Greenberg's conjecture for totally real 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, $p \geq 2$. This paper synthesizes and generalizes our articles written in french: "Approche p-adique de la conjecture de Greenberg pour les corps totalement réels", Ann. Math. Blaise Pascal **24**(2) (2017), 235–291 and "Normes d'idéaux dans la tour cyclotomique et conjecture de Greenberg", Ann. math. du Québec **43** (2019), 249–280. We show that this conjecture (nullity of the Iwasawa invariants λ, μ) depends on some 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; more precisely these images (obtained, for each fixed n, inductively via a classical algorithm in 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 (recall that $\#\mathcal{T}_k = \#\mathcal{C}\ell_k \# \mathcal{R}_k \# \mathcal{W}_k$, where the fixed field of $\mathcal{W}_k$ is the Bertrandias–Payan field). A suitable assumption of uniform p-adic distribution of these images, related to $\mathcal{C}\ell_k$ and $\mathcal{R}_k$, would constitute *a proof* of Greenberg's conjecture, which remains hopeless within the sole framework of Iwasawa's theory. We interpret the conjecture in terms of algorithmic complexity, governed by the arithmetic structure of $\mathcal{T}_k$, for which some heuristics and probabilities, and possibly accessible proofs, apply. No assumption is made on the degree of k 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 denote by k_n the degree p^n extension of k in k_∞ and by $G_n := \mathrm{Gal}(k_n/k)$.

Date: April 13, 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.

Let $\mathcal{C}\ell_k$ and $\mathcal{C}\ell_{k_n}$ be the ordinary p-class groups of k and k_n, respectively.

Let $\mathcal{T}_k$ be 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 pro-p-extension of k.

In the case $p = 2$, all the forthcoming p-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 instead of the ordinary sense. 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*, $\#\mathcal{T}_k^{\rm res} = 2^d\,\#\mathcal{T}_k^{\rm ord}$ [2, Theorem III.4.1.5], knowing that, for totally real number fields, $\#\mathcal{C}\ell_k^{\rm res} = \frac{2^d}{(E:E^{\rm pos})}\,\#\mathcal{C}\ell_k^{\rm ord}$, $\#\mathcal{R}_k^{\rm res} = \frac{(E:E^{\rm pos})}{2}\,\#\mathcal{R}_k^{\rm ord}$ and $\#\mathcal{W}_k^{\rm res} = 2\,\#\mathcal{W}_k^{\rm ord}$, which makes coherent the formulas $\#\mathcal{T} = \#\mathcal{C}\ell\,\#\mathcal{R}\,\#\mathcal{W}$ in the two senses (see the main notations for the ordinary sense in § 2.1).

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 [8, Theorems 1 and 2] for the study of two cases of decomposition of p in $k/\mathbb{Q}$). Main recent studies of this conjecture, after many others as that of [17] [18], are [5, 6, 10, 11, 12, 14, 15, 16]. In [10, Théorèmes A, B] a new criterion is given (capitulation in some k_{n_0} of the logarithmic class group of k), in [11] the Greenberg conjecture is stated in terms of "universal norms". In [16] a synthetic view of the criteria of Greenberg, Jaulent and others is given and the fact that the Greenberg conjecture is fulfilled if and only if $(X_\infty)_\Gamma$ capitulates asymptotically in k_∞, where $X_\infty = \varprojlim_n \mathcal{C}\ell_{k_n}$ and $\Gamma = \mathrm{Gal}(k_\infty/k)$.

Remark 1.1. Subject to replace k by a stage k_{n_0} in k_∞, one may assume without any limitation of the generality (but under Leopoldt's conjecture) that p is totally ramified in k_∞/k. Indeed, any stage in k_∞ remains totally real with the same Iwasawa invariants since $k_{n_0}\mathbb{Q}_\infty = k_\infty$.

We shall not put any assumption on the degree d nor on the decomposition of p in $k/\mathbb{Q}$ (even if, in the classical papers, the decomposition of p plays an important role and needs different techniques). On the contrary, we will show how this decomposition intervenes, especially regarding the regulator $\mathcal{R}_k$, for the Greenberg conjecture.

The main results of the paper are described by means of Theorem 2.8 and Corollary 2.9, then Theorems 3.3, 3.4 and 5.5.

2. Abelian p-ramification and genus theories

2.1. **Abelian p-ramification – The torsion group $\mathcal{T}_k$.** Let $r_p \geq 1$ be the number of primes $\mathfrak{p} \mid p$ in k (hence totally ramified in k_∞/k). 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 $\mathcal{T}_k$.

(i) 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 $\overline{\mathfrak{p}}$-principal units of the $\mathfrak{p}$-completion $k_\mathfrak{p}$ of k, $\overline{\mathfrak{p}}$ being the maximal ideal for $k_\mathfrak{p}$.

We put $W_k := \mathrm{tor}_{\mathbb{Z}_p}(U_k) = \bigoplus_{\mathfrak{p}\mid p} \mu_p(k_\mathfrak{p})$ and $\mathcal{W}_k := W_k/\mu_p(k)$.

Let $\iota : \{x \in k^\times \otimes \mathbb{Z}_p,\ \text{prime to } p\} \longrightarrow U_k$ be the diagonal embedding.

(ii) Let $\overline{E}_k$ be the closure of the diagonal embedding ιE_k of E_k in U_k and let H_k be the p-Hilbert class field; from class field theory, $\mathrm{Gal}(H_k^{\rm pr}/H_k) \simeq U_k/\overline{E}_k$. One checks that under Leopoldt's conjecture, $\mathrm{tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k) = U_k^*/\overline{E}_k$, where $U_k^* := \{u \in U_k,\ \mathrm{N}_{k/\mathbb{Q}}(u) = 1\}$ if $p \neq 2$ (resp. $\mathrm{N}_{k/\mathbb{Q}}(u) = \pm 1$ if $p = 2$).

(iii) Let $\mathcal{C}\ell_k$ be the p-class group of k and let $\mathcal{R}_k := \mathrm{tor}_{\mathbb{Z}_p}(\log(U_k)/\log(\overline{E}_k)) = \log(U_k^*)/\log(\overline{E}_k)$ be the normalized p-adic regulator [4, § 5]; recall that for $p \neq 2$, $\#\mathcal{R}_k = \dfrac{R_k}{p^{d-1}}$ and $\#\mathcal{R}_k = \dfrac{1}{2^{r_2-1}}\dfrac{R_k}{2^{d-1}}$ for $p = 2$, where R_k is the classical regulator.

