing n by a larger value, one may assume that L'_∞/L' is totally ramified at p (the case of L_∞/L is obvious). 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'_∞ (absurd). Thus, $I_v(L'_\infty/L) = \mathrm{Gal}(L'_\infty/L)$ or $\mathrm{Gal}(L'_\infty/L')$; but this last case, for all v, would give $L'/L/k_n$ 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 $\mathfrak{p} \mid p$ in k, $I_\mathfrak{p}(H_k^{\rm pr}/k_\infty) \simeq \mathrm{tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}}\overline{E}_k/\overline{E}_k)$, since $I_\mathfrak{p}(H_k^{\rm pr}/k)$ is the image of $U_{k,\mathfrak{p}}$ in $\mathrm{Gal}(H_k^{\rm pr}/H_k) \simeq U_k/\overline{E}_k$ (see Diagram 3.4). □

Let $\mathcal{R}_k^{\rm nr} := \mathrm{Gal}(H_k^{\rm gen}/k_\infty H_k)$ ("non-ramification") and $\mathcal{R}_k^{\rm ram} := \mathrm{Gal}(H_k^{\rm bp}/H_k^{\rm gen})$ ("ramification"). So, the top of Diagram 3.2 may be precized as follows:

Diagram 3.7.



From Proposition 3.3 and the above study, we can state:

Theorem 3.8. *Let n_0 be such that $\mathcal{G}_{k_n/k} = \mathrm{Gal}(H_{k_n/k}/k_n) \simeq \mathcal{G}_k$ for all $n \geq n_0$. Then $\#\mathcal{G}_k = \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\rm nr}$, which is equivalent to $\dfrac{p^{n\cdot(s_p-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))} = \#\mathcal{R}_k^{\rm nr}$.*

Corollary 3.9. (i) *If $s_p = d$, then $\mathcal{R}_k^{\rm ram} = 1$ and $\mathcal{R}_k^{\rm nr} = \mathcal{R}_k$.*
(ii) *If $s_p = 1$ with p totally ramified in k_∞/k, then $\mathcal{R}_k^{\rm ram} = \mathcal{R}_k$ and $\mathcal{R}_k^{\rm nr} = 1$.*

Proof. (i) If $s_p = d$, one obtains $U_{k,\mathfrak{p}}\overline{E}_k/\overline{E}_k = U_{k,\mathfrak{p}}/\overline{E}_k \cap U_{k,\mathfrak{p}}$; since $U_{k,\mathfrak{p}} = 1 + p\,\mathbb{Z}_p$ for all $\mathfrak{p} \mid p$, $\mathrm{tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}}/\overline{E}_k \cap U_{k,\mathfrak{p}}) = \mathrm{tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}})/\mathrm{tor}_{\mathbb{Z}_p}(\overline{E}_k) = 1$ whatever p. Thus the inertia field is $H_k^{\rm bp} = H_k^{\rm pr}$, giving $\mathcal{R}_k^{\rm ram} = 1$.
(ii) If $s_p = 1$, $\mathcal{R}_k^{\rm nr} = 1$ and $\mathrm{tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}}\overline{E}_k/\overline{E}_k) = \mathrm{tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k)$. □

Otherwise, these inertia groups are only accessible by means of numerical computations (this is done in [13] in the context of incomplete p-ramification); they fix $H_k^{\rm gen} = \bigcup_m H_{k_m/k}$ independently of the knowledge of $\mathcal{G}_k$.

Theorem 3.10. *Let S_{k_n} be the set of p-places of k_n.*

(i) *We have the exact sequence:*
$$1 \to \mathrm{J}_{k_n/k}(\mathcal{C}\ell_k)\, c\ell_{k_n}(S_{k_n}) \longrightarrow \mathcal{C}\ell_{k_n}^{G_n} \xrightarrow{\theta} E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)/\mathrm{N}_{k_n/k}(E_{k_n}) \to 1.$$
(ii) $\#\mathrm{J}_{k_n/k}(\mathcal{C}\ell_k)\, c\ell_{k_n}(S_{k_n}) \times \#(E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)/\mathrm{N}_{k_n/k}(E_{k_n})) \leq \#\mathcal{G}_k = \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\rm nr}$.[2]
(iii) $\mathrm{J}_{k_n/k}(\mathcal{C}\ell_k)\, c\ell_{k_n}(S_{k_n})$ *and* $E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)/\mathrm{N}_{k_n/k}(E_{k_n})$ *stabilize for $n \gg 0$.*

Proof. (i) We have the exact sequence:
$$1 \to c\ell_{k_n}(\overline{I}_{k_n}^{G_n}) = \mathrm{J}_{k_n/k}(\mathcal{C}\ell_k)\, c\ell_{k_n}(S_{k_n}) \to \mathcal{C}\ell_{k_n}^{G_n} \to^{\theta} E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)/\mathrm{N}_{k_n/k}(E_{k_n}) \to 1$$
where $\overline{I}_{k_n}$ is the $\mathbb{Z}[G_n]$-module of ideals of k_n (not necessarily prime to p) and where θ associates with $c\ell_{k_n}(\mathfrak{A})$, such that $\mathfrak{A}^{1-\sigma_n} = (\alpha)$, $\alpha \in k_n^\times$, the class of the unit $\mathrm{N}_{k_n/k}(\alpha)$ of k, modulo $\mathrm{N}_{k_n/k}(E_{k_n})$. The surjectivity and the kernel are immediate.
(ii) Whence the claim from the equalities $\#\mathcal{G}_{k_n/k} = \#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{G}_k = \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\rm nr}$, for all $n \gg 0$ (Theorem 3.8).
(iii) Since the norm maps $\mathrm{N}_{k_m/k_n} : c\ell_{k_m}(S_{k_m}) \to c\ell_{k_n}(S_{k_n})$ are surjective, for all $m \geq n \geq 0$, the n-sequence $\#c\ell_{k_n}(S_{k_n})$ is increasing and bounded, then stabilizes for n large enough.
The n-sequence $\mathrm{J}_{k_n/k}(\mathcal{C}\ell_k)$ is decreasing and stabilizes for n large enough. Whence the stabilization of the the n-sequence $E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)/\mathrm{N}_{k_n/k}(E_{k_n})$. □

4. Greenberg's conjecture and p-torsion groups.

Let k be a totally real number field, assuming p totally ramified in k_∞/k (cf. Remark 1.1). Let's give first some obvious properties of $H_k^{\rm pr}/k$ under the assumption $\lambda = \mu = 0$.

[2]This result, giving a bound equal to a computable constant of k (with equality for $n \gg 0$), is the key for the proofs of the main Theorems 1 and 2 of [15]. See also the following Theorem 4.1 for a direction in the criteria.

4.1. **Consequences of Greenberg's conjecture.** If $\lambda = \mu = 0$, there exists $\nu \geq 0$ such that $\#\mathcal{C}\ell_{k_n} = p^\nu$ for all $n \gg 0$; thus, any base field $K = k_n$, for n large enough, fulfills the same formula and properties in its tower under the convention of Remark 1.1.
Let $\mathcal{R}_{k_n}$ be the normalized p-adic regulator of k_n, then $\mathcal{R}_{k_n}^{\rm ram}$, $\mathcal{R}_{k_n}^{\rm nr} \simeq \mathcal{R}_{k_n}/\mathcal{R}_{k_n}^{\rm ram}$ and $\mathcal{G}_{k_n} = {\rm Gal}(H_{k_n}^{\rm gen}/k_\infty)$, where $H_{k_n}^{\rm gen} = \bigcup_{m\geq n} H_{k_m/k_n}$ is the maximal unramified extension of k_∞ in $H_{k_n}^{\rm pr}$ (cf. § 3.3, Diagram 3.7 applied to k_n).

Theorem 4.1. *Under Greenberg's conjecture, we have the following properties where $n \gg 0$ is fixed such that $\#\mathcal{C}\ell_{k_m} = p^\nu$, for all $m \geq n$:*

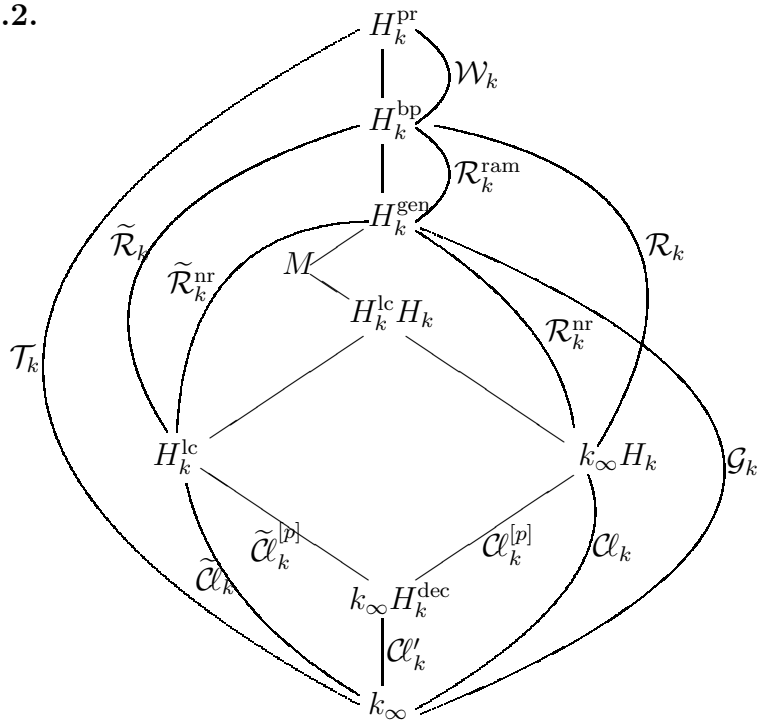
(i) *The norm maps ${\rm N}_{k_m/k_n} : \mathcal{C}\ell_{k_m} \to \mathcal{C}\ell_{k_n}$ are isomorphisms.*
(ii) $\mathcal{C}\ell_{k_m}^{G_{m/n}} = \mathcal{C}\ell_{k_m} = \mathcal{G}_{k_m}$ *of order p^ν, where $G_{m/n} = {\rm Gal}(k_m/k_n) =: \langle \sigma_{m/n} \rangle$.*
(iii) $\mathcal{R}_{k_m}^{\rm nr} = 1$*; then $\mathcal{R}_{k_m}^{\rm ram} = \mathcal{R}_{k_m}$, which means that $H_{k_m}^{\rm gen} = k_\infty H_{k_m}$, and that this field is fixed by $\left\langle {\rm tor}_{\mathbb{Z}_p}(U_{k_m,\mathfrak{p}_m}\overline{E}_{k_m}/\overline{E}_{k_m}) \right\rangle_{\mathfrak{p}_m|p}$ (use Diagram 3.7 for the field k_m).*
(iv) *For all $h \geq 0$, $\mathcal{C}\ell_{k_h}$ capitulates in k_∞.*

