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 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 ($\lambda = \mu = 0$) 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. A suitable property of uniform distribution of these images would lead to accessible proofs of density results for Greenberg's conjecture, which remains hopeless within the sole framework of Iwasawa's theory. Indeed, many "algebraic/class field theory" criteria exist for Greenberg's conjecture, which hide a broad p-adic arithmetic and algorithmic complexity governed by $\mathcal{T}_k$. No assumption is made on the degree of k nor on the decomposition of p in $k/\mathbb{Q}$.

CONTENTS

1. Introduction 2
2. Abelian p-ramification and genus theories 3
2.1. Abelian p-ramification – The torsion group $\mathcal{T}_k$ 3
2.2. Genus theory in k_n/k 4
2.3. Ramification in $H_k^{\rm pr}/k_\infty$ 6
2.4. Criteria for Greenberg's conjecture 7
3. Filtration of $\mathcal{C}\ell_{k_n}$ 10
3.1. General algorithm – Class and Norm factors 10
3.2. The n-sequences $\mathcal{C}\ell_{k_n}^{i+1}/\mathcal{C}\ell_{k_n}^{i}$ for i fixed 12
4. $\mathcal{C}\ell_k$ and $\mathcal{R}_k$ as governing invariants of the algorithms 14
4.1. Decomposition of $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$ – The fundamental ideals $\mathfrak{t}(\mathfrak{a})$ 14
4.2. Images of the ideals $\mathfrak{t}(\mathfrak{a})$ in $\mathcal{C}\ell_k$ and $\mathcal{R}_k$ 16
4.3. Galois descent of $\mathcal{T}_k$ 17
References 17

Date: May 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.

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 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.

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 (i.e., unramified outside p and ∞) 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 "*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*:

$$\#\mathcal{T}_k^{\rm res} = 2^d\,\#\mathcal{T}_k^{\rm ord} \quad [4,\ \text{Theorem III.4.1.5}],$$

knowing that, for totally real number fields:

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

which makes coherent the formulas $\#\mathcal{T} = \#\mathcal{C}\ell\,\#\mathcal{R}\,\#\mathcal{W}$ 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 the origin of the conjecture in [13, 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 [12] for new approach on Vandiver's conjecture, [9, 24] for annihilation aspects in p-ramification).

Main recent studies of this conjecture, after the pioneering work of Ozaki, Taya [25, 26, 28, 29], are [7, 10, 15, 16, 17, 21, 22, 23]. In [16, Théorème A] a new criterion is given (capitulation in some k_{n_0} of the logarithmic class group of k), in [17] the Greenberg conjecture is stated in terms of "universal norms". In [23] a synthetic view of the criteria of Greenberg, Jaulent and others, is given by means of Iwasawa's theory. See a more complete description of these criteria in § 2.4. Then we shall explain in what sense these criteria hide a tricky arithmetic complexity, materialized by the algorithm given and studied in Sections 3.

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

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 [13]:

(i) The case 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 (e.g., $p = 2$ and $k = \mathbb{Q}(\sqrt{2m})$, $m \equiv 1 \pmod 4$).

(ii) The case of p totally split in $k/\mathbb{Q}$.

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" $\mathcal{R}_k$.

Main results. The results of the paper may be described as follows. The algorithm, determining $\#\mathcal{C}\ell_{k_n}$ at the stage k_n (whence giving the Iwasawa invariants for $n \gg 0$), computes inductively the classical filtration $(\mathcal{C}\ell_{k_n}^i)_{i\geq 0}$, where $\mathcal{C}\ell_{k_n}^{i+1}/\mathcal{C}\ell_{k_n}^i := (\mathcal{C}\ell_{k_n}/\mathcal{C}\ell_{k_n}^i)^{G_n}$ for all $i \geq 0$ and $\mathcal{C}\ell_{k_n}^0 = 1$, where $G_n = {\rm Gal}(k_n/k)$. We have the decreasing sequence, where $r_p \geq 1$ is the number of p-places of k:

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

where Λ_n^i is the subgroup of $k^\times$ of elements x such that $(x) = {\rm N}_{k_n/k}(\mathfrak{A})$ for some representatives $\mathfrak{A}$ such that $\mathcal{C}\ell_{k_n}(\mathfrak{A}) \in \mathcal{C}\ell_{k_n}^i$, giving the increasing sequence (from $\Lambda_n^0 = E_k$):

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

The length of the algorithm depends on the decreasing evolution of the "class factors" $\frac{\#\mathcal{C}\ell_k}{\#{\rm N}_{k_n/k}(\mathcal{C}\ell_k^i)}$ dividing $\#\mathcal{C}\ell_k$ and the "norm factors" $\frac{p^{n\cdot(r_p-1)}}{(\Lambda_n^i : \Lambda_n^i \cap {\rm N}_{k_n/k}(k_n^\times))}$ dividing the order of a suitable quotient $\mathcal{R}_k^{\rm nr}$ of the normalized p-adic regulator $\mathcal{R}_k$, related to the ramification in $H_k^{\rm pr}/k_\infty$ (Theorems 2.8, 3.3). Whence the obvious consequence:

$$\mathcal{C}\ell_k = \mathcal{R}_k^{\rm nr} = 1 \Longleftrightarrow \lambda = \mu = \nu = 0. \tag{1}$$

When $\mathcal{C}\ell_{k_n}^{i+1}/\mathcal{C}\ell_{k_n}^i$ becomes trivial for some $i = m_n$ (thus $\mathcal{C}\ell_{k_n} = \mathcal{C}\ell_n^{m_n}$), the two factors are trivial and one gets (Theorem 3.4 and Corollary 3.5):

$$\mathcal{C}\ell_k \cdot \mathcal{R}_k^{\rm nr} \neq 1 \Longrightarrow m_n \geq \frac{1}{v_p(\#\mathcal{C}\ell_k \#\mathcal{R}_k^{\rm nr})} \cdot (\lambda \cdot n + \mu \cdot p^n + \nu), \tag{2}$$

where v_p is the p-adic valuation. Note that under Greenberg's conjecture, the algorithm must give $m_n = 1$ for all $n \gg 0$ (Theorem 2.11 (i)).

So the main question is the algorithmic complexity, analyzed in Section 4, which suggests possible analytic proof in the framework of techniques used in [19] in a particular case (degree p cyclic extensions), but very powerful.

The hope for such a proof comes from the fact that the algorithm computing $\mathcal{C}\ell_{k_n}$ is "governed" by means of finite invariants of k (that is to say $\mathcal{T}_k$, from Theorems 4.2, 4.5 giving a relation between the ideal norms in k_∞/k and some ideals $\mathfrak{t}$ of k whose Artin symbols are in $\mathcal{T}_k$). For instance, the inequality in (2) shows that if λ or μ is non-zero, the sequence m_n is unbounded while each step of the algorithm only depends on finite number of possibilities by taking the class of the random ideal $\mathfrak{t}$ of k and by computing Hasse's symbols at the p-places of the random element τ of $k^\times$ when $\mathfrak{t} = (\tau)$ is principal, in other words, a classical situation involving p-ranks of random $\mathbb{F}_p$-matrices.

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 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 [11, Appendix 1] for a wide story of abelian p-ramification theory in its various aspects).