(iv) Since $\mu(k) = \{\pm 1\}$, the sub-module of $\mathcal{T}_k$ fixing the Bertrandias–Payan field $H_k^{\rm bp}$ is $\mathcal{W}_k := W_k$ for $p \neq 2$ and $\mathcal{W}_k := W_k/\langle \pm 1\rangle$ for $p = 2$. 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 https://arxiv.org/pdf/1701.02618 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 2.1. [4, § 4, § 5]. *We have the exact sequences:*

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

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

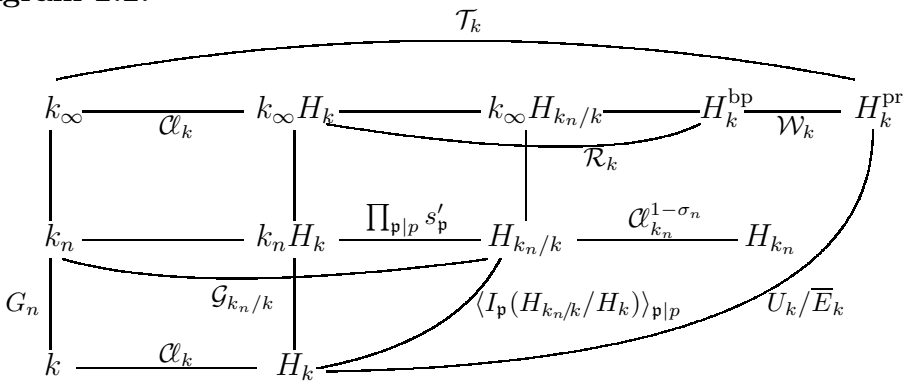
2.2. **Genus theory in the extensions k_n/k.** We denote by H_k and H_{k_n} the p-Hilbert class fields of k and k_n. Since p is totally ramified in k_n/k, the inertia groups $I_{\mathfrak{p}}(k_n/k)$ of the $\mathfrak{p} \mid p$ in k_n/k are isomorphic to $G_n = \mathrm{Gal}(k_n/k)$.

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., [2, Corollary IV.4.4.1]):

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

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

Diagram 2.2.



[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 a subfield of K.

The image of ω_n is contained in $\Omega(k_n/k)$ and the map π_n is defind as follows: with $(s_{\mathfrak{p}})_{\mathfrak{p}\vert p} \in G_n^{r_p}$, π_n associates the product of the extensions $s'_{\mathfrak{p}}$ of the $s_{\mathfrak{p}}$ 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 $(s_{\mathfrak{p}})_{\mathfrak{p}\vert p} \in \Omega(k_n/k)$, then $\prod_{\mathfrak{p}\vert p} s'_{\mathfrak{p}}$ fixes both H_k and k_n, whence k_nH_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 formula [1],

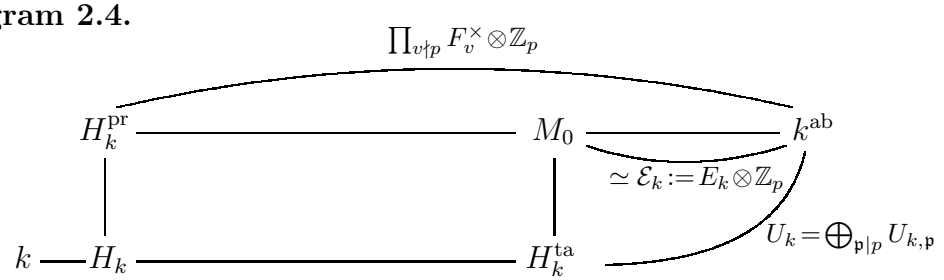
$$\#\mathcal{G}_{k_n/k} := \mathrm{Gal}(H_{k_n/k}/k_n) = \frac{\#\mathcal{C}\ell_{k_n}}{\#\mathcal{C}\ell_{k_n}^{1-\sigma_n}} = \#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{C}\ell_k \cdot \frac{p^{n\cdot(r_p-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))}.$$

The genus group $\mathcal{G}_{k_n/k}$ has, in our context, the following property that we will analyze in more details in § 2.3 to obtain Theorem 2.8.

Proposition 2.3. *For all $n \geq 0$, the sub-group $\mathcal{W}_k$ of $\mathcal{T}_k$ fixes $k_\infty H_{k_n/k}$, whence $k_\infty H_{k_n/k} \subseteq H_k^{\mathrm{bp}}$ and $\#\mathcal{G}_{k_n/k} \big| \#\mathcal{C}\ell_k \cdot \mathcal{R}_k$, equivalent to $\dfrac{p^{n\cdot(r_p-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))} \,\Big|\, \#\mathcal{R}_k$. The n-sequence $\#\mathcal{G}_{k_n/k}$ is increasing and stabilizes at a divisor of $\#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k$.*

Proof. Using the idelic global reciprocity map (under Leopoldt's conjecture), we have the fundamental diagram [2, § III.4.4.1] of the Galois group of the maximal abelian pro-p-extension k^{ab} of k, with our present notations:

Diagram 2.4.



where F_v is the residue field of the tame places v. We know that the fixed field of the maximal tame sub-extension H_k^{ta} is $U_k = \bigoplus_{\mathfrak{p}\vert p} U_{k,\mathfrak{p}}$ 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 $k_\infty H_{k_n/k}$. 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 $W_k = \bigoplus_{\mathfrak{p}\vert p} \mu_p(k_{\mathfrak{p}})$ to $\mathrm{Gal}(H_k^{\mathrm{pr}}/k)$ is isomorphic to $W_k/\mu_p(k) = \mathcal{W}_k$ whose fixed field is H_k^{bp}. Whence the first claim; the second one is obvious since non-ramification propagates (use Diagram 2.2). □

Remark 2.5. This result is obvious in the totally split case in $k/\mathbb{Q}$ (see Corollary 2.9), often considered in the literature, as in the pioneering work of Taya [18, Theorem 1.1] proving in that case that $\#\mathcal{G}_{k_n/k} = \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k$ for $n \gg 0$; indeed, in this case, $\mathcal{W}_k = 1$ since $k_{\mathfrak{p}} = \mathbb{Q}_p$ for all $\mathfrak{p} \mid p$. See analogous approaches in [5, Théorème 4.8], [10, § 2.2], [16, Théorème C], for the totally split case.