Proof. (i) Due to the total ramification of p in k_∞/k, the norm maps (i.e., the restrictions) ${\rm Gal}(H_{k_m}/k_m) \to {\rm Gal}(H_{k_n}/k_n)$ are surjective; since $\#\mathcal{C}\ell_{k_m} = \#\mathcal{C}\ell_{k_n} = p^\nu$ these maps are injective.
(ii) From Chevalley's formula, $\#\mathcal{C}\ell_{k_m}^{G_{m/n}}$ is a multiple of $\#\mathcal{C}\ell_{k_n} = p^\nu$; then we obtain $\mathcal{C}\ell_{k_m}^{G_{m/n}} = \mathcal{C}\ell_{k_m}$, $\mathcal{C}\ell_{k_m}^{1-\sigma_{m/n}} = 1$, and $\mathcal{G}_{k_m/k_n} \simeq \mathcal{C}\ell_{k_m}$ of order p^ν, for all $m \geq n$; this implies $\mathcal{G}_{k_m/k_n} \simeq \mathcal{G}_{k_n}$, of order p^ν. A fortiori, all the $\mathcal{G}_{k_m}$, $m \geq n$, are isomorphic of order p^ν.
(iii) From Theorem 3.8 and (ii), we get $\#\mathcal{R}_{k_m}^{\rm nr} = 1$ for all $m \geq n$.
(iv) Let $\mathcal{C}\ell_{k_m} =: \bigoplus_j \left\langle \mathfrak{cl}_{k_m}(\mathfrak{A}_j) \right\rangle$ be a decomposition of $\mathcal{C}\ell_{k_m}$ into a product of cyclic components. From (i), $\mathcal{C}\ell_{k_n} = \bigoplus_j \left\langle {\rm N}_{k_m/k_n}(\mathfrak{cl}_{k_m}(\mathfrak{A}_j)) \right\rangle$; for such a $\mathfrak{cl}_{k_m}(\mathfrak{A}_j)$, using Chebotarev density theorem in H_{k_m}/k_n, we may assume that $\mathfrak{A}_j$ is a prime ideal $\mathfrak{L}$ of k_m, totally split in k_m/k_n. Consider $\mathfrak{l} := {\rm N}_{k_m/k_n}(\mathfrak{L})$; thus $\mathcal{C}\ell_{k_n}$ is generated by such classes $\mathfrak{cl}_{k_n}(\mathfrak{l})$. Then ${\rm J}_{k_m/k_n}(\mathfrak{l}) = \mathfrak{L}^{\nu_{k_m/k_n}}$, where $\boldsymbol{\nu}_{k_m/k_n} = \sum_{\sigma\in{\rm Gal}(k_m/k_n)} \sigma$ is the algebraic norm. We have $\boldsymbol{\nu}_{k_m/k_n} = p^{m-n} + A(\sigma_{m/n}) \cdot (1 - \sigma_{m/n})$, $A(\sigma_{m/n}) \in \mathbb{Z}_p[\sigma_{m/n}]$. From (ii) and $m - n$ large enough, we get ${\rm J}_{k_m/k_n}(\mathfrak{cl}_{k_n}(\mathfrak{l})) = 1$. Whence also the capitulation of $\mathcal{C}\ell_{k_h}$ in k_∞ for all $h \geq 0$. □

4.2. **The logarithmic class group.** Another approach for Greenberg's conjecture is the criterion of Jaulent [26, Théorèmes A, B] proving that the conjecture is equivalent to the capitulation in k_∞ of the logarithmic class group $\widetilde{\mathcal{C}\ell}_k$ of k. This group is related to $\mathcal{T}_k$ as follows with the following diagram (from that of [26, § 2.3], under the Leopoldt and Gross–Kuz'min conjectures), where $H_k^{\rm lc} \subseteq H_k^{\rm pr}$ is the maximal abelian locally cyclotomic pro-p-extension of k (i.e., such that the p-places totally split in $H_k^{\rm lc}/k_\infty$), $\mathcal{C}\ell_k^{[p]} := \left\langle \mathfrak{cl}_k(\mathfrak{p}) \right\rangle_{\mathfrak{p}|p}$, $\widetilde{\mathcal{C}\ell}_k^{[p]}$ is the subgrup of $\widetilde{\mathcal{C}\ell}_k$ generated by the classes of logarithmic divisors of zero degree built on the p-places, $H_k^{\rm dec}$ is the maximal subfield of H_k in which the p-places totally split; whence:

$$H_k^{\rm lc} \cap k_\infty H_k = k_\infty H_k^{\rm dec} \ \&\ {\rm Gal}(k_\infty H_k^{\rm dec}/k_\infty) \simeq \mathcal{C}\ell'_k = \mathcal{C}\ell_k/\mathcal{C}\ell_k^{[p]}.$$

Diagram 4.2.



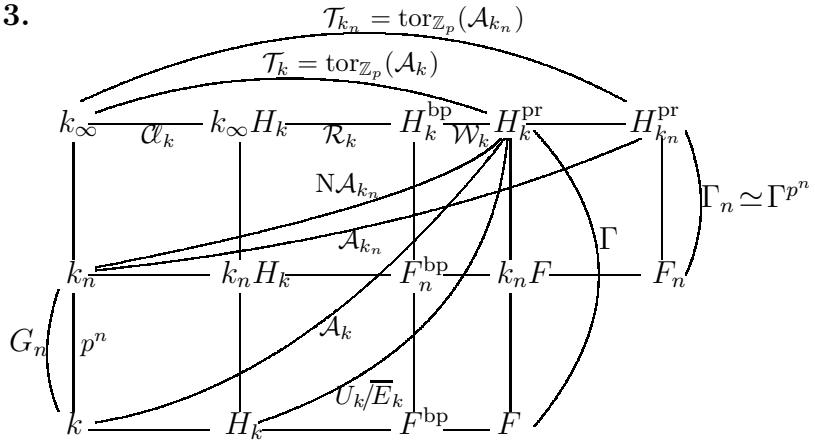
The field $H_k^{\rm gen}$ is fixed by the group generated by the inertia groups:

$$I_{\mathfrak{p}}(H_k^{\rm pr}/k_\infty) \simeq \mathrm{tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}}\overline{E}_k/\overline{E}_k),\ \mathfrak{p} \mid p \ \text{(Proposition 3.6)},$$

and $H_k^{\rm lc}$ is fixed by the group generated by the decomposition groups $D_{\mathfrak{p}}(H_k^{\rm pr}/k_\infty)$, which may be computed numerically from [7, Exercice III.7.1].
If we consider the Frobenius of the p-places in $H_k^{\rm gen}/k_\infty$ (whence in $H_k^{\rm gen}/H_k^{\rm lc}$), their projections in $\mathrm{Gal}(H_k^{\rm lc}H_k/H_k^{\rm lc})$ (as well as in $\mathrm{Gal}(k_\infty H_k/k_\infty H_k^{\rm dec})$) generate these Galois groups; but the Frobenius of the p-places in $H_k^{\rm gen}/H_k^{\rm lc}H_k$ fix an intermediate field M and p totally splits in $M/k_\infty H_k$ (see more information in [26, Lemme 15]).
In [28, Appendice, Définition 17], Jaulent defines the logarithmic regulator as $\widetilde{\mathcal{R}}_k := \mathrm{Gal}(H_k^{\rm bp}/H_k^{\rm lc})$ (use [26, Diagram, § 2.3]). This implies immediately a definition of groups $\widetilde{\mathcal{R}}_k^{\rm ram} \simeq \mathcal{R}_k^{\rm ram}$ and $\widetilde{\mathcal{R}}_k^{\rm nr} = \widetilde{\mathcal{R}}_k/\widetilde{\mathcal{R}}_k^{\rm ram} = \mathrm{Gal}(H_k^{\rm gen}/H_k^{\rm lc})$.

4.3. **Iwasawa's invariants for the torsion groups.** Put $\Gamma := \mathrm{Gal}(k_\infty/k)$. Give now some properties about the transfers J_{k_m/k_n}, the norm maps N_{k_m/k_n}, $m \geq n \geq 0$, and fixed points formulas by $G_{m/n} := \mathrm{Gal}(k_m/k_n)$:

Diagram 4.3.



4.3.1. *Groups $\mathcal{T}$.* We know that the transfer maps $\mathrm{J}_{k_m/k_n} : \mathcal{T}_{k_n} \to \mathcal{T}_{k_m}$ are injective and, in our totally real context, the norm maps $\mathrm{N}_{k_m/k_n} : \mathcal{T}_{k_m} \to \mathcal{T}_{k_n}$ are surjective, $m \geq n \geq 0$. It is easy to see that these properties are fulfilled for the modules $\mathcal{R}$, $\mathcal{R}^{\rm ram}$ and $\mathcal{G}$ (see Diagrams 3.7, 4.2, 4.3). Since the extensions k_m/k_n are trivially "p-primitively ramified", we have the fixed point formula $\mathcal{T}_{k_m}^{G_{m/n}} \simeq \mathcal{T}_{k_n}$ ([7, Theorem IV.3.3] or [13, App. A.4.2], [22, Section 2 (c)], [31, App.]).
However, $\varprojlim \mathcal{W}_{k_n}$ is not always finite and this occurs if and only if some completions $k_{\mathfrak{p}}$ contain μ_{2p}; indeed, in that case, $k_{n,\mathfrak{p}_n}$ ($\mathfrak{p}_n \mid \mathfrak{p}$ in k_n) contains $\mu_{2p^{n+1}}$ for all $n \geq 0$ (in other words, its λ-invariant is s_p; cf. Example 4.5). Otherwise, $\mathcal{W}_{k_n} = 1$ for $p \neq 2$ and $\mathcal{W}_{k_n} \simeq \mathbb{F}_2^{s_p - 1}$ for $p = 2$.
More precisely, we have the following about the $\mathcal{T}_{k_n}$ with inverse properties with respect to those of $\widetilde{\mathcal{C}\ell}_{k_n}$ for which the invariants $\widetilde{\lambda}, \widetilde{\mu}$ are conjecturally trivial:

Proposition 4.4. *Let $\overline{\lambda}$, $\overline{\mu}$, $\overline{\nu}$, be the the Iwasawa invariants for the $\mathbb{Z}_p[[\Gamma]]$-module $\varprojlim \mathcal{T}_{k_n}$ in the totally real case. Then $\overline{\lambda}+\overline{\mu} = 0$ if and only if k is p-rational (equivalent to $\mathcal{T}_k = 1$ under Leopoldt's conjecture)*[3].

Proof. If $\mathcal{T}_k = 1$, since K_n/k is p-primitively ramified, $\mathcal{T}_{k_n} = 1$ for all n; thus $\overline{\lambda} = \overline{\mu} = \overline{\nu} = 0$. If $\overline{\lambda}+\overline{\mu} = 0$, $\#\mathcal{T}_{k_n} = p^{\overline{\nu}}$ for all $n \gg 0$. The norm maps $\mathrm{N}_{k_m/k_n} : \mathcal{T}_{k_m} \to \mathcal{T}_{k_n}$ are surjective (see Diagram 4.3), whence injective, and the transfer maps $\mathrm{J}_{k_m/k_n} : \mathcal{T}_{k_n} \to \mathcal{T}_{k_m}$ are injective, for all $m \geq n \geq 0$; so $\mathrm{N}_{k_m/k_n} \circ \mathrm{J}_{k_m/k_n}(\mathcal{T}_{k_n}) = \mathcal{T}_{k_n}^{p^{m-n}} = 1$ for $m \gg n$; hence $\overline{\nu} = 0$ giving the p-rationality in the tower. □