(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

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

Since $\mu(k) = \{\pm 1\}$, $\mathcal{W}_k := W_k$ for $p \neq 2$ and $\mathcal{W}_k := W_k/\langle \pm 1\rangle$ for $p = 2$.
Let $\iota : \{x \in k^\times \otimes \mathbb{Z}_p,\ x \text{ prime to } p\} \longrightarrow U_k$ 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 $p \neq 2$ ($\mathrm{N}_{k/\mathbb{Q}}(u) = \pm 1$ 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 [8, § 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) The sub-module of $\mathcal{T}_k$ fixing the Bertrandias–Payan field $H_k^{\rm bp}$ is $\mathcal{W}_k$. 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 [5] 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. [8, § 4, § 5]. *We have the exact sequences:*

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

$$1 \to \mathcal{W}_k \longrightarrow \mathrm{tor}_{\mathbb{Z}_p}(U_k/\overline{E}_k) \longrightarrow \mathrm{tor}_{\mathbb{Z}_p}(\log(U_k)/\log(\overline{E}_k)) \simeq \mathcal{R}_k \to 0. \tag{3}$$

2.2. **Genus theory in k_n/k.** We denote by H_k and H_{k_n} the p-Hilbert class fields of k and k_n, respectively. 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 $G_n = \mathrm{Gal}(k_n/k)$.
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., [4, Corollary IV.4.4.1]):

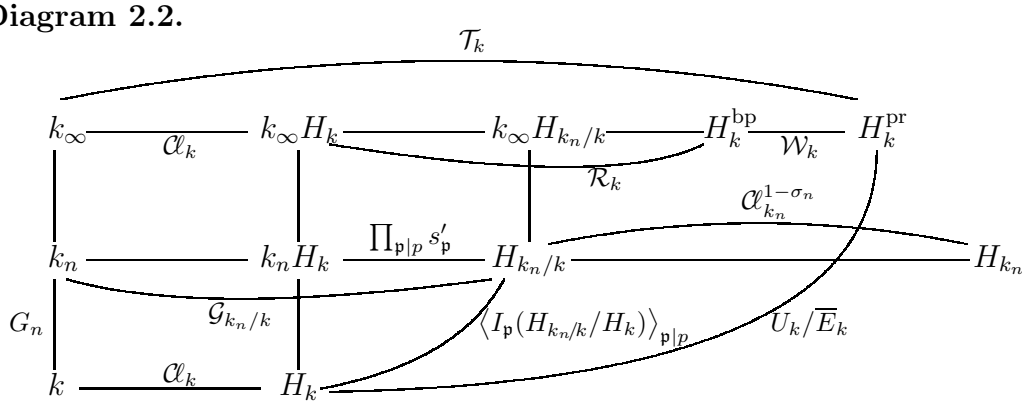
$$1 \to E_k/E_k \cap \mathrm{N}_{k_n/k}(k_n^\times) \xrightarrow{\omega_n} \Omega(k_n/k) \xrightarrow{\pi_n} \mathrm{Gal}(H_{k_n/k}/k_nH_k) \to 1,$$

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.
The image of ω_n is contained in $\Omega(k_n/k)$ and the map π_n is defind as follows: with $(s_\mathfrak{p})_{\mathfrak{p}\mid p} \in G_n^{r_p}$, 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 $(s_\mathfrak{p})_{\mathfrak{p}\mid p} \in \Omega(k_n/k)$, then $\prod_{\mathfrak{p}\mid p} s'_\mathfrak{p}$ 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 number formula [2],

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

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 in k_n/k.

Diagram 2.2.



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

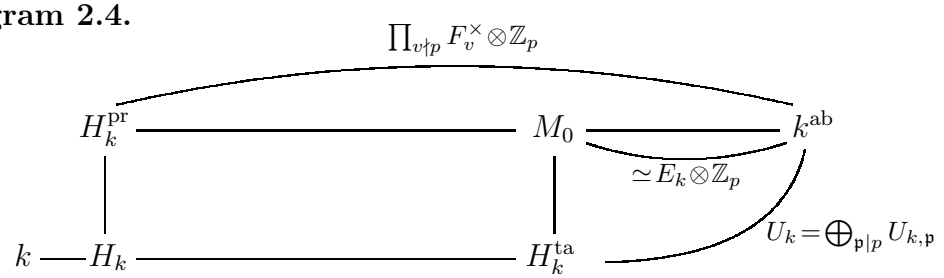
(ii) The n-sequence $\#\mathcal{G}_{k_n/k}$ is increasing and stabilizes at a divisor of $\#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k$.

(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 and let $c\ell_{k_n}(S_{k_n})$ be the subgoup of $\mathcal{C}\ell_{k_n}$ generated by the $c\ell_{k_n}(\mathfrak{p})$, $\mathfrak{p} \mid p$.

Then, for all $n \geq 0$, the orders of $\mathrm{J}_{k_n/k}(\mathcal{C}\ell_k) \cdot c\ell_{k_n}(S_{k_n})$ are bounded by $\#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k$.

Proof. Using the idelic global reciprocity map (under Leopoldt's conjecture), we have the fundamental diagram [4, § 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 place v (finite or infinite). We know that the fixed field of the maximal tame sub-extension H_k^{ta} is $U_k = \bigoplus_{\mathfrak{p}|p} U_{k,\mathfrak{p}}$ 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 $k_\infty H_{k_n/k}$ 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 $W_k/\mu_p(k) = \mathcal{W}_k$ whose fixed field is H_k^{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 2.2). Point (iii) results of the inclusion $\mathrm{J}_{k_n/k}(\mathcal{C}\ell_k) \cdot c\ell_{k_n}(S_{k_n}) \subseteq \mathcal{C}\ell_{k_n}^{G_n}$ since $\#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{G}_{k_n/k}$ for all n. □

[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.

Remarks 2.5. (i) Since $\mathcal{G}_{k_n/k}$ is "constant" for all $n \gg 0$, we can put $\mathcal{G}_k := \mathcal{G}_{k_n/k}$ independently of n large enough. This group will be called, by abuse, the genus group of k; then the field:

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

is unramified over k_∞ and of Galois group $\mathcal{G}_k$.

(ii) Let k_0 be a totally real number field in which p totally splits and totally ramifies in $k_{0,\infty}/k_0$ (i.e., $r_p = d$). We have $\mathcal{W}_{k_0} = 1$ 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 2.9). This classical case is due to Taya [29, Theorem 1.1]; see analogous approaches in [7, Théorème 4.8], [16, § 2.1, § 2.2, Corollaire 11], [23, Théorème C].

(iii) The case of a single place in k_∞ (i.e., $r_p = 1$ giving $\dfrac{p^{n\cdot(r_p-1)}}{(E_k : E_k \cap {\rm N}_{k_n/k}(k_n^\times))} = 1$ for all n) is also considered in these papers; 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 (4)) will be trivial.

We shall 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 section in which we characterize a quotient $\mathcal{R}_k^{\rm nr} = \mathcal{R}_k/\mathcal{R}_k^{\rm ram}$, of $\mathcal{R}_k$, such that $\#\mathcal{G}_k = \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\rm nr}$.

2.3. **Ramification in $H_k^{\rm pr}/k_\infty$.** Give more information about the ramification of the p-places in $H_k^{\rm pr}/k_\infty$. Recall, once for all, that the tame places totally split in $H_k^{\rm pr}/k_\infty$ [4, Remark III.4.8.2].

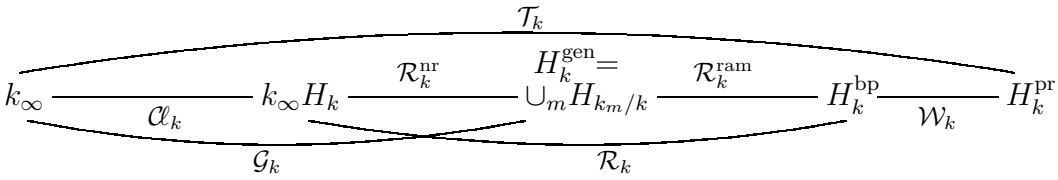
Proposition 2.6. *Let $n_0 \gg 0$ be such that $\#\mathcal{G}_{k_n/k}$ (hence the increasing normic factor $\dfrac{p^{n\cdot(r_p-1)}}{(E_k : E_k \cap {\rm N}_{k_n/k}(k_n^\times))}$) stabilizes for all $n \geq n_0$; this defines the "genus field" $H_k^{\rm gen} := \bigcup_m H_{k_m/k}$, such that ${\rm Gal}(H_k^{\rm gen}/k_\infty) = \mathcal{G}_k$. Then $H_k^{\rm gen}$ is the maximal unramified extension of k_∞ in $H_k^{\rm pr}$ and ${\rm Gal}(H_k^{\rm pr}/H_k^{\rm gen}) \simeq \big\langle {\rm tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}}\overline{E}_k/\overline{E}_k)\big\rangle_{\mathfrak{p}\mid p}$.*

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 ${\rm Gal}(L_\infty/L) \simeq {\rm Gal}(L'_\infty/L') \simeq \mathbb{Z}_p$. 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 ${\rm Gal}(L'_\infty/L)$ or ${\rm Gal}(L'_\infty/L')$, 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 ${\rm tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}}\overline{E}_k/\overline{E}_k)$ (see Diagram 2.4). □

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

Diagram 2.7.