The case where $\mathfrak{p}$ does not split in k (i.e., $r_p = 1$ giving $\dfrac{p^{n\cdot(r_p-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))} = 1$ for all n) is also considered in these papers; but, even if $\mathcal{W}_k \neq 1$, we have $\#\mathcal{G}_{k_n/k} = \#\mathcal{C}\ell_k$ and the norm factors that we shall define later (see (2)), as divisors of $\#\mathcal{R}_k$, are trivial divisors, but the regulator may be arbitrary.

We shall emphasize on the influence of the decomposition of p in $k/\mathbb{Q}$ in the following section.

2.3. **Ramification in $H_k^{\rm pr}/k_\infty$.** Give more information about the ramification of the p-places in $H_k^{\rm pr}/k_\infty$, whatever the decomposition of p in $k/\mathbb{Q}$.

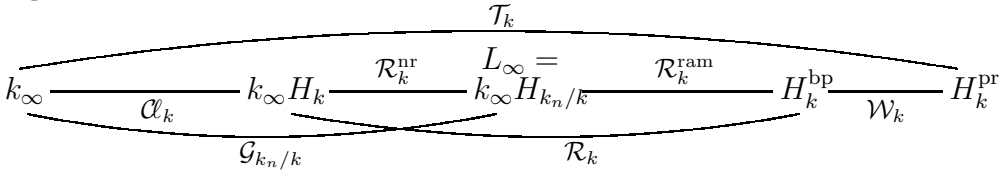
Proposition 2.6. *Let $n_0 \gg 0$ be such that $\#\mathcal{G}_{k_n/k}$ stabilizes for all $n \geq n_0$; this defines $L_\infty := k_\infty H_{k_n/k}$ independently of $n \geq n_0$. Then L_∞ is the maximal unramified extension of k_∞ in $H_k^{\rm pr}$ and $\mathrm{Gal}(H_k^{\rm pr}/L_\infty) = \langle \mathrm{tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}}\overline{E}_k/\overline{E}_k)\rangle_{\mathfrak{p}\mid p}$.*

Proof. 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 $\mathfrak{p} \mid p$ in k, the inertia group $I_\mathfrak{p}(H_k^{\rm pr}/k_\infty)$ is isomorphic to $\mathrm{tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}}\overline{E}_k/\overline{E}_k)$ (see Diagram 2.4). □

Denote by $\mathcal{R}_k^{\rm nr}$ ("non-ramification") and $\mathcal{R}_k^{\rm ram}$ ("ramification") the Galois groups $\mathrm{Gal}(L_\infty/k_\infty H_k)$ and $\mathrm{Gal}(H_k^{\rm bp}/L_\infty)$, respectively. So the top of Diagram 2.2 may be specified as follows:

Diagram 2.7.



From the Proposition 2.3 and the above study, we can state:

Theorem 2.8. *Let $n \gg 0$ so that the genus group $\mathcal{G}_{k_n/k} = \mathrm{Gal}(k_\infty H_{k_n/k}/k_\infty)$ stabilizes. Then $\#\mathcal{G}_{k_n/k} = \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\rm nr}$, equivalent to $\dfrac{p^{n\cdot(r_p-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))} = \#\mathcal{R}_k^{\rm nr}$.*

Corollary 2.9. *(i) If $r_p = 1$, one gets $\mathcal{R}_k^{\rm ram} = \mathcal{R}_k$ and $\mathcal{R}_k^{\rm nr} = 1$.*
(ii) If $r_p = d$ (p totally split),one gets $\mathcal{R}_k^{\rm ram} = 1$ and $\mathcal{R}_k^{\rm nr} = \mathcal{R}_k$.

Proof. (i) If $r_p = 1$, $\mathrm{tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}}\overline{E}_k/\overline{E}_k) = \mathrm{tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k)$, whence the result.
(ii) If $r_p = d$, we know that $\mathcal{W}_k = 1$ and 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 $\mathfrak{p}$, $\mathrm{tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}}/\overline{E}_k \cap U_{k,\mathfrak{p}}) = \mathrm{tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}})/\mathrm{tor}_{\mathbb{Z}_p}(\overline{E}_k) = 1$ whatever p. Thus the inertia field is $H_k^{\rm bp} = H_k^{\rm pr}$, giving $\mathcal{R}_k^{\rm ram} = 1$. □

Otherwise, these inertia groups are only accessible by means of numerical computations (this is done in [7] in the context of incomplete p-ramification); they give L_∞ independently of the knowledge of the $\mathcal{G}_{k_n/k}$ for $n \gg 0$. It would be interesting to interpret $\mathcal{R}_k^{\rm ram}$ in terms of units of k.

3. Filtration of the $M^n := \mathcal{C}\ell_{k_n}$ – Class and Norm factors

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", one uses the filtration of $M^n := \mathcal{C}\ell_{k_n}$:

$$M_i^n = c\ell_{k_n}(\mathcal{I}_i^n),\ \mathcal{I}_i^n \subset I_{k_n},\ i \geq 0,$$

defined inductively as follows (from [3, § 6.1]):

Definition 3.1. *For $n \geq 1$ fixed, $(M_i^n)_{i\geq 0}$ is the i-sequence of sub-G_n-modules of M^n defined by $M_0^n := 1$ and $M_{i+1}^n/M_i^n := (M^n/M_i^n)^{G_n}$, for $0 \leq i \leq m_n - 1$, where m_n is the least integer i such that $M_i^n = M^n$ (i.e., such that $M_{i+1}^n = M_i^n$).*

We then have:

Proposition 3.2. *This filtration has the following properties:*
(i) For $i = 0$, $M_1^n = (M^n)^{G_n}$ (group of ambiguous classes in k_n/k).
(ii) One has $M_i^n = \{c \in M^n,\ c^{(1-\sigma_n)^i} = 1\}$, for all $i \geq 0$.
(iii) For n fixed, the i-sequence of the $\#(M_{i+1}^n/M_i^n)$, $0 \leq i \leq m_n$, is decreasing to 1 and has the upper bound $\#M_1^n$ because of the sequence of injective maps: $M_{i+1}^n/M_i^n \hookrightarrow M_i^n/M_{i-1}^n \hookrightarrow \cdots \hookrightarrow M_2^n/M_1^n \hookrightarrow M_1^n$ defined from the action of $1-\sigma_n$.
(iv) $\#M_{m_n}^n = \prod_{i=0}^{m_n-1} \#(M_{i+1}^n/M_i^n)$.