Example 4.5. The following table, using [12, Program § 4.3] ($p = 2$, $k = \mathbb{Q}(\sqrt{m})$, $n \in [0, 3]$), gives the group invariants of $\mathcal{T}_{k_n}$ for the non-2-rational fields; it suggests some $\overline{\lambda} > 1$ (recall that for $m^* \equiv -1 \pmod 8$ the λ-invariant of $\varprojlim \mathcal{W}_{k_n}$ is $s_p = 1$):

```
m*=  7: [4] [8] [16] [32]                m = 62: [4][16,2][32,2,2,2][64,4,2,2,2,2,2]
m = 14: [2] [8] [16] [32]                m = 65: [8] [16] [32] [64]
m*= 15: [4] [8] [16] [32]                m = 66: [8] [16] [32] [64]
m = 17: [2] [2,2] [4,2,2] [8,4,4]        m = 69: [4] [4,4] [8,8] [16,16]
m = 21: [2] [2,2] [8,4] [16,8]           m = 70: [2] [2,2] [8,8] [16,16]
m*= 23: [4] [8] [16] [32]                m*= 71: [4] [8] [16] [32]
m = 30: [2] [8] [16] [32]                m = 73: [2] [8] [16] [32]
m*= 31: [8] [16,2] [32,2,2,2]            m = 77: [4] [4,4] [8,8] [16,16]
                    [64,4,2,2,2,2,2]     m = 78: [2] [8] [16] [32]
m = 33: [2] [16] [32] [64]               m*= 79: [8] [16,2] [32,8,4] [64,16,8]
m = 34: [2] [2,2] [4,2,2] [8,4,4]        m = 82: [2] [32] [64] [128]
m = 35: [2] [2,2] [8,8] [16,16]          m = 85: [2] [2,2] [2,2,2,2] [8,4,4,4]
m*= 39: [4] [8] [16] [32]                m*= 87: [4] [8] [16] [32]
m = 41: [16] [32] [64] [128]             m = 89: [2] [16] [32] [64]
m = 42: [2] [2,2] [8,4] [16,8]           m = 91: [2] [2,2] [16,8] [32,16]
m = 46: [2] [8] [16] [32]                m = 93: [2][2,2][2,2,2,2][2,2,2,2,2,2,2,2]
m*= 47: [8] [16,2] [32,4,4] [64,8,8]     m = 94: [4] [16,2] [32,4,4] [64,8,8]
m = 51: [2] [2,2] [2,2,2,2] [8,4,4,4]    m*= 95: [4] [8] [16] [32]
m*= 55: [4] [8] [16] [32]                m = 97: [2][2,2][2,2,2,2][4,2,2,2,2,2,2]
m = 57: [2] [64] [128] [256]             m = 102:[2] [2,2] [2,2,2,2] [8,4,4,4]
```

4.3.2. *Groups $\widetilde{\mathcal{C}\ell}$.* For the properties of the logarithmic class groups $\widetilde{\mathcal{C}\ell}$, see the fundamental works of Jaulent ([21], [24, Théorème 4.5, Remarque (i)]). In particular, it is shown that Greenberg's conjecture is equivalent to the same conjecture for the

[3]See [13, Appendix] for the long story of p-rationality then [7, IV (b)] for the technical use and [31] for cohomological presentation. This proposition is known for instance from [25, 40] among others.

groups $\mathcal{C}\ell'$ and for the groups $\widetilde{\mathcal{C}\ell}$. On the contrary (see Proposition 4.4), the Iwasawa invariants of the $\mathbb{Z}_p[[\Gamma]]$-modules $\varprojlim \mathcal{T}_{k_n}$ and $\varprojlim \mathcal{T}^{\rm bp}_{k_n}$ are in general nontrivial (this may also be seen via reflection theorem, [23, Téorème 2.12] and generalizations in [40]).

4.4. **Criteria of Iwasawa's theory type.** We summarize, without proofs, some well-known characterizations of Greenberg's conjecture. If one replaces k by a stage $K \subset k_\infty$, all the forthcoming statements hold true for K and its tower $\bigcup_{n\geq 0} K_n$, $[K_n : K] = p^n$ (cf. conventions of Remark 1.1); we assume the Leopoldt and Gross–Kuz'min conjectures for totally real number fields. We use the classical objects $A_\infty := \varinjlim \mathcal{C}\ell_{k_n}$, $X_\infty := \varprojlim \mathcal{C}\ell_{k_n}$, A'_∞, X'_∞, from the S_{k_n}-class groups $\mathcal{C}\ell'_{k_n}$, where S_{k_n} is the set of p-places of k_n (recall that $\widetilde{\mathcal{C}\ell}_k \simeq (X_\infty)_\Gamma$).
Let $\mathcal{C}\ell^{[p]}_{k_n} = \mathrm{Ker}(\mathcal{C}\ell_{k_n} \to \mathcal{C}\ell'_{k_n})$ and $\widetilde{\mathcal{C}\ell}^{[p]}_{k_n} = \mathrm{Ker}(\widetilde{\mathcal{C}\ell}_{k_n} \to \mathcal{C}\ell'_{k_n})$ (cf. Diagram 4.2).

Proposition 4.6. *Greenberg's conjecture is equivalent to each of the following:*

(i) X_∞ *is finite;* *(i′)* X'_∞ *is finite;* *(ii)* $A_\infty = 0$*;* *(ii′)* $A'_\infty = 0$*;*
(iii) $\mathcal{C}\ell_{k_n}$ *capitulates in* k_∞*;* *(iii′)* $\mathcal{C}\ell'_{k_n}$ *capitulates in* k_∞ *(for all* $n \geq 0$*);*
(iv) $\mathrm{N}_{k_m/k_n}(\mathcal{C}\ell_{k_m}) \simeq \mathcal{C}\ell_{k_n}$*;* *(iv′)* $\mathrm{N}_{k_m/k_n}(\mathcal{C}\ell'_{k_m}) \simeq \mathcal{C}\ell'_{k_n}$ *(for all* $m \geq n \gg 0$*);*
(v) $\widetilde{\mathcal{C}\ell}_{k_n}$ *capitulates in* k_∞ *for all* $n \geq 0$*;* *(vi)* $\mathcal{C}\ell_{k_m}^{G_{m/n}} = \mathcal{C}\ell_{k_m}$ *for all* $m \gg n \gg 0$*;*
(vii) $s_p = 1$*:* $\mathcal{C}\ell_k$ *capitulates in* k_∞*;* *(viii)* $s_p = d$*: for all* $n \gg 0$*,* $\mathcal{C}\ell_{k_n}^{G_n} = cl_{k_n}(S_{k_n})$*.*

Most characterizations are due to many authors after Iwasawa; see [16], [21], [26, Théorèmes 4, 5, 7], [27], [32, Théorème 4.2], [35, Proposition 1.1, Théorème 2.1]. Point (v) is Jaulent's criterion [24]; point (vi) follows from Theorem 4.1 (ii) and expresses that Greenberg's conjecture is equivalent to the triviality of the algorithm in k_m/k_n for all $m \geq n \gg 0$ (to be detailed in Section 5.1). Points (vii) and (viii) are the two Greenberg theorems [15, Theorems 1, 2]

Remark 4.7. In our opinion, these aesthetic statements are translations, into algebraic Iwasawa's theory, of standard formalism of class field theory and classical p-adic analytic objects of L-function type (as in the important achievement [17] for the totally real case, among many other articles). In other words, *the diophantine aspects of construction, computation or annihilation (in a "numerical" setting), of the class groups in* k_∞*, are not taken into account.* As for the well-known abelian case, one is able to give (nontrivial) equivalences between several theories (essentially Iwasawa's theory and p-adic L-functions), giving famous "main conjectures" and "main theorems", but without information on the orders of magnitude, nor on density results. We will show how this construction works and study its arithmetic complexity which becomes oversized in the tower as soon as $\lambda + \mu \neq 0$ (Corollary 5.5 in Section 5.1). These observations are strengthened by the results of [29] which show (using deep techniques in the case of degree p cyclic extensions) that it is quite possible to obtain density results and some proofs "with probability 1".

5. Filtration of $\mathcal{C}\ell_{k_n}$

5.1. **General algorithm – Class and Norm factors.** Let I_{k_n}, $n \geq 0$, be the group of ideals of k_n prime to p. In the framework of the general algorithm of computation of the p-class group $\mathcal{C}\ell_{k_n}$ of k_n, by means of "unscrewing" in a cyclic p-extension, one uses the filtration of $M_n := \mathcal{C}\ell_{k_n}$:

$$M_n^i =: cl_{k_n}(\mathscr{M}_n^i),\ \mathscr{M}_n^i \subset I_{k_n},\ i \geq 0,$$

the $\mathscr{M}_n^i$ being finitely generated subgroups of I_{k_n}, defined inductively as follows (from [9, Corollary 3.7]):

Definition 5.1. *For n 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 $G_n := \mathrm{Gal}(k_n/k) =: \langle\, \sigma_n \,\rangle$ and where b_n is the least integer i such that $M_n^i = M_n$ (i.e., such that $M_n^{i+1} = M_n^i$).*

Proposition 5.2. *This filtration has the following properties:*

(*i*) *For $i = 0$, one obtains $M_n^1 = M_n^{G_n}$ (group of ambiguous classes in k_n/k).*
(*ii*) *One has $M_n^i = \{c \in M_n,\ c^{(1-\sigma_n)^i} = 1\}$, for all $i \geq 0$.*
(*iii*) *For n fixed, the i-sequence $\#(M_n^{i+1}/M_n^i)$, $0 \leq i \leq b_n$, is decreasing to 1 and has the upper bound $\#M_n^1$ since $M_n^{i+1}/M_n^i \hookrightarrow M_n^i/M_n^{i-1}$ from the action of $1-\sigma_n$.*
(*iv*) $\#M_n^{b_n} = \prod_{i=0}^{b_n-1} \#(M_n^{i+1}/M_n^i)$.

Recall that for n fixed, a generalization of the Chevalley ambiguous class number formula [9, Formula (29), § 3.2] [4], leads, by means of the norm groups $\mathrm{N}_{k_n/k}(M_n^i) = \mathscr{C}\ell_{k_n}(\mathrm{N}_{k_n/k}(\mathscr{M}_n^i))$ and the groups of numbers $\Lambda_n^i := \{x \in k^\times,\ (x) \in \mathrm{N}_{k_n/k}(\mathscr{M}_n^i)\}$, to the i-sequence: $\#\big(M_n^{i+1}/M_n^i\big) = \dfrac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_n^i)} \cdot \dfrac{p^{n\cdot(s_p-1)}}{(\Lambda_n^i : \Lambda_n^i \cap \mathrm{N}_{k_n/k}(k_n^\times))}$, where:

$$\frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_n^i)} \quad \& \quad \frac{p^{n\cdot(s_p-1)}}{(\Lambda_n^i : \Lambda_n^i \cap \mathrm{N}_{k_n/k}(k_n^\times))} \tag{7}$$

are integers called *the class factor* and *the norm factor*, respectively, at the step i of the algorithm in the stage k_n. These factors are independent of the choice of the ideals in $\mathscr{M}_n^i$ up to principal ideals of k_n and the groups Λ_n^i may be defined up to $\mathrm{N}_{k_n/k}(k_n^\times)$. The groups $\mathscr{M}_n^i$ are built inductively from $\mathscr{M}_n^0 = 1$, hence $\Lambda_n^0 = E_k$ [10, § 6.2]; then $\mathscr{M}_n^1$ is generated by ideals $\mathfrak{A}$ of k_n, prime to p, such that $\mathfrak{A}^{1-\sigma_n} = (\alpha)$, $\alpha \in k_n^\times$, which is equivalent to solve $\varepsilon = \mathrm{N}_{k_n/k}(\alpha)$, with $\varepsilon \in E_k$ local norm at the p-places.