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

Theorem 2.8. *Let n_0 be such that the genus groups $\mathcal{G}_{k_n/k} = \mathrm{Gal}(k_\infty H_{k_n/k}/k_\infty)$ stabilize for all $n \geq n_0$ giving the genus group $\mathcal{G}_k$.*
Then $\#\mathcal{G}_k = \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\mathrm{nr}}$, equivalent to $\dfrac{p^{n\cdot(r_p-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))} = \#\mathcal{R}_k^{\mathrm{nr}}$ for all $n \geq n_0$.

Corollary 2.9. *(i) If p is totally split in k ($r_p = d$) and totally ramified in k_∞/k, then $\mathcal{R}_k^{\mathrm{ram}} = 1$ and $\mathcal{R}_k^{\mathrm{nr}} = \mathcal{R}_k$.*
(ii) If there is a unique p-place in k_∞ ($r_p = 1$), then $\mathcal{R}_k^{\mathrm{ram}} = \mathcal{R}_k$ and $\mathcal{R}_k^{\mathrm{nr}} = 1$.

Proof. (i) If $r_p = d$, one obtains $\mathcal{W}_k = 1$ and $U_{k,\mathfrak{p}}\overline{E}_k/\overline{E}_k = U_{k,\mathfrak{p}}/\overline{E}_k \cap U_{k,\mathfrak{p}}$; 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 $H_k^{\mathrm{bp}} = H_k^{\mathrm{pr}}$, giving $\mathcal{R}_k^{\mathrm{ram}} = 1$.
(ii) 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. □

Otherwise, these inertia groups are only accessible by means of numerical computations (this is done in [11] in the context of incomplete p-ramification); they give $H_k^{\mathrm{gen}} = \bigcup_m H_{k_m/k}$ independently of the knowledge of $\mathcal{G}_k$. It would be interesting to interpret $\mathcal{R}_k^{\mathrm{ram}}$ in terms of units of k.

Corollary 2.10. *Let S_{k_n} be the set of p-places of k_n. We have the exact sequence $1 \to \mathrm{J}_{k_n/k}(\mathcal{C}\ell_k)\,\mathcal{C}\ell_{k_n}(S_{k_n}) \longrightarrow \mathcal{C}\ell_{k_n}^{G_n} \xrightarrow{\theta} E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)/\mathrm{N}_{k_n/k}(E_{k_n}) \to 1$. Thus the orders of the subgroups $\mathrm{J}_{k_n/k}(\mathcal{C}\ell_k)\,\mathcal{C}\ell_{k_n}(S_{k_n})$ are bounded by $\#\mathcal{G}_k = \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\mathrm{nr}}$.*

Proof. We have the exact sequence:

$$1 \to \mathcal{C}\ell_{k_n}(I_{k_n}^{G_n}) = \mathrm{J}_{k_n/k}(\mathcal{C}\ell_k)\,\mathcal{C}\ell_{k_n}(S_{k_n}) \to \mathcal{C}\ell_{k_n}^{G_n} \xrightarrow{\theta} E_k \cap \mathrm{N}_{k_n/k}(k_n^\times)/\mathrm{N}_{k_n/k}(E_{k_n}) \to 1$$

where I_{k_n} is the $\mathbb{Z}[G_n]$-module of ideals of k_n and where θ associates with $\mathcal{C}\ell_{k_n}(\mathfrak{A})$, 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.
Then $\mathcal{C}\ell_{k_n}(I_{k_n}^{G_n}) = \mathrm{J}_{k_n/k}(\mathcal{C}\ell_k)\,\mathcal{C}\ell_{k_n}(S_{k_n})$. Whence the claim from the equalities $\#\mathcal{G}_{k_n/k} = \#\mathcal{C}\ell_{k_n}^{G_n} = \#\mathcal{G}_k = \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\mathrm{nr}}$ for all $n \gg 0$ (Theorem 2.8). □

2.4. **Criteria for Greenberg's conjecture.** Let k be a totally real number field assuming p totally ramified in k_∞/k (cf. Remark 1.1). We first give some obvious properties of k_∞ under the assumption $\lambda = \mu = 0$.

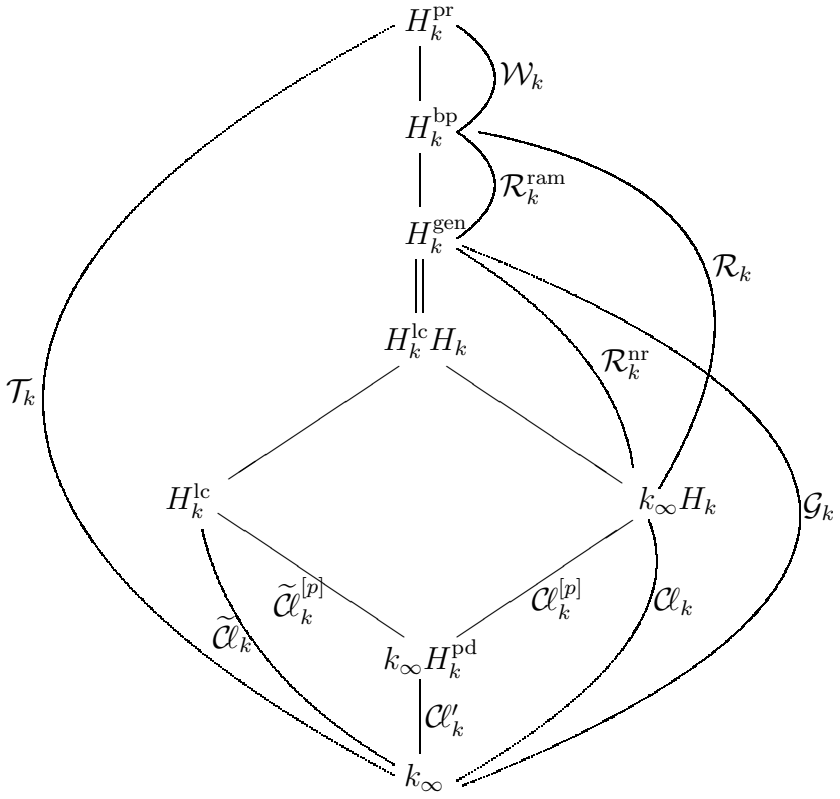
2.4.1. *Consequences of Greenberg's conjecture.* If $\lambda = \mu = 0$, there exists $\nu \geq 0$ and $n_0 \geq 0$ such that $\#\mathcal{C}\ell_{k_n} = p^\nu$ for all $n \geq n_0$; thus, any property fulfilled at the stage k_{n_0} is fulfilled at any stage k_n, $n \geq n_0$. Let $G_n^{n_0} := \mathrm{Gal}(k_n/k_{n_0})$.
Let $\mathcal{R}_{k_n}$ be the normalized p-adic regulator of k_n, then $\mathcal{R}_{k_n}^{\mathrm{ram}}$, $\mathcal{R}_{k_n}^{\mathrm{nr}} \simeq \mathcal{R}_{k_n}/\mathcal{R}_{k_n}^{\mathrm{ram}}$, $\mathcal{G}_{k_n} = \mathrm{Gal}(H_{k_n}^{\mathrm{gen}}/k_\infty)$, where $H_{k_n}^{\mathrm{gen}} = \bigcup_m H_{k_m/k_n}$ is the maximal unramified extension of k_∞ in $H_{k_n}^{\mathrm{pr}}$ (cf. § 2.3, Diagram 2.7).