Recall that for $n \geq 1$ fixed, a generalization of the Chevalley ambiguous class number formula [3], leads, by means of the norm groups $\mathrm{N}_{k_n/k}(M_i^n)$ and the groups of numbers $\Lambda_i^n := \{x \in k^\times,\ (x) \in \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)\} \supseteq \Lambda_0^n = E_k$, to the i-sequence of integers defined by:

$$\#\big(M_{i+1}^n/M_i^n\big) = \frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)} \cdot \frac{p^{n\cdot(r_p-1)}}{(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}({k_n}^\times))},$$

(2) where the integers:

$$\frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)} \quad \& \quad \frac{p^{n\cdot(r_p-1)}}{(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}({k_n}^\times))}$$

are called *the class factor* and *the norm factor*, respectively, at the step i of the algorithm in k_n. These factors are independent of the choice of the ideals in $\mathcal{I}_i^n$ up to principal ideals of k_n and the groups Λ_i^n may be defined up to $\mathrm{N}_{k_n/k}(k_n^\times)$. The groups $\mathcal{I}_i^n$ are built inductively from $\mathcal{I}_0^n$.
From the above, we can state, for any fixed integer n:

Theorem 3.3. *(i) The class factors $\frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)}$ divide the order of the class group $\mathcal{C}\ell_k$ of k; they define a decreasing i-sequence of integers from $\#\mathcal{C}\ell_k$.*
(ii) The norm factors $\frac{p^{n\cdot(r_p-1)}}{(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}({k_n}^\times))}$ divide the order of the quotient $\mathcal{R}_k^{\mathrm{nr}}$ of the normalized regulator $\mathcal{R}_k$ of k (see Diagram 2.7); they define a decreasing i-sequence of integers from $\frac{p^{n\cdot(r_p-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}({k_n}^\times))}$.

Proof. This is obvious for the class factors and comes from the injective maps:

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

for the norm factors since for all n, $\frac{p^{n\cdot(r_p-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))} \,\big|\, \#\mathcal{R}_k^{\mathrm{nr}}$ from § 2.3, with equality for $n \gg 0$. □

Therefore, for $i = m_n$, using the above formula (2), we obtain $M_{m_n}^n = \mathcal{C}\ell_{k_n}$, $\mathrm{N}_{k_n/k}\big(M_{m_n}^n\big) = \mathcal{C}\ell_k$ and $(\Lambda_{m_n}^n : \Lambda_{m_n}^n \cap \mathrm{N}_{k_n/k}(k_n^\times)) = p^{n\cdot(r_p-1)}$, which explains that $\#\mathcal{C}\ell_{k_n}$ essentially depends on the number of steps m_n of the algorithm, which will be expressed in terms of Iwasawa invariants as follows.

Theorem 3.4. *Let k be a totally real number field for which p fulfills the Leopoldt conjecture. We recall that, without any loss of generality, we may assume p totally ramified in k_∞/k (cf. Remark 1.1).*

Let $\mathcal{C}\ell_k$ and $\mathcal{R}_k$ be the p-class group and the normalized p-adic regulator of k, respectively and let $\mathcal{R}_k^{\rm nr} := {\rm Gal}(L_\infty/k_\infty H_k)$ defined in § 2.3. 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 m_n be the length of the algorithm. Then:

(i) One has the inequalities $m_n \leq \lambda\cdot n+\mu\cdot p^n+\nu \leq v_p(\#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr})\cdot m_n$ for all $n \geq n_0$, where v_p denotes the p-adic valuation.

(ii) If $\mathcal{C}\ell_k = \mathcal{R}_k^{\rm nr} = 1$, then $\lambda = \mu = \nu = 0$.

(iii) If $\#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr} \neq 1$, then there exists $c(n)$, $\dfrac{1}{v_p(\#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr})} \leq c(n) \leq 1$, such that $m_n = c(n)\cdot(\lambda\cdot n+\mu\cdot p^n+\nu)$.

Proof. Consider $M^n := \mathcal{C}\ell_k$. As $\#\big(M_{i+1}^n/M_i^n\big) \geq p$ for $0 \leq i \leq m_n-1$, the Proposition (3.2) (iv) implies $\#\mathcal{C}\ell_{k_n} = \#M_{m_n}^n \geq p^{m_n}$; whence $m_n \leq \lambda\cdot n+\mu\cdot p^n+\nu$; then, from the fact that $\#\big(M_{i+1}^n/M_i^n\big) \mid \#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr}$, this yields $\#\big(M_{i+1}^n/M_i^n\big) \leq \#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr}$ for $0 \leq i \leq m_n-1$; whence $\#\mathcal{C}\ell_{k_n} \leq (\#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr})^{m_n}$ from Proposition (3.2) (iv), which completes the proof. Points (i) and (ii) are immediate. □

Corollary 3.5. *If $\#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\rm nr} \neq 1$, the number of steps m_n of the algorithm fulfills the following inequality linking Iwasawa's theory and algorithmic complexity:*

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

Thus, the Greenberg conjecture reduces to an estimation of the number m_n of steps of the algorithm. But m_n (for n fixed) depends of the i-progression of the class and norm factors (2) and under natural probabilities on their evolution (Theorem 3.3), 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 $\mathcal{R}_k^{\rm nr}$). See more details on the complexity of the algorithm in [6, § 6].

This is strengthened by the results of [13] which show, in a particular case, that there is no obstruction to obtain effective density results and some proofs "with probability 1".

4. The n-sequences M_{i+1}^n/M_i^n for i fixed

Now, contrary to the previous studies, we fix the step i of the algorithms and we consider the n-sequences M_i^n, for $n \to \infty$. We study the integers $\#\big(M_{i+1}^n/M_i^n\big)$ from their class and norm factors (2), knowing that "$M^n = \mathcal{C}\ell_{k_n}$".

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 $H_{k_n}\cap k_{n+1} = k_n$, by ramification of p, but not that on M_i^{n+1} (it may be a priori not injective nor surjective):

Diagram 4.1.