From the above, we can state, for any fixed integer n:

Theorem 5.3. (i) *The class factors $\dfrac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_n^i)}$ divide the order of $\mathcal{C}\ell_k$ and define a decreasing i-sequence of integers from $\#\mathcal{C}\ell_k$.*

(ii) *The norm factors $\dfrac{p^{n\cdot(s_p-1)}}{(\Lambda_n^i : \Lambda_n^i \cap \mathrm{N}_{k_n/k}(k_n^\times))}$ divide the order of $\mathcal{R}_k^{\mathrm{nr}} := \mathcal{R}_k/\mathcal{R}_k^{\mathrm{ram}}$ (see Diagram 3.7, § 3.3) and define a decreasing i-sequence of integers from $i = 0$ where $\Lambda_n^0 = E_k \subseteq \cdots \subseteq \Lambda_n^i \subseteq \Lambda_n^{i+1} \cdots$.*

Proof. For the norm factors, this comes from the injective maps:

$$E_k/E_k\cap\mathrm{N}_{k_n/k}(k_n^\times) \hookrightarrow \cdots \hookrightarrow \Lambda_n^i/\Lambda_n^i\cap\mathrm{N}_{k_n/k}(k_n^\times) \hookrightarrow \Lambda_n^{i+1}/\Lambda_n^{i+1}\cap\mathrm{N}_{k_n/k}(k_n^\times) \hookrightarrow \cdots$$

Then $\dfrac{p^{n\cdot(s_p-1)}}{(\Lambda_n^i : \Lambda_n^i \cap \mathrm{N}_{k_n/k}(k_n^\times))}$ divides $\#\mathcal{R}_k^{\mathrm{nr}}$, with equality for $n \gg 0$ (§ 3.3). □

Therefore, for $i = b_n$, using the above expressions (7), we obtain $M_n^{b_n} = \mathcal{C}\ell_{k_n}$, $\mathrm{N}_{k_n/k}\big(M_n^{b_n}\big) = \mathcal{C}\ell_k$ and $(\Lambda_n^{b_n} : \Lambda_n^{b_n} \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(s_p-1)}$, which explains that $\#\mathcal{C}\ell_{k_n}$ essentially depends on the number of steps b_n of the algorithm, which will be expressed in terms of Iwasawa invariants as follows under the convention of Remark 1.1.

[4] The generalization to arbitrary cyclic extensions was given in [6], then translated into english in [9] with improvements. So it applies in the k_n/k.

Theorem 5.4. *Let $\mathcal{R}_k^{\rm nr} := {\rm Gal}(H_k^{\rm gen}/k_\infty H_k)$ (Diagram 3.7, § 3.3), where $H_k^{\rm gen}$ is the union of the genus class fields $H_{k_m/k}$ (Proposition 3.6). Let $n_0 \geq 0$ be such that, for all $n \geq n_0$, the Iwasawa formula $\#\mathcal{C}\ell_{k_n} = p^{\lambda\cdot n+\mu\cdot p^n+\nu}$ is fulfilled. Let b_n be the length of the algorithm. Then (where v_p denotes the p-adic valuation):*

(i) One has $b_n \leq \lambda\cdot n+\mu\cdot p^n+\nu \leq v_p(\#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr})\cdot b_n$ for all $n \geq n_0$.
(ii) If $\mathcal{C}\ell_k = \mathcal{R}_k^{\rm nr} = 1$, then $\lambda = \mu = \nu = 0$.

Proof. Consider $M_n := \mathcal{C}\ell_{k_n}$. As $\#\big(M_n^{i+1}/M_n^i\big) \geq p$ for $0 \leq i \leq b_n - 1$, the Proposition 5.2 (iv) implies $\#\mathcal{C}\ell_{k_n} = \#M_n^{b_n} \geq p^{b_n}$; whence $b_n \leq \lambda\cdot n+\mu\cdot p^n+\nu$; then, from the fact that $\#\big(M_n^{i+1}/M_n^i\big) \mid \#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr}$, (Theorem 5.3) this yields $\#\big(M_n^{i+1}/M_n^i\big) \leq \#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr}$ for $0 \leq i \leq b_n - 1$; whence $\#\mathcal{C}\ell_{k_n} \leq (\#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr})^{b_n}$ from Proposition 5.2 (iv), which completes the proof of (i). Point (ii) implies $\mathcal{G}_{k_n/k} = 1$, whence $\mathcal{C}\ell_{k_n} = 1$. □

Corollary 5.5. *If $\#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr} \neq 1$, the number of steps b_n of the algorithm fulfills the following inequality linking Iwasawa's theory and algorithmic complexity:*

$$b_n \geq \frac{1}{v_p(\#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr})}\big(\lambda\cdot n+\mu\cdot p^n+\nu\big),\ \textit{for all } n \geq n_0.$$

We know also that taking, as base field, a stage $K \subset k_\infty$, large enough, one may expect (from Theorem 4.1 (ii)) that the algorithm in K_m/K ($[K_m : K] = p^m$ and $G_m = {\rm Gal}(K_m/K)$, $m \geq 0$) gives $b_m = 1$, i.e., $\mathcal{C}\ell_{K_m}^{G_m} = \mathcal{C}\ell_{K_m}$, of order p^ν, for all $m \geq 0$. This means that the class and norm factors trivialize at the first step of the algorithm: ${\rm N}_{K_m/K}(\mathcal{C}\ell_{K_m}^{G_m}) = \mathcal{C}\ell_K$ and $(\Lambda_m^1 : \Lambda_m^1 \cap {\rm N}_{K_m/K}(K_m^\times)) = p^{m\,(s_p-1)}$, for all $m \geq 0$.

Example 5.6. This stage K is not effective; so we have computed the structure of $\mathcal{C}\ell_{k_n}$, $n \in [0,4]$, for real quadratic fields $k = \mathbb{Q}(\sqrt{m})$ and $p = 2$. If $m \equiv 2 \pmod 8$, the first stage k_1 is contained in H_k, which gives an exception to the surjectivity $\mathcal{C}\ell_{k_n} \to \mathcal{C}\ell_k$, of the norm map and explains that in this case one must take k_1 as base field (e.g., $m = 10$). We give some excerpts which only suggest a rapid stabilization:

m=10	[2] [] [] [] []	m=226	[8] [4] [4] [4]
m=15	[2] [2] [2] [2] [2]	m=267	[2] [2,2] [4,2] [4,2]
m=41	[] [2] [4] [8] [8]	m=291	[4] [4,2] [4,2] [4,2]
m=51	[2] [2,2] [2,2] [2,2] [2,2]	m=323	[4] [8,2] [8,2] [8,2]
m=65	[2] [4] [4] [4] [4]	m=357	[2] [2,2] [4,2,2] [4,2,2]
m=82	[4] [2] [4] [8] [8]	m=399	[4,2] [4,2] [4,2] [4,2]
m=113	[] [4] [4] [4] [4]	m=435	[2,2] [4,2] [4,2] [4,2]
m=119	[2] [2,2] [2,2,2] [2,2,2]	m=442	[4,2] [4] [4] [4]
m=130	[2,2] [4] [4] [4] [4]	m=483	[2,2] [2,2,2] [2,2,2] [2,2,2]
m=137	[] [2] [4] [4] [4]	m=1011	[4] [4,2] [4,2,2,2] [4,2,2,2]
m=145	[4] [4] [4] [4] [4]	m=1023	[4,2] [8,2] [16,2] [32,2] [64,2]
m=219	[4] [4,2] [4,2] [4,2]	m=30030	[2,2,2,2] [4,4,2,2] [8,4,2,2] [8,4,2,2]

The case of $m = 1023 = 3\cdot 11\cdot 31$ does not show a stabilization at the stage k_4 (unfortunately it took three days of computer to get $\mathcal{C}\ell_{k_4} = [64,2]$); we have $\#\mathcal{C}\ell_k = 8$, $\#\mathcal{R}_k = \#\mathcal{R}_k^{\rm ram} = 16$ and $\mathcal{T}_k = [64,2]$, but $\mathcal{T}_{k_3} = [512, 32, 8, 2, 2, 2, 2, 2, 2]$ which may explain the difficulties. Since $\mathcal{R}_k^{\rm nr} = 1$, we have $\widetilde{\mathcal{C}\ell}_k \simeq \mathcal{C}\ell'_k \simeq \mathbb{Z}/4\mathbb{Z}$ which is here such that $\mathcal{C}\ell_k = \mathcal{C}\ell'_k \oplus \mathbb{Z}/2\mathbb{Z}$ (we compute that $\widetilde{\mathcal{C}\ell}_{k_1} \simeq \mathbb{Z}/8\mathbb{Z}$, $\widetilde{\mathcal{C}\ell}_{k_2} \simeq \mathbb{Z}/16\mathbb{Z}$, $\widetilde{\mathcal{C}\ell}_{k_3} \simeq \mathbb{Z}/32\mathbb{Z}$).

Remark 5.7. At this step of the study, we make the following observations: Greenberg's conjecture reduces to an estimation of the number b_n of steps of the algorithm. But b_n (n fixed) depends of the i-progression of the class and norm factors (7) and under natural probabilities on their evolution (Theorem 5.3), each of them is, a priori, rapidly trivial since the computations only use the complexity of the base field k (i.e.,

$\mathcal{C}\ell_k$ and $\mathcal{R}_k^{\rm nr}$). We observe the huge discontinuity between the cases $\#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\rm nr} = 1$ ($b_n = 0$, $\lambda = \mu = \nu = 0$) and $\#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\rm nr} \neq 1$ with $\lambda + \mu \neq 0$ (giving $b_n \to \infty$ with n). But the most spectacular argument is that, for K large enough in k_∞ one must find, in practice, $b_m = 1$ from Theorem 4.1 (ii) giving, for $m \geq 0$, $\mathcal{C}\ell_{K_m}^{G_m} = \mathcal{C}\ell_{K_m}$ of order p^ν as the numerical experiments show.

We do not know any analogous algorithm computing the filtration $\overline{M}_n^i$ of $\overline{M}_n := \mathcal{T}_{k_n}$ (or for the $\mathcal{T}_{k_n}^{\rm bp}$ or the $\mathcal{R}_{k_n}$); it seems that either such algorithm does not exist or is of a very different nature, so that there is no contradiction with the fact that $\overline{\lambda}$ is often non-zero. In particular, one sees that the analogue of Chevalley's formula is rather trivial since $\mathcal{T}_{k_n}^{G_n} = {\rm J}_{k_n/k}(\mathcal{T}_k) \simeq \mathcal{T}_k$ (i.e., $\overline{M}_n^1 \simeq \mathcal{T}_k$), without any "class factor" since $\dfrac{\#\mathcal{T}_k}{{\rm N}_{k_n/k}({\rm J}_{k_n/k}(\mathcal{T}_k))} = \#\mathcal{T}_k$ as soon as p^n is larger than the exponent p^e of $\mathcal{T}_k$, nor any "normic factor".

On the contrary, such an algorithm very probably exists for the filtration $\widetilde{M}_n^i := \widetilde{\mathcal{C}\ell}_{k_n}^i$ of the logarithmic class groups $\widetilde{\mathcal{C}\ell}_{k_n}$ and implies the same comments and conclusions as those given in this paper.