Theorem 2.11. *Under Greenberg's conjecture, we have the following properties:*
(i) $\mathcal{R}_{k_n}^{\mathrm{nr}} = 1$ for all $n \geq n_0$, then $\mathcal{R}_{k_n}^{\mathrm{ram}} = \mathcal{R}_{k_n}$ which means that the fixed field $H_{k_n}^{\mathrm{gen}}$ of $\langle \mathrm{tor}_{\mathbb{Z}_p}(U_{k_n,\mathfrak{p}}\overline{E}_{k_n}/\overline{E}_{k_n})\rangle_{\mathfrak{p}|p}$ is $k_\infty H_{k_n}$ (see Diagram 2.7 applied to k_n).
(i′) Whence $\mathcal{C}\ell_{k_n}^{G_n^{n_0}} = \mathcal{C}\ell_{k_n}$, of order p^ν, for all $n \geq n_0$.
(ii) For $m \geq n \geq n_0$ the norm maps $\mathrm{N}_{k_m/k_n} : \mathcal{C}\ell_{k_m} \longrightarrow \mathcal{C}\ell_{k_n}$ are isomorphisms.
(iii) For all $n \geq 0$, $\mathcal{C}\ell_{k_n}$ capitulates in k_∞.

Proof. (i) We have (Theorem 2.8), $\#\mathcal{C}\ell_{k_n}^{G_n^{n_0}} = \#\mathcal{C}\ell_{k_{n_0}} \cdot \#\mathcal{R}_{k_{n_0}}^{\rm nr} = p^\nu \cdot \#\mathcal{R}_{k_{n_0}}^{\rm nr}$, for all $n \geq n_0$; thus, as soon as $\#\mathcal{R}_{k_{n_0}}^{\rm nr} > 1$, we get $\#\mathcal{C}\ell_{k_n} \geq \#\mathcal{C}\ell_{k_n}^{G_n^{n_0}} > p^\nu$ (contradiction). We deduce that $\mathcal{C}\ell_{k_n}^{G_n^{n_0}} = \mathcal{C}\ell_{k_n} = \mathcal{G}_{k_n}$, for all $n \geq n_0$.
(ii) Due to the totale ramification of p in k_∞/k, the norm maps $\mathrm{Gal}(H_{k_m}/k_m) \to \mathrm{Gal}(H_{k_n}/k_n)$ are surjective; since $\#\mathcal{C}\ell_{k_m} = \#\mathcal{C}\ell_{k_n} = p^\nu$ these maps are injective.
(iii) Let $\mathcal{C}\ell_{k_m} =: \bigoplus_j \langle c\ell_{k_m}(\mathfrak{A}_j) \rangle$ be a decomposition of the p-class group of k_m into cyclic components. Then, from (ii), $\mathcal{C}\ell_{k_n} = \bigoplus_j \big\langle \mathrm{N}_{k_m/k_n}(c\ell_{k_m}(\mathfrak{A}_j)) \big\rangle$; for such a $c\ell_{k_m}(\mathfrak{A}_j)$, 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 $\mathfrak{l} := \mathrm{N}_{k_m/k_n}(\mathfrak{L})$ in k_n; then $\mathrm{J}_{k_m/k_n}(\mathfrak{l}) = \nu_{k_m/k_n}(\mathfrak{L})$, where $\nu_{k_m/k_n} = \sum_{\sigma \in \mathrm{Gal}(k_m/k_n)} \sigma$ is the algebraic norm. We have $\nu_{k_m/k_n} = p^{m-n} + A(\sigma_n^m) \cdot (1 - \sigma_n^m)$ where σ_n^m is a generator of G_n^m and $A(\sigma_n^m) \in \mathbb{Z}_p[\sigma_n^m]$. Thus, from (i′) with $m - n$ large enough, we get $\mathrm{J}_{k_m/k_n}(c\ell_{k_n}(\mathfrak{l})) = 1$. This proves the capitulation of $\mathcal{C}\ell_{k_n}$ in k_∞ for all $n \geq 0$. □

2.4.2. *The logarithmic class group.* Another approach in Iwasawa's theory is the criterion of Jaulent [16, Théorèmes A, B] proving that Greenberg's conjecture is equivalent to the capitulation in k_∞ of the logarithmic class group $\widetilde{\mathcal{C}\ell}_k$ of k which is much related to $\mathcal{T}_k$ as follows (from the general diagram [16, § 2.3]):

Diagram 2.12.



where $H_k^{\rm lc}$ is the maximal abelian locally cyclotomic pro-p-extension of k (i.e., such that all p-places totally split in $H_k^{\rm lc}/k_\infty$), $\mathcal{C}\ell_k^{[p]} := \big\langle c\ell_k(\mathfrak{p}) \big\rangle_{\mathfrak{p}|p}$, $\widetilde{\mathcal{C}\ell}_k^{[p]}$ is the subgrup of $\widetilde{\mathcal{C}\ell}_k$ generated by the classes of logarithmic divisors of zero degree built on the p-places, and $H_k^{\rm pd}$ is the maximal subfield of H_k in which the p-places totally split; whence $H_k^{\rm lc} \cap k_\infty H_k = k_\infty H_k^{\rm pd}$ & $\mathrm{Gal}(k_\infty H_k^{\rm pd}/k_\infty) \simeq \mathcal{C}\ell'_k$.

Lemma 2.13. *Let $H_k^{\rm gen} = \bigcup_m H_{k_m/k}$; then $H_k^{\rm gen} = H_k^{\rm lc} H_k$ (see Diagram 2.7).*

Proof. Since by definition $H_k^{\rm lc}$ is the maximal extension of k_∞ in which the p-places split completely, the extension $H_k^{\rm gen}/H_k^{\rm lc}$ is unramified and p does not split; thus its Galois group is generated by the Frobenius of the p-places and is isomorphic to $\left\langle cl_k(\mathfrak{p})\right\rangle_{\mathfrak{p}\mid p}$. □

In other words, $H_k^{\rm gen}$ is fixed by the group generated by the inertia groups $I_{\mathfrak{p}}(H_k^{\rm pr}/k_\infty) \simeq {\rm tor}_{\mathbb{Z}_p}(U_{k,\mathfrak{p}}\overline{E}_k/\overline{E}_k)$, $\mathfrak{p} \mid p$, and $H_k^{\rm lc}$ is fixed by the group generated by the decomposition groups $D_{\mathfrak{p}}(H_k^{\rm pr}/k_\infty)$, $\mathfrak{p} \mid p$, which may be computed numerically from [4, Exercice III.7.1].

In [18, Appendice, Définition 17], Jaulent defines the logarithmic regulator as $\widetilde{\mathcal{R}}_k := {\rm Gal}(H_k^{\rm bp}/H_k^{\rm lc})$ (use [16, Diagram, § 2.3]). In the split case where $\mathcal{R}_k^{\rm ram} = 1$, this logarithmic regulator is isomorphic to $\mathcal{C}l_k^{[p]} := {\rm Gal}(k_\infty H_k/k_\infty H_k^{\rm pd})$.

2.4.3. *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 $k_e \subset k_\infty$, all the forthcoming statements hold true for $k' := k_e$ and its tower $\bigcup_{n\geq 0} k'_n$, $[k'_n : k'] = p^n$. We assume the conventions of Remark 1.1, then the Leopoldt and Gross–Kuz'min conjectures for totally real number fields. Let $\Gamma := {\rm Gal}(k_\infty/k)$.

We use the classical objects $A_\infty := \varinjlim \mathcal{C}l_{k_n}$, $X_\infty := \varprojlim \mathcal{C}l_{k_n}$ and similarly A'_∞, X'_∞, from the S_{k_n}-class groups $\mathcal{C}l'_{k_n}$, where S_{k_n} is the set of p-places of k_n. Let $\mathcal{C}l_{k_n}^{[p]} = {\rm Ker}(\mathcal{C}l_{k_n} \to \mathcal{C}l'_{k_n})$ and $\widetilde{\mathcal{C}}l_{k_n}^{[p]} = {\rm Ker}(\widetilde{\mathcal{C}}l_{k_n} \to \mathcal{C}l'_{k_n})$ (cf. Diagram 2.12).