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

We have $\mathrm{N}_{k_{n+1}/k_n}(M_i^{n+1}) \subseteq M_i^n$; thus, for all $\mathfrak{A}^{n+1} \in \mathcal{I}_i^{n+1}$, $\mathrm{N}_{k_{n+1}/k_n}(\mathfrak{A}^{n+1}) = (\alpha^n)\,\mathfrak{A}^n$, where $\alpha^n \in k_n^\times$ and $\mathfrak{A}^n \in \mathcal{I}_i^n$, in what case, *modifying* $\mathcal{I}_i^n$ modulo principal ideals, one gets $\mathrm{N}_{k_{n+1}/k_n}(\mathcal{I}_i^{n+1}) \subseteq \mathcal{I}_i^n$ whence $\mathrm{N}_{k_{n+1}/k}(\mathcal{I}_i^{n+1}) \subseteq \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)$; this reduces to modify the sets $\Lambda_i^n = \{x \in k^\times, (x) \in \mathrm{N}_{k_n/k}(\mathcal{I}_i^n)\}$ modulo global norms of elements of $k_n^\times$ leaving invariant $(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}(k_n^\times))$. Whence, one may suppose that, for all given $h \geq 1$:

$$E_k \subseteq \Lambda_i^{n+h} \subseteq \cdots \subseteq \Lambda_i^{n+1} \subseteq \Lambda_i^n. \tag{3}$$

In the next section, we shall give a more p-adic approach of the properties of ideal norms $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$, replacing the ideal $\mathfrak{a}$ of k by an ideal $\mathfrak{t}$ whose Artin symbol is in $\mathcal{T}_k$.

Proposition 4.2. *For all $i \geq 0$ fixed, the integers $\#\big(M_{i+1}^n/M_i^n\big)$ define an increasing stationary n-sequence of divisors of $\#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\mathrm{nr}}$, and the integers $\#M_i^n$ define an increasing stationary n-sequence.*

Proof. As $\mathrm{N}_{k_{n+1}/k}(M_i^{n+1}) \subseteq \mathrm{N}_{k_n/k}(M_i^n)$, the class factors $\frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)}$ define an *increasing* n-sequence $p^{c_i^n}$, stationary at a maximal value $p^{c_i} \mid \#\mathcal{C}\ell_k$. The norm factors are $\frac{p^{n\cdot(r_p-1)}}{\#\omega_n(\Lambda_i^n)} =: p^{\rho_i^n}$ (see § 2.2) and $p^{\rho_i^{n+1}-\rho_i^n} = p^{r_p-1}\,\frac{\#\omega_n(\Lambda_i^n)}{\#\omega_{n+1}(\Lambda_i^{n+1})}$; since by (3) one may assume $\Lambda_i^{n+1} \subseteq \Lambda_i^n$, this yields $\#\omega_{n+1}(\Lambda_i^{n+1}) \leq \#\omega_{n+1}(\Lambda_i^n)$, then we obtain $p^{\rho_i^{n+1}-\rho_i^n} \geq p^{r_p-1}\,\frac{\#\omega_n(\Lambda_i^n)}{\#\omega_{n+1}(\Lambda_i^n)}$; in the restriction $\Omega(k_{n+1}/k) \twoheadrightarrow \Omega(k_n/k)$ of Hasse's symbols, the image of $\omega_{n+1}(\Lambda_i^n)$ is $\omega_n(\Lambda_i^n)$, whence an increasing n-sequence $p^{\rho_i^n} \mid \#\mathcal{R}_k^{\mathrm{nr}}$. Thus $\lim\limits_{n\to\infty} \#\big(M_{i+1}^n/M_i^n\big) = p^{c_i} \cdot p^{\rho_i} \mid \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\mathrm{nr}}$.

If one assumes, by induction, that the n-sequence $\#M_i^n$ is increasing stationary, the property follows for the n-sequence $\#M_{i+1}^n$. □

Proposition 4.3. *The i-sequences p^{c_i} and p^{ρ_i} are decreasing, stationary at a divisor of $\#\mathcal{C}\ell_k$ and R_k^{nr}, respectively.*

Proof. For n large enough (to get $c_i^n = c_i$ and $\rho_i^n = \rho_i$), we have $\frac{\#\mathrm{N}_{k_n/k}(M_i^n)}{\#\mathrm{N}_{k_n/k}(M_{i+1}^n)} \leq 1$ and $\frac{\#\omega_n(\Lambda_i^n)}{\#\omega_n(\Lambda_{i+1}^n)} \leq 1$ since $\Lambda_i^n \subseteq \Lambda_{i+1}^n$. □

Corollary 4.4. *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 $\lim\limits_{i\to\infty} \big(p^{c_i} \cdot p^{\rho_i}\big) = p^{c+\rho} \mid \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\mathrm{nr}}$; from Theorem 3.4, Greenberg's conjecture holds true if and only if $c = \rho = 0$.*

We refer to [5, 6] for complements, conjectures and numerical experiments; in particular, for $x \in \Lambda_i^n$ we then have $(x) = \mathrm{N}_{k_n/k}(\mathfrak{A})$, $\mathfrak{A} \in \mathcal{I}_i^n$, and when we compute that x is local norm at p, hence $x = \mathrm{N}_{k_n/k}(y_n)$, $y_n \in k_n^\times$, the random aspects occur in the mysterious "evolution relation" (see [6, § 6.1]):

$$(y_n) = \mathfrak{A}\,\mathfrak{B}^{1-\sigma_n} \mapsto \mathfrak{B} \in \mathcal{I}_{i+1}^n \mapsto \mathfrak{b} := \mathrm{N}_{k_n/k}(\mathfrak{B}) \mapsto \Lambda_{i+1}^n \cdots$$

The natural conjecture being that the class and norm factors become trivial in a bounded number of steps (uniformly in n large enough). In other words, $c+\rho \neq 0$ should indicate a very strange and incredible algorithmic phenomenon.

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

We have seen the significance of the ideals of k of the form $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$, $\mathfrak{A}$ in the group I_{k_n} of prime to p ideals of k_n. This concerns the two following directions:

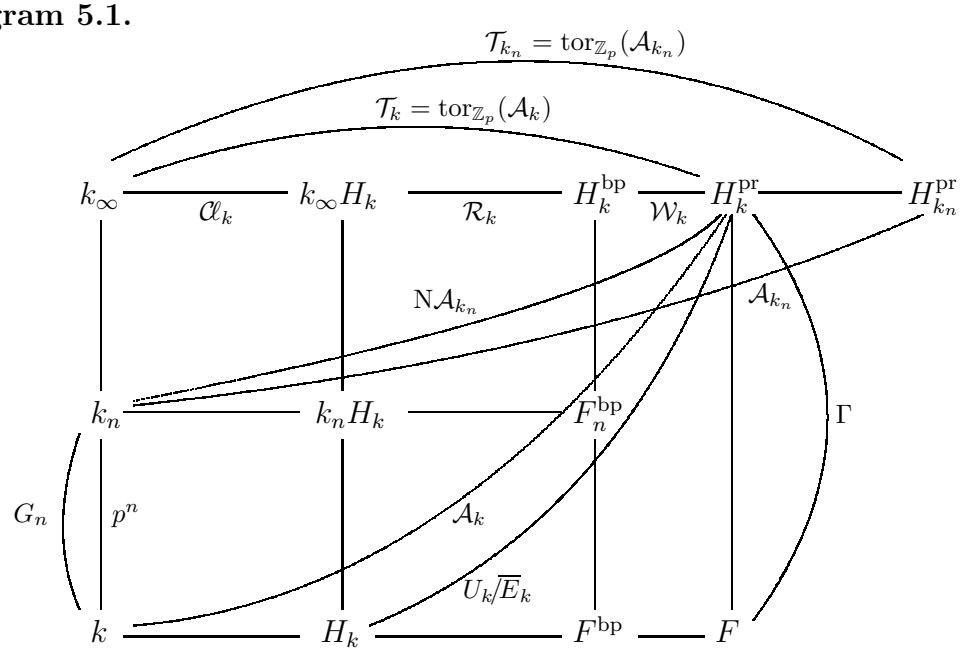
(i) The class factors $\frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_i^n)}$ where $\mathrm{N}_{k_n/k}(M_i^n)$ is generated by the classes of $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$, $\mathfrak{A} \in \mathcal{I}_i^n$, where the $\mathcal{I}_i^n$ (n fixed) are given by an algorithm.