5.2. **The n-sequences $\mathcal{C}\ell_{k_n}^{i+1}/\mathcal{C}\ell_{k_n}^i$ for i fixed.** Now, contrary to the previous studies, we fix the step i of the algorithms and consider the n-sequence of integers $\#\big(M_n^{i+1}/M_n^i\big) := \#\big(M_n/M_n^i\big)^{G_n}$ from their class and norm factors (7), knowing that $M_n^i := \mathcal{C}\ell_{k_n}$ if $i \geq b_n$. One has, for all $n \geq 0$, the following diagram where the norm maps ${\rm N}_{k_{n+1}/k_n}$, on M_{n+1} and $(M_{n+1})^{(1-\sigma_{n+1})^i}$, are surjective since $H_{k_n} \cap k_{n+1} = k_n$, but not necessarily on M_{n+1}^i (they are, a priori, not injective nor surjective):

Diagram 5.8.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & M_{n+1}^i & \longrightarrow & M_{n+1} & \xrightarrow{(1-\sigma_{n+1})^i} & (M_{n+1})^{(1-\sigma_{n+1})^i} & \longrightarrow & 1 \\
 & & {\scriptstyle {\rm N}_{k_{n+1}/k_n}}\downarrow & & {\scriptstyle {\rm N}_{k_{n+1}/k_n}}\Downarrow & & {\scriptstyle {\rm N}_{k_{n+1}/k_n}}\Downarrow & & \\
1 & \longrightarrow & M_n^i & \longrightarrow & M_n & \xrightarrow{(1-\sigma_n)^i} & (M_n)^{(1-\sigma_n)^i} & \longrightarrow & 1\,.
\end{array}$$

We have ${\rm N}_{k_{n+1}/k_n}(M_{n+1}^i) \subseteq M_n^i$; thus, for all $\mathfrak{A}_{n+1} \in \mathscr{M}_{n+1}^i$, we obtain a relation of the form ${\rm N}_{k_{n+1}/k_n}(\mathfrak{A}_{n+1}) = (\alpha_n)\,\mathfrak{A}_n$, where $\alpha_n \in k_n^\times$ and $\mathfrak{A}_n \in \mathscr{M}_n^i$, in what case, *modifying* $\mathscr{M}_n^i$ modulo suitable principal ideals, one gets ${\rm N}_{k_{n+1}/k_n}(\mathscr{M}_{n+1}^i) \subseteq \mathscr{M}_n^i$, whence ${\rm N}_{k_{n+1}/k}(\mathscr{M}_{n+1}^i) \subseteq {\rm N}_{k_n/k}(\mathscr{M}_n^i)$; this reduces to modify $\Lambda_n^i = \{x \in k^\times, (x) \in {\rm N}_{k_n/k}(\mathscr{M}_n^i)\}$ modulo ${\rm N}_{k_n/k}(k_n^\times)$ leaving invariant $(\Lambda_n^i : \Lambda_n^i \cap {\rm N}_{k_n/k}(k_n^\times))$. So, one may suppose that, for all given $m \geq n$:

$$\Lambda_m^i \subseteq \cdots \subseteq \Lambda_{n+1}^i \subseteq \Lambda_n^i. \tag{8}$$

Theorem 5.9. *For all $i \geq 0$ fixed, $\#\big(M_n^{i+1}/M_n^i\big)$ define an increasing stationary n-sequence of divisors of $\#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\rm nr}$, and $\#M_n^i$ define an increasing stationary n-sequence. Thus $\lim\limits_{n\to\infty} \#\big(M_n^{i+1}/M_n^i\big) =: p^{c^i}p^{\rho^i}$, $p^{c^i} \mid \#\mathcal{C}\ell_k$, $p^{\rho^i} \mid \#\mathcal{R}_k^{\rm nr}$. The i-sequences p^{c^i} and p^{ρ^i} are decreasing, stationary at a divisor of $\#\mathcal{C}\ell_k$ and $\mathcal{R}_k^{\rm nr}$, respectively.*

Proof. As ${\rm N}_{k_{n+1}/k}(M_{n+1}^i) \subseteq {\rm N}_{k_n/k}(M_n^i)$, the class factors $\frac{\#\mathcal{C}\ell_k}{\#{\rm N}_{k_n/k}(M_n^i)}$ define an *increasing* n-sequence $p^{c_n^i}$, stationary at a maximal value $p^{c^i} \mid \#\mathcal{C}\ell_k$. The norm factors are $\frac{p^{n\cdot(s_p-1)}}{\#\omega_n(\Lambda_n^i)} =: p^{\rho_n^i}$ (see § 3.2) and $p^{\rho_{n+1}^i - \rho_n^i} = p^{s_p-1}\,\frac{\#\omega_n(\Lambda_n^i)}{\#\omega_{n+1}(\Lambda_{n+1}^i)}$; since by (8) one may assume $\Lambda_{n+1}^i \subseteq \Lambda_n^i$, this yields $\#\omega_{n+1}(\Lambda_{n+1}^i) \leq \#\omega_{n+1}(\Lambda_n^i)$, then we obtain $p^{\rho_{n+1}^i - \rho_n^i} \geq p^{s_p-1}\,\frac{\#\omega_n(\Lambda_n^i)}{\#\omega_{n+1}(\Lambda_n^i)}$; in the restriction $\Omega(k_{n+1}/k) \longrightarrow\!\!\!\!\!\rightarrow \Omega(k_n/k)$ of Hasse's

symbols (with kernel isomorphic to $\mathbb{F}_p^{s_p-1}$), the image of $\omega_{n+1}(\Lambda_n^i)$ is $\omega_n(\Lambda_n^i)$, whence an increasing n-sequence $p^{\rho_n^i} \mid \#\mathcal{R}_k^{\rm nr}$. Thus $\lim_{n\to\infty} \#\big(M_n^{i+1}/M_n^i\big) = p^{c^i}\cdot p^{\rho^i} \mid \#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr}$.
If one assumes, by induction, that the n-sequence $\#M_n^i$ is increasing stationary, the property follows for the n-sequence $\#M_n^{i+1}$. Whence the first part of the claim.
For n large enough (to get $c_n^i =: c^i$ and $\rho_n^i =: \rho^i$), we have $\frac{\#{\rm N}_{k_n/k}(M_n^i)}{\#{\rm N}_{k_n/k}(M_n^{i+1})} \leq 1$ and $\frac{\#\omega_n(\Lambda_n^i)}{\#\omega_n(\Lambda_n^{i+1})} \leq 1$ since $\Lambda_n^i\cdot{\rm N}_{k_n/k}(k_n^\times) \subseteq \Lambda_n^{i+1}\cdot{\rm N}_{k_n/k}(k_n^\times)$. □

Corollary 5.10. *There exists $i_{\min}\geq 0$ and some constants $c\geq 0$, $\rho\geq 0$ such that $c^i = c$ et $\rho^i = \rho$ for all $i\geq i_{\min}$. Whence $\lim\limits_{i\to\infty}\big(p^{c^i}\cdot p^{\rho^i}\big) = p^{c+\rho} \mid \#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr}$ and Greenberg's conjecture holds true if and only if $c=\rho=0$ (from Theorem 5.4).*

Remark 5.11. From Theorem 4.1 (ii), under Greenberg's conjecture, the previous results should be, for a base field K large enough in k_∞ (cf. Remark 1.1), that $M_n^i = M_n^1$, $c^i=\rho^i=0$, for all $i\geq 1$; thus $i_{\min}\leq 1$, $b_n\leq 1$, $c=\rho=0$. Unfortunately, numerical examples need to take K large enough, which is not effective. We refer to [10, 12] for complements, conjectures and numerical experiments

For $x\in\Lambda_n^i$ we have $(x) = {\rm N}_{k_n/k}(\mathfrak{A})$, $\mathfrak{A}\in\mathscr{M}_n^i$, and when x is local norm at p, hence $x = {\rm N}_{k_n/k}(y_n)$, $y_n\in k_n^\times$, the random aspects occur in the mysterious "evolution relation" from the equality ${\rm N}_{k_n/k}(y_n) = {\rm N}_{k_n/k}(\mathfrak{A})$, giving the existence of $\mathfrak{B}$ (having, a priori, no obvious algebraic link with the previous data), such that:

$$(y_n) = \mathfrak{A}\,\mathfrak{B}^{1-\sigma_n} \mapsto \mathfrak{B}\in\mathscr{M}_n^{i+1} \mapsto {\rm N}_{k_n/k}(\mathfrak{B}) \mapsto \Lambda_n^{i+1}\cdots \tag{9}$$

6. $\mathcal{C}\ell_k$ and $\mathcal{R}_k$ as governing invariants of the algorithms

We have seen the significance of the ideals of k of the form ${\rm N}_{k_n/k}(\mathfrak{A})$. This concerns the class factors $\frac{\#\mathcal{C}\ell_k}{\#{\rm N}_{k_n/k}(M_n^i)}$ where ${\rm N}_{k_n/k}(M_n^i)$ is generated by the $c\ell_k({\rm N}_{k_n/k}(\mathfrak{A}))$, $\mathfrak{A}\in\mathscr{M}_n^i\subset I_{k_n}$ (prime to p ideals of k_n), where the $\mathscr{M}_n^i$ (n fixed) are given by the algorithm, and the norm factors $\frac{p^{n\cdot(s_p-1)}}{(\Lambda_n^i : \Lambda_n^i\cap{\rm N}_{k_n/k}(k_n^\times))}$, where $\Lambda_n^i = \big\{x\in k^\times,\ (x) = {\rm N}_{k_n/k}(\mathfrak{A})\big\}$, $\mathfrak{A}\in\mathscr{M}_n^i$ as above.
We have seen that the ideals $\mathfrak{A}\in\mathscr{M}_n^i$ may be arbitrarily modified modulo principal ideals of k_n, whence ${\rm N}_{k_n/k}(\mathfrak{A})$ defined up to ${\rm N}_{k_n/k}(k_n^\times)$ and prime to p. This non-unicity hides some structural aspects of Greenberg's conjecture that we intend to analyze in relation with the invariant $\mathcal{T}_k$, more precisely its "sub-invariants" $\mathcal{C}\ell_k$ and $\mathcal{R}_k$, to obtain canonical representatives of these ideals and finite in number.

6.1. Decomposition of ${\rm N}_{k_n/k}(\mathfrak{A})$ – 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 such that $H_k^{\rm pr}$ be the direct compositum of F and $k_\infty H_k$ over H_k (which is possible because $k_\infty\cap H_k = k$); we put $\Gamma = {\rm Gal}(H_k^{\rm pr}/F)\simeq\mathbb{Z}_p$ (see Diagram 4.3). We 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 $\mathcal{A}_k$ and $\mathcal{A}_{k_n}$; their kernels are the groups of infinitesimal principal ideals $\mathcal{P}_{k,\infty}$ and $\mathcal{P}_{k_n,\infty}$, where $\mathcal{P}_{k,\infty}$ is the set of ideals (x_∞), $x_\infty\in k^\times\otimes\mathbb{Z}_p$, prime to p, such that $\iota x_\infty = 1$ in U_k (idem for k_n) (see, e.g., [7, Theorem III.2.4, Proposition III.2.4.1] and [22, Chap. 1, § (d)]).