Proposition 2.14 ([15], [16, Théorèmes 4, 5, 7], [17], [20, Théorème 4.2] for $(X_\infty)_\Gamma \simeq \widetilde{\mathcal{C}}l_k$, [23, Proposition 1.1, Théorème 2.1])**.** *Geenberg's conjecture is equivalent to each of the following properties:*

(i) X_∞ is finite;

(i′) X'_∞ is finite;

(ii) $A_\infty = 0$;

(ii′) $A'_\infty = 0$;

(iii) $\mathcal{C}l_{k_n} = p^\nu$ for all $n \gg 0$;

(iii′) $\mathcal{C}l'_{k_n} = p^{\nu'}$ for all $n \gg 0$;

(iv) ${\rm J}_{k_m/k_n}(\mathcal{C}l_{k_n}) = 0$ for all $m \gg n$ (capitulation of $\mathcal{C}l_{k_n}$ in k_∞ for all $n \geq 0$);

(iv′) ${\rm J}_{k_m/k_n}(\mathcal{C}l'_{k_n}) = 0$ for all $m \gg n$ (capitulation of $\mathcal{C}l'_{k_n}$ in k_∞ for all $n \geq 0$);

(v) $(X_\infty)_\Gamma$ capitulates asymptotically;

(v′) $(X'_\infty)_\Gamma$ capitulates asymptotically;

(vi) $\widetilde{\mathcal{C}}l_k$ capitulates in k_∞, or $\widetilde{\mathcal{C}}l_k^{[p]}$ and $\mathcal{C}l'_k$ capitulate in k_∞;

In our opinion, these aesthetic statements are translations of standard formalism of class field theory in terms of the algebraic tools of Iwasawa's theory; they do not take into account what is needed (in a "numerical" setting) to "construct" the class groups at each stage of the tower. In the next section we will show how does this construction work and study its arithmetic complexity which becomes oversized as soon as $\lambda + \mu \neq 0$ (cf. Corollary 3.5). Moreover, we shall see in Section 4 that the algorithm depends rather weakly of the stage k_n, at least for n large enough.

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

3.1. **General algorithm – 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" in a cyclic p-extension, one uses the filtration of $M_n := \mathcal{C}\ell_{k_n}$:

$$M_n^i = c\ell_{k_n}(\mathcal{I}_n^i),\ \mathcal{I}_n^i \subset I_{k_n},\ i \geq 0,$$

defined inductively as follows (from [6, Corollary 3.7]) [2]:

Definition 3.1. *For $n \geq 1$ 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 $0 \leq i \leq m_n - 1$, where $G_n := \mathrm{Gal}(k_n/k) =: \langle \sigma_n \rangle$ and where m_n is the least integer i such that $M_n^i = M_n$ (i.e., such that $M_n^{i+1} = M_n^i$).*

We then have:

Proposition 3.2. *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 of the $\#(M_n^{i+1}/M_n^i)$, $0 \leq i \leq m_n$, is decreasing to 1 and has the upper bound $\#M_n^1$ because of the sequence of injective maps: $M_n^{i+1}/M_n^i \hookrightarrow M_n^i/M_n^{i-1} \hookrightarrow \cdots \hookrightarrow M_n^2/M_n^1 \hookrightarrow M_n^1$ defined from the action of $1-\sigma_n$.

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

Recall that for $n \geq 1$ fixed, a generalization of the Chevalley ambiguous class number formula [6, Formula (29), § 3.2], leads, by means of the norm groups $\mathrm{N}_{k_n/k}(M_n^i)$ and the groups of numbers:

$$\Lambda_n^i := \{x \in k^\times,\ (x) \in \mathrm{N}_{k_n/k}(\mathcal{I}_n^i)\},$$

to the i-sequence: $\#\big(M_n^{i+1}/M_n^i\big) = \frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_n^i)} \cdot \frac{p^{n\cdot(r_p-1)}}{(\Lambda_n^i : \Lambda_n^i \cap \mathrm{N}_{k_n/k}(k_n^\times))}$, where the integers:

$$\frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_n^i)} \quad \& \quad \frac{p^{n\cdot(r_p-1)}}{(\Lambda_n^i : \Lambda_n^i \cap \mathrm{N}_{k_n/k}(k_n^\times))} \tag{4}$$

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 $\mathcal{I}_n^i$ 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 $\mathcal{I}_n^i$ are built inductively from $\mathcal{I}_n^0 = 1$, then $\Lambda_n^0 = E_k$ [7, § 6.2].

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

Theorem 3.3. *(i) The class factors $\frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_n^i)}$ 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 $\frac{p^{n\cdot(r_p-1)}}{(\Lambda_n^i : \Lambda_n^i \cap \mathrm{N}_{k_n/k}(k_n^\times))}$ 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 $\frac{p^{n\cdot(r_p-1)}}{(E_k : E_k \cap \mathrm{N}_{k_n/k}(k_n^\times))}$.

[2] In some former papers this filtration is considered for cyclic extensions of prime degree p; the generalization to arbitrary cyclic extensions was given in [3], then translated into english in [6] with improvements. So it applies in the k_n/k.

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

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

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

Therefore, for $i=m_n$, using the above formula (4), we obtain $M_n^{m_n}=\mathcal{C}\ell_{k_n}$, $\mathrm{N}_{k_n/k}\big(M_n^{m_n}\big)=\mathcal{C}\ell_k$ and $(\Lambda_n^{m_n} : \Lambda_n^{m_n}\cap \mathrm{N}_{k_n/k}(k_n^\times))=p^{n\cdot(r_p-1)}$, 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 $\mathcal{R}_k^{\mathrm{nr}}:=\mathrm{Gal}(H_k^{\mathrm{gen}}/k_\infty H_k)$ (Diagram 2.7 in § 2.3), where H_k^{gen} is the union of the genus class fields $H_{k_m/k}$ (Proposition 2.6). 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 m_n be the length of the algorithm. Then:

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

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

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

Proof. Consider $M_n:=\mathcal{C}\ell_{k_n}$. As $\#\big(M_n^{i+1}/M_n^i\big)\geq p$ for $0\leq i\leq m_n-1$, the Proposition (3.2) (iv) implies $\#\mathcal{C}\ell_{k_n}=\#M_n^{m_n}\geq p^{m_n}$; whence $m_n\leq\lambda\cdot n+\mu\cdot p^n+\nu$; then, from the fact that $\#\big(M_n^{i+1}/M_n^i\big)\mid\#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\mathrm{nr}}$, (Theorem 3.3) this yields $\#\big(M_n^{i+1}/M_n^i\big)\leq\#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\mathrm{nr}}$ for $0\leq i\leq m_n-1$; whence $\#\mathcal{C}\ell_{k_n}\leq(\#\mathcal{C}\ell_k\cdot\#\mathcal{R}_k^{\mathrm{nr}})^{m_n}$ from Proposition (3.2) (iv), which completes the proof of (i). Point (ii) is equivalent to $\mathcal{G}_{k_n/k}=1$, whence $\mathcal{C}\ell_{k_n}=1$ and (iii) is immediate. □

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

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

We know also that taking, as base field, a stage $k_{n_0}\subset k_\infty$, large enough, one may expect (from Theorem 2.11 (i′)) that the algorithm in k_n/k_{n_0} gives $m_n^{n_0}=1$, that is to say $\mathcal{C}\ell_{k_n}^{G_n^{n_0}}=\mathcal{C}\ell_{k_n}$, of order p^ν, for all $n\geq n_0$.

Example 3.6. The integer n_0 is not effective and in general $n_0>0$ as shown by the following PARI/GP [27] program for real quadratic fields k and $p=2$. The program computes the structure of $\mathcal{C}\ell_{k_n}$ for $n\in[0,4]$; if $k=\mathbb{Q}(\sqrt{2\,m'})$, with $m'\equiv 1 \pmod 4$, the first stage k_1 is contained in the Hilbert class field of k, which gives an exception to the surjectivity $\mathcal{C}\ell_{k_n}\to\mathcal{C}\ell_k$, $n\geq 1$, of the norm and explains that in this case one must take k_1 as base field.