(ii) The norm factors $\frac{p^{n\cdot(r_p-1)}}{(\Lambda_i^n : \Lambda_i^n \cap \mathrm{N}_{k_n/k}({k_n}^\times))}$, where the groups Λ_i^n are the sets of numbers $x \in k^\times$ such that $(x) = \mathrm{N}_{k_n/k}(\mathfrak{A})$, $\mathfrak{A} \in \mathcal{I}_i^n$ as above.

We have seen that in the two cases, the ideals $\mathfrak{A} \in \mathcal{I}_i^n$ may be arbitrarily modified modulo principal ideals of k_n, whence $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$ defined up to $\mathrm{N}_{k_n/k}(k_n^\times)$. This non-unicity hides some structural aspects of Greenberg's conjecture. So we intend to analyze these ideal norms in relation with the invariant $\mathcal{T}_k$ or more precisely its "sub-invariants" $\mathcal{C}\ell_k$ and $\mathcal{R}_k$.

5.1. **Decomposition of $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$ – The fundamental ideal $\mathfrak{t}$.** We consider the following diagram where H_k^{pr} and $H_{k_n}^{\mathrm{pr}}$ are 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^{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 $\Gamma = \mathrm{Gal}(H_k^{\mathrm{pr}}/F) \simeq \mathbb{Z}_p$.

Diagram 5.1.



We consider the Artin symbols $\left(\frac{H_k^{\mathrm{pr}}/k}{\cdot}\right)$ and $\left(\frac{H_{k_n}^{\mathrm{pr}}/k_n}{\cdot}\right)$, defined on $I_k \otimes \mathbb{Z}_p$ and $I_{k_n} \otimes \mathbb{Z}_p$, where I_k and I_{k_n} are the groups of prime to p ideals of k and k_n, respectively. Their images are the Galois groups $\mathcal{A}_k$ and $\mathcal{A}_{k_n}$; their kernels are the groups of infinitesimal principal ideals $\mathcal{P}_{k,\infty}$ et $\mathcal{P}_{k_n,\infty}$, where $\mathcal{P}_{k,\infty}$ is the set of ideals (x_∞), $x_\infty \in k^\times \otimes \mathbb{Z}_p$, prime to p, with trivial image in U_k (idem for k_n) (see, e.g., [2, Theorem III.2.4, Proposition III.2.4.1] and [9, Chap. 1, § (d)]).

The action of the arithmetic norm in k_n/k is given by the diagram; in particular, $\mathrm{N}_{k_n/k}(\mathcal{A}_{k_n}) = \mathrm{Gal}(H_k^{\mathrm{pr}}/k_n)$ and $\mathrm{N}_{k_n/k}(\mathcal{T}_{k_n}) = \mathcal{T}_k$.

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 by the following result:

Proposition 5.2. *Let $\mathfrak{A} \in I_{k_n}$ (ordinary ideal seen in $I_{k_n} \otimes \mathbb{Z}_p$).*

(i) There exist ideals $\mathfrak{c},\mathfrak{t}\in I_k\otimes\mathbb{Z}_p$ *and* $(x_\infty)\in\mathcal{P}_{k,\infty}$*, such that:*

$$\mathrm{N}_{k_n/k}(\mathfrak{A})=\mathfrak{c}^{p^n}\cdot\mathfrak{t}\cdot(x_\infty),\quad\text{with }\left(\frac{H_k^{\rm pr}/k}{\mathfrak{c}}\right)\in\Gamma,\ \left(\frac{H_k^{\rm pr}/k}{\mathfrak{t}}\right)\in\mathcal{T}_k.$$

(ii) There exist some $\alpha_n\in k_n^\times$ *such that* $\iota\mathrm{N}_{k_n/k}(\alpha_n)$ *is arbitrarily close to* 1 *in* U_k *and such that* $\mathrm{N}_{k_n/k}(\mathfrak{A})\,\mathrm{N}_{k_n/k}(\alpha_n)^{-1}=\mathfrak{t}'\cdot(x_\infty)$, $\left(\frac{H_k^{\rm pr}/k}{\mathfrak{t}'}\right)\in\mathcal{T}_k$.

(iii) Under this condition of approximation, $\mathfrak{t}$ *is unique (modulo* $\mathcal{P}_{k,\infty}$*).*

Proof. (i) The map $\mathrm{N}_{k_n/k}$ on $I_{k_n}\otimes\mathbb{Z}_p$ induces the restriction $\mathcal{A}_{k_n}\to\mathcal{A}_k$ giving $\mathrm{N}_{k_n/k}(\mathcal{A}_{k_n})=\Gamma^{p^n}\oplus\mathcal{T}_k$ since $\mathrm{N}_{k_n/k}(\mathcal{A}_{k_n})=\mathrm{Gal}(H_k^{\rm pr}/H_k^{\rm pr}\cap k_n)=\mathrm{Gal}(H_k^{\rm pr}/k_n)$. It follows that $\mathrm{N}_{k_n/k}(\mathfrak{A})$ is of the required form.