The action of the arithmetic norm in k_n/k (or restriction) is given by:

$$\mathrm{N}_{k_n/k}(\mathcal{A}_{k_n}) = \mathrm{Gal}(H_k^{\mathrm{pr}}/k_n) \text{ and } \mathrm{N}_{k_n/k}(\mathcal{T}_{k_n}) = \mathcal{T}_k. \tag{10}$$

Let $\mathfrak{t} \in I_k \otimes \mathbb{Z}_p$ of finite order modulo $\mathcal{P}_{k,\infty}$ (i.e., whose Artin symbol is in $\mathcal{T}_k$). Then $\mathfrak{t}$ is principal if and only if its Artin symbol is in $\mathrm{Gal}(H_k^{\mathrm{pr}}/k_\infty H_k)$; in that case, $\mathfrak{t} = (\tau)$, $\tau \in k^\times \otimes \mathbb{Z}_p$ such that $\tau^{p^e} = \varepsilon \cdot x_\infty$, for some $e \geq 0$, $\varepsilon \in E_k \otimes \mathbb{Z}_p$, $\iota x_\infty = 1$.
In the sequel, x_∞, $y_\infty \ldots$, always denote "infinitesimal" elements, taking into account the following lemma:

Lemma 6.1. *If $(x_\infty) \in \mathcal{P}_{k,\infty} \cap \mathrm{N}_{k_n/k}(I_{k_n} \otimes \mathbb{Z}_p)$, then $(x_\infty) \in \mathrm{N}_{k_n/k}(\mathcal{P}_{k_n,\infty})$.*

Proof. The assumption implies $x_\infty = \mathrm{N}_{k_n/k}(y)$, $y \in k_n^\times \otimes \mathbb{Z}_p$; we check, using the total ramification of p in k_n/k, that y is prime to p. Thus we get $\iota \mathrm{N}_{k_n/k}(y) = \mathrm{N}_{k_n/k}(\iota y) = 1$ and $\iota y = u^{1-\sigma_n}$, $u \in U_{k_n}$; write $u = \iota z$, $z \in k_n^\times \otimes \mathbb{Z}_p$, then $\iota y = \iota(z^{1-\sigma_n})$ giving $y = z^{1-\sigma_n} \cdot y_\infty$, whence $x_\infty = \mathrm{N}_{k_n/k}(y_\infty)$. □

The link between ideal norms in k_n/k and the torsion group $\mathcal{T}_k$ (more precisely $\mathcal{C}\ell_k$ and $\mathcal{R}_k$) is given, for n large enough, by the following main result:

Theorem 6.2. *Let $\mathcal{A}_k = \mathcal{T}_k \oplus \Gamma$, $\mathcal{A}_{k_n} = \mathcal{T}_{k_n} \oplus \Gamma_n$, be any decompositions as illustrated by Diagram 4.3. Let $\mathfrak{A} \in I_{k_n} \otimes \mathbb{Z}_p$ (prime to p ideal of k_n).*
(i) There exist (modulo $\mathcal{P}_{k_n,\infty}$) unique ideals $\mathfrak{T}, \mathfrak{C} \in I_{k_n} \otimes \mathbb{Z}_p$, such that:

$$\mathfrak{A} = \mathfrak{T} \cdot \mathfrak{C} \cdot (y_\infty), \quad \text{with } (y_\infty) \in \mathcal{P}_{k_n,\infty}, \ \left(\frac{H_{k_n}^{\mathrm{pr}}/k_n}{\mathfrak{T}}\right) \in \mathcal{T}_{k_n}, \ \left(\frac{H_{k_n}^{\mathrm{pr}}/k_n}{\mathfrak{C}}\right) \in \Gamma_n.$$

(ii) There exists $c \in k^\times \otimes \mathbb{Z}_p$ and $(x_\infty) \in \mathcal{P}_{k,\infty}$ such that $\mathrm{N}_{k_n/k}(\mathfrak{C}) = (c^{p^n}) \cdot (x_\infty)$.
(iii) There exists $\alpha_n \in k_n^\times \otimes \mathbb{Z}_p$ such that $\mathrm{N}_{k_n/k}(\mathfrak{A}\,(\alpha_n)) = \mathrm{N}_{k_n/k}(\mathfrak{T}) =: \mathfrak{t}$, with $\left(\frac{H_k^{\mathrm{pr}}/k}{\mathfrak{t}}\right) \in \mathcal{T}_k$ and $\iota \mathrm{N}_{k_n/k}(\alpha_n)$ arbitrarily close to 1 in U_k regarding n.
(iv) The representative $\mathfrak{t}$, associated to the class $\mathrm{N}_{k_n/k}(\mathfrak{A}) \cdot \mathrm{N}_{k_n/k}(k_n^\times \otimes \mathbb{Z}_p)$, is unique (modulo $\mathcal{P}_{k,\infty}$) and does not depend on the choices of F and F_n ($n \gg 0$).

Proof. (i) Since Γ and Γ_n are free components, $\mathfrak{A}$ is of the required form, with unicity of $\mathfrak{T}$ and $\mathfrak{C}$ modulo $\mathcal{P}_{k_n,\infty}$.
(ii) By restriction, the image of Γ_n in Γ is Γ^{p^n}; thus $\mathrm{N}_{k_n/k}(\mathfrak{C}) = \mathfrak{c}^{p^n}\,(x_\infty)$ for an ideal $\mathfrak{c} \in I_k \otimes \mathbb{Z}_p$ such that $\left(\frac{H_k^{\mathrm{pr}}/k}{\mathfrak{c}}\right) \in \Gamma$ and $(x_\infty) \in \mathcal{P}_{k,\infty}$; but since $H_k \subseteq F$, $\left(\frac{H_k^{\mathrm{pr}}/k}{\mathfrak{c}}\right)\Big|_{H_k} = \left(\frac{H_k/k}{\mathfrak{c}}\right) = 1$, hence $c\ell_k(\mathfrak{c}) = 1$ and $\mathfrak{c} = (c)$, $c \in k^\times \otimes \mathbb{Z}_p$.
(iii) We have $\mathrm{N}_{k_n/k}(\mathfrak{A}) = \mathrm{N}_{k_n/k}(\mathfrak{T})\,(c^{p^n})\,(x_\infty)\,\mathrm{N}_{k_n/k}(y_\infty) =: \mathfrak{t}\,(c^{p^n})\,(x'_\infty)$, where $\left(\frac{H_k/k}{\mathfrak{t}}\right) \in \mathcal{T}_k$. From Lemma 6.1, $x'_\infty = \mathrm{N}_{k_n/k}(y'_\infty)$, whence $\mathrm{N}_{k_n/k}\big(\mathfrak{A}\,(c)^{-1}\,(y'_\infty)^{-1}\big) =: \mathfrak{t}$. Let $\alpha_n = c^{-1}\,y'^{-1}_\infty$; then $\iota \mathrm{N}_{k_n/k}(\alpha_n) = \iota(c^{-p^n})$ is arbitrarily close to 1 regarding n.
(iv) Let F'/k be another solution; we get, with obvious notations for F, F', with $u := \mathrm{N}_{k_n/k}(\alpha_n)$, $u' := \mathrm{N}_{k_n/k}(\alpha'_n)$, ιu, $\iota u'$ arbitrary close to 1 regarding n, $\mathrm{N}_{k_n/k}(\mathfrak{A}) \cdot (u) = \mathfrak{t}$, $\mathrm{N}_{k_n/k}(\mathfrak{A}) \cdot (u') = \mathfrak{t}'$.
Whence $\mathfrak{t}'\,\mathfrak{t}^{-1} = (a)$ with ιa close to 1. So, if p^e is the exponent of $\mathcal{T}_k$, we get $(a)^{p^e} = (a_\infty) \in \mathcal{P}_{k,\infty}$, which gives $a^{p^e} = \varepsilon\, a_\infty$, $\varepsilon \in E_k \otimes \mathbb{Z}_p$ with $\iota\varepsilon$ close to 1, hence of the form $\varepsilon = \eta^{p^e}$, $\eta \in E_k \otimes \mathbb{Z}_p$, with $\iota\eta$ close to 1 assuming $n \gg 0$ (Leopoldt's conjecture). From $(a\,\eta^{-1})^{p^e} = a_\infty$, we get $\iota(a\,\eta^{-1}) = \xi \in W_k$; but, both ιa and $\iota\eta$ are close to 1 in U_k, thus $\xi = 1$ and $a\,\eta^{-1} = a'_\infty$ giving $\mathfrak{t}'\,\mathfrak{t}^{-1} = (a'_\infty)$. □

The non-unique extension F/k provides, in a numerical context, the repartition of the Artin symbols $\left(\frac{F/k}{\mathrm{N}_{k_n/k}(\mathfrak{A})}\right)$ or $\left(\frac{F/k}{\mathfrak{t}}\right)$ (see an example in [12, § 8.1]). The field F (more precisely F^{bp}) is, in some sense, a "governing field" for Greenberg's conjecture.

6.2. **Images of the fundamental ideals $\mathfrak{t}$ in $\mathcal{C}\ell_k$ and $\mathcal{R}_k$.** The ideals $\mathrm{N}_{k_n/k}(\mathfrak{A})$ play two different roles in the evolution of the class and norm factors, which will be stated in terms of fundamental ideals $\mathfrak{t}$ as follows since one may replace, modulo $k_n^\times \otimes \mathbb{Z}_p$, $\mathfrak{A}$ by the representative $\mathfrak{A} \cdot (\alpha_n)$ whose norm is $\mathfrak{t}$:

6.2.1. *Class factors and ideals* $\mathfrak{t}$. The $\mathrm{N}_{k_n/k}(\mathscr{M}_n^i)$, representing $\mathrm{N}_{k_n/k}(M_n^i)$ and defining the class factors, are generated, modulo $\mathrm{N}_{k_n/k}(k_n^\times \otimes \mathbb{Z}_p)$, by fundamental ideals $\mathfrak{t} \in I_k \otimes \mathbb{Z}_p$, of finite order modulo $\mathcal{P}_{k,\infty}$, with $\mathscr{C}\ell_k(\mathfrak{t}) \in \mathrm{N}_{k_n/k}(M_n^i)$. Thus, a priori, $\mathscr{C}\ell_k(\mathfrak{t})$ runs throughout $\mathcal{C}\ell_k$.

6.2.2. *Norm factors and ideals* $\mathfrak{t}$. The $\Lambda_n^i = \{x \in k^\times, (x) \in \mathrm{N}_{k_n/k}(\mathscr{M}_n^i)\}$, defining the norm factors, are generated, modulo $\mathrm{N}_{k_n/k}(k_n^\times \otimes \mathbb{Z}_p)$, via principal ideals $(\tau) = \mathfrak{t}$, of finite order modulo $\mathcal{P}_{k,\infty}$. The question is to examine the domain of variation of principal $\mathfrak{t}$; this is done taking the logarithm, as follows, showing that, a priori, $\log(\mathfrak{t})$ runs throughout $\mathcal{R}_k$.

6.2.3. *Definition of* $\log(\mathfrak{t}) \in \mathcal{R}_k$ *for* $\mathfrak{t}$ *principal.* Let $\mathfrak{t} = (\tau)$, $\tau \in k^\times \otimes \mathbb{Z}_p$ (thus $\left(\frac{H_k^{\rm pr}/k}{\mathfrak{t}}\right) \in \mathrm{Gal}(H_k^{\rm pr}/k_\infty H_k) \simeq \mathrm{tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k)$). There exists a power p^e such that $\tau^{p^e} = \varepsilon\, x_\infty$, $\varepsilon \in E_k \otimes \mathbb{Z}_p$; thus $\iota \mathrm{N}_{k/\mathbb{Q}}(\tau) = 1$ or ± 1 and the image of $\iota\tau$ is defined in $\mathrm{tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k) = U_k^*/\overline{E}_k$. Then we consider the image of $\log(\iota\tau)$ in $\log(U_k^*)/\log(\overline{E}_k) = \mathcal{R}_k$ (see (5)), which defines the element:

$$\log(\mathfrak{t}) := \log(\iota\tau) \pmod{\log(\overline{E}_k)}.$$

Lemma 6.3. *We have* $W_k := \bigoplus_{\mathfrak{p}\mid p} \mu_p(k_\mathfrak{p}) \subset \mathrm{N}_{k_n/k}(U_{k_n})$.