Then we give some excerpts which only suggest a rapid stabilization:

```
{for(m=2,10^3,if(core(m)!=m,next);P0=x^2-m;
P1=polcompositum(P0,x^2-2)[1];
P2=polcompositum(P0,(x^2-2)^2-2)[1];
P3=polcompositum(P0,((x^2-2)^2-2)^2-2)[1];
P4=polcompositum(P0,(((x^2-2)^2-2)^2-2)^2-2)[1];
K0=bnfinit(P0,1);H0=K0.cyc;K1=bnfinit(P1,1);H1=K1.cyc;
K2=bnfinit(P2,1);H2=K2.cyc;K3=bnfinit(P3,1);H3=K3.cyc;
K4=bnfinit(P4,1);H4=K4.cyc;
print("m=",m," ",H0," ",H1," ",H2," ",H3," ",H4))}
```

```
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 $\widetilde{\mathcal{C}\ell}_k \simeq \mathcal{C}\ell'_k$ which is here such that $\mathcal{C}\ell_k = \mathcal{C}\ell'_k \oplus \mathbb{Z}/2\mathbb{Z}$.

Remarks 3.7. (i) Thus, Greenberg's conjecture reduces to an estimation of the number m_n of steps of the algorithm. But m_n (n fixed) depends of the i-progression of the class and norm factors (4) 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 $\mathcal{R}_k^{\rm nr}$).
(ii) We observe the huge discontinuity between the cases $\#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\rm nr} = 1$ (giving $\lambda = \mu = \nu = 0$) and $\#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\rm nr} \neq 1$ with $\lambda + \mu \neq 0$ (giving $m_n \to \infty$ with n).
(iii) But the most spectacular argument is that, for n large enough, assuming to simplify that $n_0 = 0$, one must find, in practice, $m_n = 1$ from Theorem 2.11 (i$'$) giving, for $n \gg 0$, $\mathcal{C}\ell_{k_n}^{G_n} = \mathcal{C}\ell_{k_n}$ of order p^ν as the numerical experiments show.

See comments on the complexity of the algorithm in [10, § 6]. These observations are strengthened by the results of [19] which show, in a particular case, that it is quite possible to obtain density results and some proofs "with probability 1".

3.2. **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 we consider the n-sequences $M_n^i := \mathcal{C}\ell_{k_n}^i$, for $n \to \infty$. We study the n-sequence of integers:

$$\#\big(M_n^{i+1}/M_n^i\big) := \#\big(M_n/M_n^i\big)^{G_n},$$

where $G_n := {\rm Gal}(k_n/k)$, from their class and norm factors (4), knowing that $M_n := \mathcal{C}\ell_{k_n}$ is obtained for $i = m_n$.
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 that on M_{n+1}^i (they may be a priori not injective nor surjective):

Diagram 3.8.

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

We have $\mathrm{N}_{k_{n+1}/k_n}(M_{n+1}^i) \subseteq M_n^i$; thus, for all $\mathfrak{A}_{n+1} \in \mathcal{I}_{n+1}^i$:

$$\mathrm{N}_{k_{n+1}/k_n}(\mathfrak{A}_{n+1}) = (\alpha_n)\,\mathfrak{A}_n, \text{ where } \alpha_n \in k_n^\times \text{ and } \mathfrak{A}_n \in \mathcal{I}_n^i,$$

in what case, *modifying* $\mathcal{I}_n^i$ modulo suitable principal ideals, one gets:

$$\mathrm{N}_{k_{n+1}/k_n}(\mathcal{I}_{n+1}^i) \subseteq \mathcal{I}_n^i, \text{ whence } \mathrm{N}_{k_{n+1}/k}(\mathcal{I}_{n+1}^i) \subseteq \mathrm{N}_{k_n/k}(\mathcal{I}_n^i);$$

this reduces to modify the sets $\Lambda_n^i = \{x \in k^\times, (x) \in \mathrm{N}_{k_n/k}(\mathcal{I}_n^i)\}$ modulo global norms of elements of $k_n^\times$ leaving invariant $(\Lambda_n^i : \Lambda_n^i \cap \mathrm{N}_{k_n/k}(k_n^\times))$.

So, one may suppose that, for all given $h \geq 1$:

$$\Lambda_{n+h}^i \subseteq \cdots \subseteq \Lambda_{n+1}^i \subseteq \Lambda_n^i. \tag{5}$$

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 $\mathfrak{t}(\mathfrak{a})$ whose Artin symbol is in $\mathcal{T}_k$.

Proposition 3.9. *For all $i \geq 0$ fixed, the integers $\#\big(M_n^{i+1}/M_n^i\big)$ define an increasing stationary n-sequence of divisors of $\#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\mathrm{nr}}$, and the integers $\#M_n^i$ define an increasing stationary n-sequence.*

Proof. As $\mathrm{N}_{k_{n+1}/k}(M_{n+1}^i) \subseteq \mathrm{N}_{k_n/k}(M_n^i)$, the class factors $\frac{\#\mathcal{C}\ell_k}{\#\mathrm{N}_{k_n/k}(M_n^i)}$ 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 $\frac{p^{n\cdot(r_p-1)}}{\#\omega_n(\Lambda_n^i)} =: p^{\rho_n^i}$ (see § 2.2) and $p^{\rho_{n+1}^i - \rho_n^i} = p^{r_p-1}\,\frac{\#\omega_n(\Lambda_n^i)}{\#\omega_{n+1}(\Lambda_{n+1}^i)}$; since by (5) 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 $p^{\rho_{n+1}^i - \rho_n^i} \geq p^{r_p-1}\,\frac{\#\omega_n(\Lambda_n^i)}{\#\omega_{n+1}(\Lambda_n^i)}$; in the restriction $\Omega(k_{n+1}/k) \twoheadrightarrow \Omega(k_n/k)$ of Hasse's symbols (with kernel isomorphic to $\mathbb{F}_p^{r_p-1}$), the image of $\omega_{n+1}(\Lambda_n^i)$ is $\omega_n(\Lambda_n^i)$, whence an increasing n-sequence $p^{\rho_n^i} \mid \#\mathcal{R}_k^{\mathrm{nr}}$. Thus:

$$\lim_{n\to\infty} \#\big(M_n^{i+1}/M_n^i\big) = p^{c^i} \cdot p^{\rho^i} \mid \#\mathcal{C}\ell_k \cdot \#\mathcal{R}_k^{\mathrm{nr}}.$$

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

Proposition 3.10. *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 $c_n^i = c^i$ and $\rho_n^i = \rho^i$), we have $\frac{\#\mathrm{N}_{k_n/k}(M_n^i)}{\#\mathrm{N}_{k_n/k}(M_n^{i+1})} \leq 1$ and $\frac{\#\omega_n(\Lambda_n^i)}{\#\omega_n(\Lambda_n^{i+1})} \leq 1$ since $\Lambda_n^i \cdot \mathrm{N}_{k_n/k}(k_n^\times) \subseteq \Lambda_n^{i+1} \cdot \mathrm{N}_{k_n/k}(k_n^\times)$. □

Corollary 3.11. *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 $c = \rho = 0$.*

Remark 3.12. From Theorem 2.11 (i′), under Greenberg's conjecture, the previous results should be, for all n large enough:

$$M_n^i = M_n^1,\ c^i = \rho^i = 0,\ \text{for all } i \geq 1, \text{ thus } m_n = 1,\ c = \rho = 0.$$

Unfortunately, numerical examples need to take n large enough, which is not effective.

We refer to [7, 10] for complements, conjectures and numerical experiments; in particular, for $x \in \Lambda_n^i$ we then have $(x) = \mathrm{N}_{k_n/k}(\mathfrak{A})$, $\mathfrak{A} \in \mathcal{I}_n^i$, 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 [10, § 6.1]) from the equality $(x) = \mathrm{N}_{k_n/k}(y_n) = \mathrm{N}_{k_n/k}(\mathfrak{A})$, giving the existence of $\mathfrak{B}$ (having, a priori, no algebraic link with the previous data), such that:

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

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.

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

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

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

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