(ii) Let $N\gg n$; from the total ramification of p in k_N/k_n, we see that $\mathcal{C}\ell_{k_n}=\mathrm{N}_{k_N/k_n}(\mathcal{C}\ell_{k_N})$. Write $\mathfrak{A}=\mathrm{N}_{k_N/k_n}(\mathfrak{A}_N)\,(\alpha_n^N)$, $\mathfrak{A}_N\in I_{k_N}\otimes\mathbb{Z}_p$, $\alpha_n^N\in k_n^\times$; then $\mathrm{N}_{k_n/k}(\mathfrak{A})=\mathrm{N}_{k_N/k}(\mathfrak{A}_N)\,\mathrm{N}_{k_n/k}(\alpha_n^N)$. The previous decomposition yields:

$$\mathrm{N}_{k_N/k}(\mathfrak{A}_N)=\mathfrak{c}'^{p^N}\cdot\mathfrak{t}'=(\alpha'^N)\cdot\mathfrak{t}'\pmod{\mathcal{P}_{k,\infty}},$$

$\alpha'^N\in k^\times$, with $\iota\alpha'^N$ arbitrarily close to 1 in U_k regarding N. Thus, being local norm at the tame places (as p^nth power of an ideal) and local norm at p (as p^nth power in U_k), $\alpha'^N=\mathrm{N}_{k_n/k}(\alpha_n'^N)$, with $\alpha_n'^N\in k_n^\times$, whence the claim with $\alpha_n:=\alpha_n'^N\,\alpha_n^N$.

(iii) Assume that (modulo $\mathcal{P}_{k,\infty}$) $\mathrm{N}_{k_N/k}(\mathfrak{A})=(\alpha)\cdot\mathfrak{t}=(\alpha')\cdot\mathfrak{t}'$ in k, with $\iota\alpha$ and $\iota\alpha'$ close to 1 as in (ii), whence $\mathfrak{t}'\,\mathfrak{t}^{-1}=(a)$ with ιa close to 1; then there exists p^e (e.g., the exponent of $\mathcal{T}_k$) such that $(a^{p^e})=(a_\infty)\in\mathcal{P}_{k,\infty}$, which gives $a^{p^e}=\varepsilon\,a_\infty$, $\varepsilon\in E_k\otimes\mathbb{Z}_p$, so that $\iota\varepsilon$ is close to 1, hence of the form $\varepsilon=\eta^{p^e}$ with $\iota\eta$ close to 1 (Leopoldt's conjecture). From the relation $(a\,\eta^{-1})^{p^e}=a_\infty$ we get $\iota(a\,\eta^{-1})=\xi\in W_k$; but we know that both ιa and $\iota\eta$ are close to 1 in U_k, thus $\xi=1$ and $a\,\eta^{-1}=a'_\infty$ giving $\mathfrak{t}'\,\mathfrak{t}^{-1}=(a'_\infty)$. □

Definition 5.3. *We shall call this unique ideal* $\mathfrak{t}$*, of finite order modulo* $\mathcal{P}_{k,\infty}$*, the fundamental ideal associated to the class* $\mathrm{N}_{k_n/k}(\mathfrak{A})\cdot\mathrm{N}_{k_n/k}(k_n^\times)$ *of* $\mathrm{N}_{k_n/k}(\mathfrak{A})$*. We denote it* $\mathfrak{t}(\mathfrak{a})$*, where* $\mathfrak{a}:=\mathrm{N}_{k_n/k}(\mathfrak{A})$ *up to* $\mathrm{N}_{k_n/k}(k_n^\times)$*.*

5.2. Images of the ideal $\mathfrak{t}$ in $\mathcal{C}\ell_k$ and $\mathcal{R}_k$.

5.2.1. *Class factors and ideals* $\mathfrak{t}$*.* The $\mathrm{N}_{k_n/k}(\mathcal{I}_i^n)$, representing $\mathrm{N}_{k_n/k}(M_i^n)$ and defining the class factors, are generated, modulo $\mathrm{N}_{k_n/k}(k_n^\times)$, by some $\mathfrak{t}\in I_k\otimes\mathbb{Z}_p$, of finite order modulo $\mathcal{P}_{k,\infty}$, with $\mathcal{C}\ell_k(\mathfrak{t})\in\mathrm{N}_{k_n/k}(M_i^n)$.

5.2.2. *Norm factors and ideals* $\mathfrak{t}$*.* The $\Lambda_i^n=\{x\in k^\times,(x)\in\mathrm{N}_{k_n/k}(\mathcal{I}_i^n)\}$, defining the norm factors, are obtained via ideals (x) such that $(x)\,\mathrm{N}_{k_n/k}(\alpha_n)^{-1}=\mathfrak{t}$ (mod $\mathcal{P}_{k,\infty}$), $\alpha_n\in k_n^\times$, where $\mathfrak{t}$ is principal of finite order modulo $\mathcal{P}_{k,\infty}$.

5.2.3. *Definition of* $\log(\mathfrak{t})\in\mathcal{R}_k$ *for* $\mathfrak{t}$ *principal.* Let $\mathfrak{t}=(x)$, $x\in k^\times\otimes\mathbb{Z}_p$, be a principal fundamental ideal (of finite order modulo $\mathcal{P}_{k,\infty}$). There exists a power p^e such that $x^{p^e}=\varepsilon\,x_\infty$, $\varepsilon\in E_k\otimes\mathbb{Z}_p$; thus $\iota\mathrm{N}_{k/\mathbb{Q}}(x)=1$ or ±1 and the image of ιx is defined in $U_k^*/\overline{E}_k$. Then we consider the image of $\log(\iota x)$ in $\log(U_k^*)/\log(\overline{E}_k)=\mathcal{R}_k$, which defines the element of $\mathcal{R}_k$:

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

Lemma 5.4. *Let* $x\in k^\times\otimes\mathbb{Z}_p$*, such that* $(x)\in\mathrm{N}_{k_n/k}(\mathcal{I}_i^n)$*. Then* x *is local norm at* p *in* k_n/k *(whence global norm) if and only if any representative of* x *modulo* $W_k=\bigoplus_{\mathfrak{p}|p}\mu_p(k_\mathfrak{p})$ *is local norm at* p*.*

Proof. Let $\mathfrak{p} \mid p$ in k and let $\mathfrak{p}_n \mid \mathfrak{p}$ be the unique prime of k_n above $\mathfrak{p}$. Let $k_\mathfrak{p}$ and $k_{n,\mathfrak{p}_n}$ be the respective completions. We must show that each $\mu_p(k_\mathfrak{p})$ is in the local norm group. We have four cases:

(i) Case $p \neq 2$ and $\mu_p(k_\mathfrak{p}) = 1$. The norm condition is trivially fulfilled.