Proof. Let $\mathfrak{p} \mid p$ in k and let $\mathfrak{p}_n \mid \mathfrak{p}$ above $\mathfrak{p}$ in k_n. Let $k_\mathfrak{p}$ and $k_{n,\mathfrak{p}_n}$ be the respective completions and let's show that $\mu_p(k_\mathfrak{p}) \subseteq \mathrm{N}_{k_{n,\mathfrak{p}_n}/k_\mathfrak{p}}(k_{n,\mathfrak{p}_n}^\times)$.
Let p^ν, $\nu \geq 0$, be the order of $\mu_p(k_\mathfrak{p})$ and consider the extension of *global fields* $\mathbb{Q}_n(\mu_{p^\nu})/\mathbb{Q}(\mu_{p^\nu})$; then any $\zeta \in \mu_{p^\nu}$ is local norm at the tame places, thus at the *unique* p-place, in this extension (the real infinite place intervenes only for $p = 2$ and $\nu = 1$, but, in this case, $\mathbb{Q}_n(\mu_{p^\nu}) = \mathbb{Q}_n$ is real for all n). □

If $\mathfrak{t} = (\tau)$, the norm properties of $\iota\tau$ in k_n/k do not depend on the representative of $\iota\tau$ modulo $W_k = \mathrm{Ker}(\log)$, and the map:

$$\left\{\mathfrak{t} = (\tau) \in \mathcal{T}_k,\ \mathfrak{t}^{p^e} = (x_\infty)\right\} \xrightarrow{\log} \mathcal{R}_k = \log(U_k^*)/\log(\overline{E}_k) \tag{11}$$

is surjective of kernel the set of $\mathfrak{t} = (\tau)$, such that $\iota\tau \in W_k$, whence $\left(\frac{H_k^{\rm pr}/k}{\mathfrak{t}}\right) \in \mathcal{W}_k$.

6.2.4. *The main conjecture.* Assuming that the representatives $\mathfrak{t}$ (*finite in number*) are random, both $\mathscr{C}\ell_k(\mathfrak{t})$ and $\log(\iota\tau) \pmod{\log(\overline{E}_k)}$ (when $\mathfrak{t} = (\tau)$) are random in $\mathcal{C}\ell_k$ and $\mathcal{R}_k$, respectively. This is likely to avoid unbounded algorithms and yields the following conjecture which is apart from Iwasawa's theory and whose proof would be the key for Greenberg's conjecture:

Conjecture 6.4. For $n \gg 0$ fixed, $i \in [1, b_n]$, where b_n is the number of steps of the algorithm, let $\mathfrak{t}$ (or τ, when $\mathfrak{t} = (\tau)$ is principal), be the fundamental ideals or numbers encountered at the step i of the algorithm in k_n; then:

(*i*) The classes $\mathscr{C}\ell_k(\mathfrak{t})$ are random and uniformly distributed in $\mathcal{C}\ell_k$.
(*ii*) When $\mathfrak{t} = (\tau)$, the images $\log(\mathfrak{t}) := \log(\iota\tau) \pmod{\log(\overline{E}_k)}$ are random and uniformly distributed in the normalized regulator $\mathcal{R}_k := \log(U_k^*)/\log(\overline{E}_k)$.

6.2.5. *The algorithm in terms of fundamental ideals.* In this subsection, we fix the stage $K = k_n$ (n large enough) and, to simplify, we delete indices n in most cases, e.g., $M_n^i \to M^i$, $\Lambda_n^i \to \Lambda^i$, $\mathrm{N}_{k_n/k} \to \mathrm{N}$, $G_n = \langle \sigma_n \rangle \to G = \langle \sigma \rangle$, $b_n \to b$ (number of steps in K); then uppercase (respectively lowercase) letters for ideals are reserved to K (respectively k). We do not write infinitesimal ideals.
We can write, from Theorem 6.2 (iii), for any prime to p ideals $\mathfrak{A}$ of K and a suitable $\alpha \in K^\times \otimes \mathbb{Z}_p$:

$$\mathfrak{A}\,(\alpha) = \mathfrak{T} \cdot \mathfrak{C} \cdot (\alpha) \quad \& \quad \mathrm{N}(\mathfrak{A}\,(\alpha)) = \mathrm{N}(\mathfrak{T}) =: \mathfrak{t},$$

for ideals $\mathfrak{T}$ and $\mathfrak{t}$ of finite orders modulo $\mathcal{P}_{K,\infty}$ and $\mathcal{P}_{k,\infty}$, respectively.
Using a suitable finite set $\{\mathfrak{A}'^{i,j}\}_j$ of representatives $\mathfrak{A}'^{i,j} = \mathfrak{A}^{i,j}\,(\alpha^{i,j})$, of the ordinary ideals $\mathfrak{A}^{i,j} = \mathfrak{T}^{i,j}\,\mathfrak{C}^{i,j}$, given by the algorithm at the step i, one gets:

$$M^i =: cl_K(\mathscr{T}^i), \quad \mathscr{T}^i := \big\langle\, \{\mathfrak{A}'^{i,j}\}_j \,\big\rangle \text{ and } \mathrm{N}(\mathscr{T}^i) = \mathcal{t}^{\,i} := \big\langle\, \{\,\mathfrak{t}^{i,j}\,\}_j \,\big\rangle,$$

where the group $\mathscr{T}^i$ replaces $\mathscr{M}^i$ and $\mathfrak{t}^{i,j} = \mathrm{N}(\mathfrak{T}^{i,j})$, with Artin symbols in $\mathcal{T}_k$; then:

$$\mathrm{N}(M^i) = cl_k(\mathcal{t}^{\,i}) \text{ and } \Lambda^i = \big\{\tau \in k^\times \otimes \mathbb{Z}_p,\, (\tau) \in \mathcal{t}^{\,i}\big\}. \tag{12}$$

This does not modify the class and norm factors (7) since $cl_k(\mathrm{N}(\mathfrak{A})) = cl_k(\mathfrak{t})$, and $\mathrm{N}(\mathfrak{A})$ is principal if and only if $\mathfrak{t} = (\tau)$, $\tau \in k^\times \otimes \mathbb{Z}_p$.
Choose, once for all, a set (finite under Leopoldt's conjecture):

$$\mathbb{T}(k) = \big\{\,\mathfrak{t}_\ell\,\big\}_{\ell=1,\ldots,\#\mathcal{T}_k}, \tag{13}$$

of representatives $\mathfrak{t}_\ell \in I_k \otimes \mathbb{Z}_p$ modulo $\mathcal{P}_{k,\infty}$, of $\mathcal{T}_k$. Recall that $\mathcal{T}_k = \mathrm{N}(\mathcal{T}_K)$; thus any $\tau \in k^\times \otimes \mathbb{Z}_p$, is such that $(\tau) \in \mathbb{T}(k)$ is norm of an ideal (using Lemma 6.1), whence τ is local norm outside the p-places.
We have $\mathrm{N}(\mathscr{T}^i) = \mathcal{t}^{\,i} \subseteq \mathbb{T}(k)$ (modulo $\mathcal{P}_{k,\infty}$), the inclusion being in general strict, otherwise, the equality implies the end of the algorithm (triviality, from (12), of the class and norm factors since $cl_k(\mathcal{t}^{\,i}) = \mathcal{C}l_k$ and using the log map (11)).
Then, in Λ^i, one must find the elements τ^i such that $(\tau^i) \in \mathcal{t}^{\,i}$ (whence by definition of the form $\mathrm{N}(\mathfrak{T}^i)$, $\mathfrak{T}^i \in \mathscr{T}^i$), such that τ^i is local norm at the p-places 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:

$$\mathrm{N}(\mathfrak{T}^i) = \mathrm{N}(y^i),$$

with the following evolution relation (replacing (9)):

$$\begin{aligned}(y^i) =& \mathfrak{T}^i \cdot \mathfrak{B}^{1-\sigma} \mapsto \mathfrak{B} \mapsto \mathfrak{B} = \mathfrak{T}^{i+1}\,\mathfrak{C}^{i+1} \mapsto \mathfrak{T}^{i+1} \in \mathscr{T}^{i+1} \mapsto \\ & \mathrm{N}(\mathfrak{B} \cdot (\beta)) = \mathrm{N}(\mathfrak{T}^{i+1}) =: \mathfrak{t}^{i+1} \in \mathrm{N}(\mathscr{T}^{i+1}) = \mathcal{t}^{\,i+1} \mapsto \\ \Lambda^{i+1} =& \big\{\tau^{i+1},\, (\tau^{i+1}) \in \mathcal{t}^{\,i+1}\big\} \mapsto (\tau^{i+1}) = \mathrm{N}(\mathfrak{T}^{i+1}) = \mathrm{N}(y^{i+1}) \ldots\end{aligned} \tag{14}$$

The set $\mathbb{T}(k)$ being finite, the sets $\mathcal{t}^{\,i}$ are finite in number whatever K and $i \in [1, b]$; but if λ or μ do not vanish, there exist in (14) (when $[K : k] \to \infty$) arbitrary large sequences of $O(b)$ sets $\mathcal{t}^{\,i}$, $i \in [0, b]$, such that the class and norm factors are constant, which seems incredible because of the nature of the arithmetic relation $(y^i) = \mathfrak{T}^i \cdot \mathfrak{B}^{1-\sigma}$, when $\mathrm{N}(\mathfrak{T}^i) = \mathrm{N}(y^i)$, the ideal (y^i) being a priori random since its existence is due to the Hasse norm theorem which is only based of local norm properties, without known formula giving a solution y^i; a question which would deserve further study; see some comments and numerical experiments in [12, Remarques 11, § 6 and § 7]).
A philosophy should be that it is (y^i) (then $\mathfrak{B}$) which governs (numerically) the G-structure of the class groups in K/k and not the inverse.

Let's give now a more precise description of the algorithm. In the following comments, we assume that $\mathcal{W}_k = 1$ and that $1 \to \mathcal{R}_k \to \mathcal{T}_k \to \mathcal{C}\ell_k \to 1$ is an exact sequence of $\mathbb{F}_p$-vector spaces (the general case is similar with more complex reasonings with elementary abelian group theory):
Consider the following exact sequence at the step i of the algorithm, where we recall that $c\ell_k\big(t^i\big) = \mathrm{N}(\mathcal{C}\ell_K^i)$ and that $\Lambda^i = \big\{\tau \in k^\times \otimes \mathbb{Z}_p,\ (\tau) \in t^i\big\}$:

$$1 \longrightarrow \Lambda^i/E_k \otimes \mathbb{Z}_p \xrightarrow{(\,.\,)} t^i \xrightarrow{c\ell} c\ell_k\big(t^i\big) \longrightarrow 1. \tag{15}$$

Let $\mathfrak{t}^{i+1} := \mathrm{N}(\mathfrak{T}^{i+1})$ (obtained via (14)); then various cases may arrive for the new exact sequence:

$$1 \longrightarrow \Lambda^{i+1}/E_k \otimes \mathbb{Z}_p \xrightarrow{(\,.\,)} t^{i+1} \xrightarrow{c\ell} c\ell_k\big(t^{i+1}\big) \longrightarrow 1 :$$

(*a*) $c\ell_k(\mathfrak{t}^{i+1}) \notin c\ell_k\big(t^i\big)$. This strictly decreases the class factor but there is no new relation between ideals and $\Lambda^{i+1} = \Lambda^i$; so the norm factor is unchanged.

(*b*) $c\ell_k(\mathfrak{t}^{i+1}) \in c\ell_k\big(t^i\big)$. Thus $c\ell_k\big(t^{i+1}\big) = c\ell_k\big(t^i\big)$, and the class factor is unchanged, but there exists a new relation between the ideal classes giving $\tau \notin \Lambda^i$. Then two cases are to be considered:

(*i*) τ modulo Λ^i is non-norm in K/k, which strictly decreases the norm factor.