Since any ideal class can be represented by a prime to p ideal, we assume that $\mathfrak{A} \in \mathcal{I}_n^i$ is taken in the group I'_{k_n} of prime to p ideals of k_n. We have seen that the ideals $\mathfrak{A} \in \mathcal{I}_n^i$ may be arbitrarily modified modulo principal ideals of k_n, whence $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$ defined up to $\mathrm{N}_{k_n/k}(k_n^\times)$ 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.

4.1. Decomposition of $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$ − The fundamental ideals $\mathfrak{t}(\mathfrak{a})$.

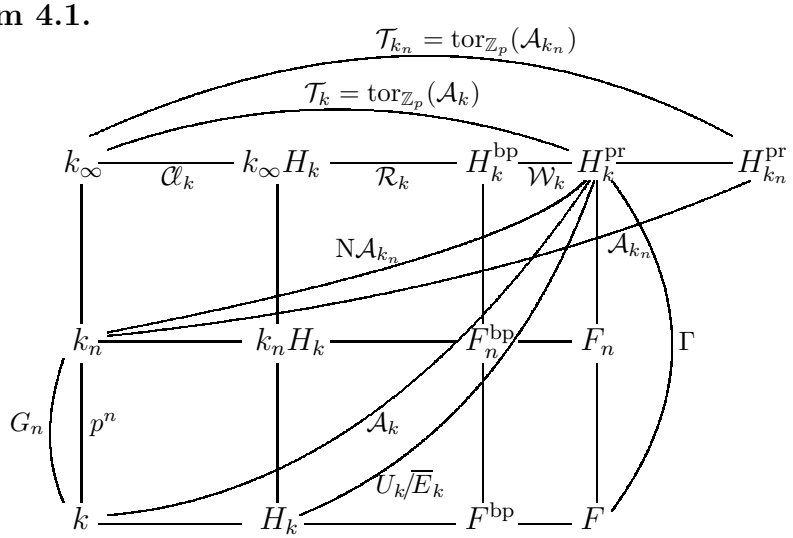
Let H_k^{pr} and $H_{k_n}^{\mathrm{pr}}$ be the maximal abelian p-ramified pro-p-extensions of k and k_n, respectively. Let F be an extension of H_k such that H_k^{pr} be the direct compositum of F and $k_\infty H_k$ over H_k (which is possible because $k_\infty \cap H_k = k$); we put $\Gamma = \mathrm{Gal}(H_k^{\mathrm{pr}}/F) \simeq \mathbb{Z}_p$.

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., [4, Theorem III.2.4, Proposition III.2.4.1] and [14, Chap. 1, § (d)]).

The action of the arithmetic norm in k_n/k is given by the following diagram; in particular:

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

Diagram 4.1.



The link between ideal norms in the stage 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 in k_n for n large enough (but relative to the choice of F, whence of Γ; in Theorem 4.5 we will prove that this link is independent of the decomposition of $\mathcal{A}_k = \Gamma \oplus \mathcal{T}_k$):

Theorem 4.2. *Let $\mathfrak{A} \in I'_{k_n}$ (ordinary ideal seen in $I'_{k_n} \otimes \mathbb{Z}_p$).*
(i) There exist unique ideals $\mathfrak{c}, \mathfrak{t} \in I'_k \otimes \mathbb{Z}_p$ and $(x_\infty) \in \mathcal{P}_{k,\infty}$, such that:

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

(ii) There exist some $\alpha_n \in k^\times \otimes \mathbb{Z}_p$ such that $\mathrm{N}_{k_n/k}(\mathfrak{A}\,(\alpha_n)) = \mathfrak{t} \pmod{\mathcal{P}_{k,\infty}}$, with $\iota \mathrm{N}_{k_n/k}(\alpha_n) = \iota(\alpha_n^{p^n})$ arbitrarily close to 1 in U_k regarding $n \gg 0$.

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 $\mathrm{N}_{k_n/k}(\mathcal{A}_{k_n}) = \mathrm{Gal}(H_k^{\mathrm{pr}}/H_k^{\mathrm{pr}} \cap k_n) = \mathrm{Gal}(H_k^{\mathrm{pr}}/k_n)$. It follows that $\mathrm{N}_{k_n/k}(\mathfrak{A})$ is of the required form for a given subgroup Γ.
(ii) Let $N \geq n$; from the total ramification of p in k_N/k, $\mathcal{C}\ell_k = \mathrm{N}_{k_N/k}(\mathcal{C}\ell_{k_N})$, and there exists $c_N \in k^\times \otimes \mathbb{Z}_p$ such that $\mathfrak{c} \cdot (c_N) = \mathrm{N}_{k_N/k}(\mathfrak{C}_N)$, $\mathfrak{C}_N \in I'_{k_N}$. The previous decomposition for the stage k_N yields:

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

with $\mathfrak{c}', \mathfrak{t}' \in I'_k \otimes \mathbb{Z}_p$; thus:

$$\mathrm{N}_{k_n/k}(\mathfrak{A}\,(c_N)) = (\mathfrak{c}\,(c_N))^{p^n} \cdot \mathfrak{t} \cdot (x_\infty) = \mathfrak{c}'^{p^{n+N}} \cdot \mathfrak{t}'^{p^n} \cdot \mathfrak{t} \pmod{\mathcal{P}_{k,\infty}}.$$

For p^n larger than the exponent p^e of $\mathcal{T}_k$ we get $\mathfrak{t}'^{p^n} \in \mathcal{P}_{k,\infty}$ and:

$$\mathrm{N}_{k_n/k}(\mathfrak{A}\,(c_N)) = (\gamma_N) \cdot \mathfrak{t} \pmod{\mathcal{P}_{k,\infty}},$$

with $\iota\gamma_N$ arbitrarily close to 1 in U_k regarding N; indeed, $\mathfrak{c}'^{p^n} =: (\gamma'_n)$ in $I'_k \otimes \mathbb{Z}_p$, thus $\gamma_N = \gamma_n'^{p^N}$ is of the form $\mathrm{N}_{k_n/k}(\gamma_n)$, $\gamma_n \in k^\times \otimes \mathbb{Z}_p$. Whence the claim taking $\alpha_n := c_N \cdot \gamma_n^{-1}$ since $\mathrm{N}_{k_n/k}(c_N \cdot \gamma_n^{-1}) = c_N^{p^n} \cdot \gamma_N^{-1}$ is close to 1 in U_k, but regarding n because of the factor $c_N^{p^n} \in (k^\times \otimes \mathbb{Z}_p)^{p^n}$. □

Definition 4.3. *We shall call this unique ideal $\mathfrak{t}$ of finite order modulo $\mathcal{P}_{k,\infty}$ the fundamental ideal associated to the class $\mathrm{N}_{k_n/k}(\mathfrak{A})\mathrm{N}_{k_n/k}(k_n^\times \otimes \mathbb{Z}_p)$ of $\mathrm{N}_{k_n/k}(\mathfrak{A})$. We denote this representative $\mathfrak{t}(\mathfrak{a})$ where $\mathfrak{a} := \mathrm{N}_{k_n/k}(\mathfrak{A}) \pmod{\mathrm{N}_{k_n/k}(k_n^\times \otimes \mathbb{Z}_p)}$.*

We remark that this representative $\mathfrak{t}(\mathfrak{a})$ belongs to $\mathfrak{a} \cdot (k^\times \otimes \mathbb{Z}_p)^{p^n}$.

4.2. **Images of the ideals $\mathfrak{t}(\mathfrak{a})$ in $\mathcal{C}\ell_k$ and $\mathcal{R}_k$.** The ideals $\mathfrak{a} := \mathrm{N}_{k_n/k}(\mathfrak{A})$ play two different roles, in the evolution of the class factors (via the class of $\mathfrak{a}$) and in that of the norm factors (via principal $\mathfrak{a}$), which will be stated in terms of ideals $\mathfrak{t}$ as follows:

4.2.1. *Class factors and ideals* $\mathfrak{t}$. The $\mathrm{N}_{k_n/k}(\mathcal{I}_n^i)$, 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 some $\mathfrak{t} \in I'_k \otimes \mathbb{Z}_p$, of finite order modulo $\mathcal{P}_{k,\infty}$, with $\mathscr{cl}_k(\mathfrak{t}) \in \mathrm{N}_{k_n/k}(M_n^i)$. Thus, a priori, $\mathscr{cl}_k(\mathfrak{t})$ runs through $\mathcal{C}\ell_k$.

4.2.2. *Norm factors and ideals* $\mathfrak{t}$. The $\Lambda_n^i = \{x \in k^\times, (x) \in \mathrm{N}_{k_n/k}(\mathcal{I}_n^i)\}$, defining the norm factors, are obtained via ideals (x) such that $(x)\,\mathrm{N}_{k_n/k}(\alpha_n)^{-1} = \mathfrak{t} \pmod{\mathcal{P}_{k,\infty}}$, $\alpha_n \in k_n^\times \otimes \mathbb{Z}_p$, where $\mathfrak{t}$ is principal 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 through $\mathcal{R}_k$.

4.2.3. *Definition of* $\log(\mathfrak{t}) \in \mathcal{R}_k$ *for* $\mathfrak{t}$ *principal.* Let $\mathfrak{t} = (\tau)$, $\tau \in k^\times \otimes \mathbb{Z}_p$, be a principal fundamental ideal (of finite order modulo $\mathcal{P}_{k,\infty}$). 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 $U_k^*/\overline{E}_k$.

Then we consider the image of $\log(\iota\tau)$ in $\log(U_k^*)/\log(\overline{E}_k) = \mathcal{R}_k$, which defines the element of $\mathcal{R}_k$:

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

Lemma 4.4. *Let $x \in k^\times \otimes \mathbb{Z}_p$, such that $(x) \in \mathrm{N}_{k_n/k}(\mathcal{I}_n^i)$. Then x is local norm at p in k_n/k (whence global norm) if and only if any representative of x modulo $W_k = \bigoplus_{\mathfrak{p}\mid p} \mu_p(k_\mathfrak{p})$ 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 exact sequence (3) and Lemma 4.4, 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:

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

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

4.2.4. *Conclusion about the role of the fundamental ideals.* It is immediate to see that, using suitable representatives of ideals $\mathfrak{A} \in \mathcal{I}_n^i$ in k_n (from Theorem 4.2), the filtration $M_n^i =: \mathscr{cl}_{k_n/k}(\mathcal{I}_n^i)$ may be such that $\mathrm{N}_{k_n/k}(\mathcal{I}_n^i) = \langle \mathfrak{t}_{i,j} \rangle_j$, generated by fundamental ideals, and $\Lambda_n^i = \{\tau \in k^\times \otimes \mathbb{Z}_p,\ (\tau) \in \langle \mathfrak{t}_{i,j} \rangle_j\}$ in which one finds the $\tau = \mathrm{N}_{k_n/k}(y_n)$, $y_n \in k_n^\times \otimes \mathbb{Z}_p$.

So the algorithm continues with the evolution relation:

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

The main consequence being that *the fundamental ideals* $\mathfrak{t}$ *are finite in number* (modulo $\mathcal{P}_{k,\infty}$).

Assuming that the ideals $\mathfrak{A}$ of k_n are random as well as the norms $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$, this suggests that the $\mathfrak{t}(\mathfrak{a})$ are random. In other words, both $cl_k(\mathfrak{t}(\mathfrak{a}))$ and $\log(\mathfrak{t}(\mathfrak{a}))$ (when $\mathfrak{t}(\mathfrak{a})$ is principal) are random in $\mathcal{C}l_k$ 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 $\mathcal{C}l_k$.

(ii) When $\mathfrak{t}(\mathfrak{a}) = (\tau)$, the image $\log(\mathfrak{t}(\mathfrak{a})) = \log(\iota\tau) \pmod{\log(\overline{E}_k)}$, 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 Greenberg's conjecture.

4.3. **Galois descent of $\mathcal{T}_k$.** The Galois descent of $H_k^{\mathrm{pr}}/k_\infty$, by means of F/k (Diagram 4.1), provides, in a numerical context (see an example in [10, § 8.1]), the repartition of the Artin symbols $\left(\frac{F/k}{\mathfrak{a}}\right)$, for $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$ or for the ideals $\mathfrak{t}(\mathfrak{a})$. The field F (more precisely F^{bp}) is, in some sense, a "governing field" for Greenberg's conjecture. This is enforced according to the essential following result:

Theorem 4.5. *The ideal* $\mathfrak{t}(\mathfrak{a})$*, deduced from the class of the ideal* $\mathfrak{a} = \mathrm{N}_{k_n/k}(\mathfrak{A})$ *modulo* $\mathrm{N}_{k_n/k}(k_n^\times \otimes \mathbb{Z}_p)$*, does not depend (modulo* $\mathcal{P}_{k,\infty}$*) on the choice of* F*.*

Proof. Let F'/k be another solution; then, referring to suitable expressions of Theorem 4.2 (ii), we get, modulo $\mathcal{P}_{k,\infty}$, with obvious notations for F and F':

$$\mathrm{N}_{k_n/k}(\mathfrak{A}) = (u)\,\mathfrak{t}, \quad \mathrm{N}_{k_n/k}(\mathfrak{A}) = (u')\,\mathfrak{t}' \pmod{\mathcal{P}_{k,\infty}}, \quad u, u' \in k^\times \otimes \mathbb{Z}_p,$$

ιu, $\iota u'$ arbitrary close to 1 regarding n; whence $\mathfrak{t}'\,\mathfrak{t}^{-1} = (a)$ with ιa close to 1.

So, $(a)^{p^e} = (a_\infty) \in \mathcal{P}_{k,\infty}$, 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 $\varepsilon = \eta^{p^e}$ 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, both ιa and $\iota\eta$ are close to 1 in U_k, thus $\xi = 1$ and $a\,\eta^{-1} = a'_\infty$ giving $\mathfrak{t}'\,\mathfrak{t}^{-1} = (a'_\infty)$. □

References

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

[2] 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/

[3] Gras, G.: Classes généralisées invariantes. J. Math. Soc. Japan **46**(3) (1994), 467–476. https://projecteuclid.org/download/pdf_1/euclid.jmsj/1227104692

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

[5] Gras, G.: 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: https://arxiv.org/pdf/1701.02618

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

[7] Gras, G.: 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
[8] 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
[9] Gras, G.: Annihilation of $\mathrm{tor}_{\mathbb{Z}_p}(\mathcal{G}_{K,S}^{\mathrm{ab}})$ for real abelian extensions $K/\mathbb{Q}$, Comm. in Advanced Mathematical Sciences, **1**(1) (2018), 5–34. https://doi.org/10.33434/cams.441035
[10] Gras, G.: 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
[11] Gras, G.: Practice of the Incomplete p-Ramification Over a Number Field – History of Abelian p-Ramification. Comm. in Advanced Mathematical Sciences **2**(4) (2019), 251–280. https://doi.org/10.33434/cams.573729
[12] Gras, G.: 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
[13] Greenberg, R.: On the Iwasawa invariants of totally real number fields. Amer. J. Math. **98**(1) (1976), 263–284. https://doi.org/10.2307/2373625
[14] 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
[15] 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/
[16] Jaulent, J-F.: Note sur la conjecture de Greenberg. J. Ramanujan Math. Soc. **34** (2019) 59–80. https://www.math.u-bordeaux.fr/~jjaulent/
[17] Jaulent, J-F.: Normes universelles et conjecture de Greenberg. Acta Arithmetica **194** (2020), 99–109. https://www.math.u-bordeaux.fr/~jjaulent/
[18] Jaulent, J-F.: Annulateurs circulaires et conjecture de Greenberg (preprint 2020). https://www.math.u-bordeaux.fr/~jjaulent
[19] 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
[20] Nguyen Quang Do, T.: 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
[21] 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. https://doi.org/10.1142/S1793042106000395
[22] 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
[23] Nguyen Quang Do, T.: 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
[24] Nguyen Quang Do, T. and Nicolas, V.: Nombres de Weil, sommes de Gauss et annulateurs galoisiens, Amer. J. Math. **133** (2011), 1533–1571. https://muse.jhu.edu/article/458549
[25] Ozaki, M.: The class group of $\mathbb{Z}_p$-extensions over totally real number fields. Tohoku Math. J. **49** (1997), 431-435. https://doi.org/10.2748/tmj/1178225114
[26] Ozaki, M. and Taya, H.: A note on Greenberg's conjecture for real abelian number fields. Manuscripta Math. **88**(1) (1995), 311–320. https://doi.org/10.1007/BF02567825
[27] The PARI Group: PARI/GP version `2.9.0`. Université de Bordeaux (2016). http://pari.math.u-bordeaux.fr/.
[28] Taya, H.: 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
[29] 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