(ii) Case $p \neq 2$ and $\mu_p(k_\mathfrak{p}) \neq 1$. Let p^ν, $\nu \geq 1$, be the order of $\mu_p(k_\mathfrak{p})$; then $\mu_p(k_{n,\mathfrak{p}_n})$ is of order $p^{\nu+n}$. Thus, in that case, $\mathrm{N}_{k_{n,\mathfrak{p}_n}/k_\mathfrak{p}}(\mu_p(k_{n,\mathfrak{p}_n})) = \mu_p(k_\mathfrak{p})$.

(iii) Case $p = 2$ and $\mu_2(k_\mathfrak{p}) \supseteq \mu_4$. The proof is similar to that of case (ii).

(iv) Case $p = 2$ and $\mu_2(k_\mathfrak{p}) = \mu_2$. We know that, in $\mathbb{Q}_n/\mathbb{Q}$, -1 is a global norm as norm of the generating cyclotomic unit of $\mathbb{Q}_n$. □

From the exact sequence (1) and the Lemma 5.4, the norm properties of x in k_n/k do not depend on the representative of x modulo W_k, which is precisely the kernel of log, and the map:

$$\{\mathfrak{t} = (x), \text{ of finite order modulo } \mathcal{P}_{k,\infty}\} \xrightarrow{\log} \mathcal{R}_k$$

is surjective of kernel $\{\mathfrak{t} = (x),\ x \in k^\times \otimes \mathbb{Z}_p, \text{ such that } \iota x \in W_k\}$.

5.2.4. *Conclusion about the role of the fundamental ideals* $\mathfrak{t}$. We assume that the ideals $\mathfrak{A}$ of k_n are random variables as well as the norms $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$; so this suggests that the fundamental ideal $\mathfrak{t} = \mathfrak{t}(\mathfrak{a})$ of k is a random variable. In other words, both $\mathcal{cl}_k(\mathfrak{t}(\mathfrak{a}))$ and $\log(\mathfrak{t}(\mathfrak{a}))$ (when $\mathfrak{t}(\mathfrak{a})$ is principal) are random in $\mathcal{C}\ell_k$ and $\mathcal{R}_k$, respectively.

This yields the following heuristics/conjectures:

(i) The class of $\mathfrak{t}(\mathfrak{a})$, governing the class factor, is uniformly distributed in $\mathcal{C}\ell_k$.

(ii) When $\mathfrak{t}(\mathfrak{a}) = (x)$, the image $\log(\mathfrak{t}(\mathfrak{a})) = \log(\iota x) \pmod{\log(\overline{E}_k)}$, governing the norm factor, is uniformly distributed in the normalized regulator $\mathcal{R}_k$.

A proof of such density results would be the key for the proof of Greenberg's conjecture since the reciprocal is obvious (use Theorem 3.4 and consider comments following Corollary 3.5).

5.3. **Galois descent of $\mathcal{T}_k$.** Although the Galois descent of $H_k^{\mathrm{pr}}/k_\infty$, into F/k, is not necessary in a theoretical point of view, it shows, in a numerical context, the conditions of repartition of the Artin symbols $\left(\frac{F/k}{\mathfrak{a}}\right)$, of norms $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$ in the cyclotomic tower, which is the key for any heuristic about class and norm factors of the algorithms, via the ideals $\mathfrak{t}(\mathfrak{a})$. The field F (more precisely its subfield F^{bp}) is, in some sense, a "governing field" for Greenberg's conjecture. See a numerical example in [6, § 8.1].

Theorem 5.5. *The fundamental ideal* $\mathfrak{t}(\mathfrak{a})$, $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$, *deduced from the class of* $\mathfrak{a} \pmod{\mathrm{N}_{k_n/k}(k_n^\times)}$, *is intrinsic and does not depend on the choice of* F.

Proof. Let F'/k be another solution; then, referring to suitable expressions of Proposition 5.2, we get, modulo $\mathcal{P}_{k,\infty}$, with obvious notations for F and F':

$$\mathrm{N}_{k_n/k}(\mathfrak{A})\,\mathrm{N}_{k_n/k}(\alpha_n)^{-1} = \mathfrak{t}, \quad \mathrm{N}_{k_n/k}(\mathfrak{A})\,\mathrm{N}_{k_n/k}(\alpha'_n)^{-1} = \mathfrak{t}',$$

with $\iota\mathrm{N}_{k_n/k}(\alpha_n)$, $\iota\mathrm{N}_{k_n/k}(\alpha'_n)$ close to 1. Thus $\mathfrak{t}'\,\mathfrak{t}^{-1} = (a)$, $a \in k^\times$, with ιa close to 1, giving $\mathfrak{t}' = \mathfrak{t}$ (modulo $\mathcal{P}_{k,\infty}$) from proof of point (iii) of Proposition 5.2. □

References

[1] Chevalley, C.: 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://archive.numdam.org/item/THESE_1934__155__365_0/

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

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

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

[5] Gras, G.: Approche p-adique de la conjecture de Greenberg pour les corps totalement réels. Annales Mathématiques Blaise Pascal **24**(2) (2017), 235–291. https://ambp.cedram.org/cedram-bin/article/AMBP_2017__24_2_235_0.pdf

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

[7] Gras, G.: 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://dergipark.org.tr/en/download/article-file/906434

[8] Greenberg, R.: On the Iwasawa invariants of totally real number fields. Amer. J. Math. **98**(1) (1976), 263–284. http://www.jstor.org/stable/2373625?seq=1#page_scan_tab_contents

[9] Jaulent, J-F.: 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] Jaulent, J-F.: Note sur la conjecture de Greenberg. J. Ramanujan Math. Soc. **34** (2019) 59–80. https://www.math.u-bordeaux.fr/~jjaulent/

[11] Jaulent, J-F.: Normes universelles et conjecture de Greenberg. Acta Arithmetica **194** (2020), 99–109. https://www.math.u-bordeaux.fr/~jjaulent/

[12] Jaulent, J-F.: 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/

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

[14] Nguyen Quang Do, T.: Sur la conjecture faible de Greenberg dans le cas abélien p-décomposé. Int. J. of Number Theory **2**(1) (2006), 49–64. http://www.worldscientific.com/doi/pdf/10.1142/S1793042106000395

[15] Nguyen Quang Do, T.: 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

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

[17] Ozaki, M. and Taya, H.: A note on Greenberg's conjecture for real abelian number fields. Manuscripta Math., **88**(1) (1995), 311–320. http://link.springer.com/article/10.1007/BF02567825

[18] Taya, H.: 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://www.jstage.jst.go.jp/article/tmj1949/51/1/51_1_21/_pdf

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