(*ii*) τ modulo Λ^i is a norm in K/k. So the class and norm factors are unchanged. This represents the "bad case" which must occur at least $O(n)$ times if $\lambda+\mu \neq 0$ and give a contradiction if Conjecture 6.4 holds true and if the evolution relation (14) gives independent random ideals $\mathfrak{t} \in \mathbb{T}(k)$.

6.2.6. *Conclusion.* Thus, the algorithms in k_∞/k run classically giving, from $\mathcal{C}\ell_k$, increasing class groups: $\mathcal{C}\ell_{k_1}, \ldots, \mathcal{C}\ell_{k_{n_0}}$, up to k_{n_0} such that Iwasawa's formula holds for all $n \geq n_0$ and gives $\#\mathcal{C}\ell_{k_n} = p^\nu$ in b_n steps of the filtration M_n^i, with $\#M_n^1 = \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\mathrm{nr}}$ (Theorem 3.8).
This is not to be confused with all the relative algorithms in k_m/k_n, $m \geq n \geq n_0$, which reduce to one step with $\mathcal{C}\ell_{k_m}^{G_{m/n}} = \mathcal{C}\ell_{k_m}$ (Theorem 4.1 (ii)); but this is not effective.
Now, considering the algorithms in any k_n/k and k_m/k, $m \geq n \geq n_0$, we note that the relative norms, $\mathrm{N}_{m/n} := \mathrm{N}_{k_m/k_n}$, are isomorphisms; then, in Diagram 5.8 the maps $\mathrm{N}_{m/n} : M_m^i \longrightarrow M_n^i$ are injective for all i (but not necessarily surjective), so that $b_n \leq b_m$. The algorithm for k_m is longer than that of k_n but there is some limit, given by Theorem 5.4 which yields:

$$\frac{\nu}{v_p(\#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\mathrm{nr}})} \leq b_n \leq b_m \leq \nu.$$

Since the number of steps is increasing, there exist $N_k \geq 0$ and $B_k \geq 0$ such that $b_n = B_k$ for all $n \geq N_k$ (this is related to the reasonings giving Theorem 5.9 and Corollary 5.10 when the limits are reached). The algorithm does not depend on $n \geq N_k$ in the meaning that in the evolution relation (14), from the main identity:

$$(y_m^i) = \mathfrak{T}_m^i \cdot \mathfrak{B}_m^{1-\sigma_m},$$

the relative norm $\mathrm{N}_{m/n}$ yields $\mathrm{N}_{m/n}(y_m^i) = \mathrm{N}_{m/n}(\mathfrak{T}_m^i) \cdot \mathrm{N}_{m/n}(\mathfrak{B}_m)^{1-\sigma_m}$, whence:

$$y_n^i := \mathrm{N}_{m/n}(y_m^i),\ \mathfrak{T}_n^i := \mathrm{N}_{m/n}(\mathfrak{T}_m^i),\ \mathfrak{B}_n := \mathrm{N}_{m/n}(\mathfrak{B}_m), \text{ and } (y_n^i) = \mathfrak{T}_n^i \cdot \mathfrak{B}_n^{1-\sigma_n},$$

giving the identity at the level n, only using the finite set $\mathbb{T}(k)$ defined by (13).
This process yields analogous inclusions as (8), giving here:

$$\Lambda_m^i \subseteq \cdots \subseteq \Lambda_n^i, \text{ with } \Lambda_h^i = \big\{\tau \in k^\times \otimes \mathbb{Z}_p,\ (\tau) \in t_h^i\big\},\ n \leq h \leq m.$$

If for instance $\lambda \geq 1$, then $\mathcal{T}_k \neq 1$ and classical probability laws will give, roughly (for the length of the algorithm in k_n), $\mathbb{P}\mathrm{r}(b_n = O(n)) = O\big(\big(\#\mathcal{T}_k\big)^{-n}\big)$ giving, since n is unbounded, the probability 1 for Greenberg's conjecture.

Acknowledgments. We are grateful to Jean-François Jaulent for checking some claims about logarithmic class groups in the framework of Iwasawa's theory.

References

[1] C. Chevalley, Sur la théorie du corps de classes dans les corps finis et les corps locaux. Thèse no. 155, Jour. of the Faculty of Sciences Tokyo **2** (1933), 365–476. http://www.numdam.org/issue/THESE_1934__155__365_0.pdf

[2] T. Fukuda, Greenberg's Conjecture and Relative Unit Groups for Real Quadratic Fields, J. of Number Theory **65**(215) (1997), 23–39. https://doi.org/10.1006/jnth.1997.2126

[3] T. Fukuda, Cyclotomic Units and Greenberg's Conjecture for Real Quadratic Fields, Math. Comp. **65** (1996), 1339–1348. https://doi.org/10.1090/S0025-5718-96-00730-2

[4] T. Fukuda, K. Komatsu, On $\mathbb{Z}_p$-extensions of real quadratic fields, J. Math. Soc. Japan **38**(1) (1986), 95–102. https://doi.org/10.2969/jmsj/03810095

[5] T. Fukuda, H. Taya, The Iwasawa λ-invariants of $\mathbb{Z}_p$-extensions of real quadratic fields, Acta Arith. **69** (1995)(3), 277–292. http://matwbn.icm.edu.pl/ksiazki/aa/aa69/aa6936.pdf

[6] G. Gras, Classes généralisées invariantes, J. Math. Soc. Japan **46**(3) (1994), 467–476. http://dx.doi.org/10.2969/jmsj/04630467

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

[8] G. Gras, Les θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques, Canadian J. Math., **68**(3) (2016), 571–624. http://dx.doi.org/10.4153/CJM-2015-026-3
English translation: Local θ-regulators of an algebraic number: p-adic Conjectures (2017). https://arxiv.org/pdf/1701.02618

[9] 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

[10] 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

[11] G. Gras, The p-adic Kummer–Leopoldt Constant: Normalized p-adic Regulator, Int. J. of Number Theory, **14**(2) (2018), 329–337. https://doi.org/10.1142/S1793042118500203

[12] 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

[13] 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

[14] G. Gras, New criteria for Vandiver's conjecture using Gauss sums – Heuristics and numerical experiments, Proc. Indian Acad. Sci. (Math. Sci.) **130**, art. 32 (2020). https://rdcu.be/b30wt https://doi.org/10.1007/s12044-020-00561-z

[15] 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

[16] R. Greenberg, Iwasawa theory-past and present. Class field theory - its centenary and prospect (Tokyo, 1998), *Advanced Studies in Pure Math., Math. Soc. Japan* **30** (2001), 335–385. https://sites.math.washington.edu/~greenber/iwhi.ps

[17] C. Greither, T. Kataoka, M. Kurihara, Fitting ideals of p-ramified Iwasawa modules over totally real fields. https://arxiv.org/abs/2006.05667

[18] Y. Hiroshi, On the iwasawa invariants of totally real number fields, Manuscripta Math. **79**(6) (1993), 1–6. https://doi.org/10.1007/BF02568324

[19] H. Ichimura, H. Sumida, On the Iwasawa invariants of certain real abelian fields II, Internat. J. of Mathematics **7**(6) (1996), 721–744. https://doi.org/10.1142/S0129167X96000384

[20] H. Ichimura, H. Sumida, On the Iwasawa invariants of certain real abelian fields, Tohoku Math. J. **49**(2) (1997), 203–215. https://doi.org/10.2748/tmj/1178225147

[21] J-F. Jaulent, L'arithmétique des ℓ-extensions (Thèse de doctorat d'Etat, 1986), Pub. Math. Besançon (1986), 1–349. https://pmb.centre-mersenne.org/
[22] 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
[23] J-F. Jaulent, La théorie de Kummer et le K_2 des corps de nombres, J. Théorie des Nombres de Bordeaux **2** (1990)(2), 377–411. http://www.numdam.org/item/JTNB_1990__2_2_377_0/
[24] J-F. Jaulent, Classes logarithmiques des corps de nombres, J. Théorie des Nombres de Bordeaux **6** (1994), 301–325. https://jtnb.centre-mersenne.org/item/JTNB_1994__6_2_301_0
[25] J-F. Jaulent, Généralisation d'un théorème d'Iwasawa, J. Théor. Nombres de Bordeaux **17** (2005), 527–553. https://doi.org/10.5802/jtnb.506
[26] 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
[27] J-F. Jaulent, Normes universelles et conjecture de Greenberg, Acta Arithmetica **194** (2020), 99–109. https://doi.org/10.4064/aa190623-27-9
[28] J-F. Jaulent, Annulateurs circulaires et conjecture de Greenberg. (2020). https://arxiv.org/abs/2003.12301
[29] P. Koymans, C. Pagano, On the distribution of $\mathcal{C}\ell(K)[\ell^\infty]$ for degree ℓ cyclic fields (2018). https://arxiv.org/pdf/1812.06884
[30] M. Le Floc'h, A. Movahhedi, T. Nguyen Quang Do, On Capitulation Cokernels in Iwasawa Theory, American Journal of Mathematics **127**(4) (2005), 851–877. https://www.jstor.org/stable/40067984
[31] A. Movahhedi, T. Nguyen Quang Do, Sur l'arithmétique des corps de nombres p-rationnels, Séminaire de Théorie des Nombres, Paris 1987–88, Progress in Math., **81** (1990), 155–200. https://doi.org/10.1007/978-1-4612-3460-9_9
[32] 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
[33] T. Nguyen Quang Do, Sur la conjecture faible de Greenberg dans le cas abélien p-décomposé, Int. J. of Number Theory **2**(1) (2006), 49–64. https://doi.org/10.1142/S1793042106000395
[34] T. Nguyen Quang Do, Sur une forme faible de la conjecture de Greenberg II, Int. J. of Number Theory **13**(4) (2017), 1061–1070. https://doi.org/10.1142/S1793042117500567
[35] T. Nguyen Quang Do, Formules de genres et conjecture de Greenberg, Ann. Math. du Québec **42**(2) (2018), 267–280. https://doi.org/10.1007/s40316-017-0093-y
[36] Y. Nishino, On the Iwasawa invariants of the cyclotomic $\mathbb{Z}_2$-extensions of certain real quadratic fields, Tokyo J. Math. **29**(1) (2006), 239–245. https://doi.org/10.3836/tjm/1166661877
[37] T. Nguyen Quang Do, V. Nicolas, Nombres de Weil, sommes de Gauss et annulateurs galoisiens, Amer. J. Math. **133** (2011), 1533–1571. https://muse.jhu.edu/article/458549
[38] M. Ozaki, The class group of $\mathbb{Z}_p$-extensions over totally real number fields, Tohoku Math. J. **49**(3) (1997), 431-435. https://doi.org/10.2748/tmj/1178225114
[39] M. Ozaki, H. Taya, A note on Greenberg's conjecture for real abelian number fields, Manuscripta Math. **88**(1) (1995), 311–320. https://doi.org/10.1007/BF02567825
[40] G. Perbet, Sur les invariants d'Iwasawa dans les extensions de Lie p-adiques, Algebra and Number Theory **5**(6) (2011), 819–848. https://doi.org/10.2140/ant.2011.5.819
[41] H. Taya, On cyclotomic $\mathbb{Z}_p$-extensions of real quadratic fields, Acta Arithmetica **74**(2) (1996), 107–119. http://matwbn.icm.edu.pl/ksiazki/aa/aa74/aa7422.pdf
[42] 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
[43] H. Taya, On p-adic L-functions and $\mathbb{Z}_p$-extensions of certain real abelian number fields, J. of Number Theory **75**(2) (1999), 170–184. https://doi.org/10.1006/jnth.1998.2326

Georges Gras, 4 chemin de Château Gagnière, 38520 Le Bourg d'Oisans
E-mail address: g.mn.gras@wanadoo.fr