WEBER'S CLASS NUMBER PROBLEM AND p–RATIONALITY IN THE CYCLOTOMIC $\widehat{\mathbb{Z}}$–EXTENSION OF $\mathbb{Q}$

GEORGES GRAS

ABSTRACT. Let K be the Nth layer in the cyclotomic $\widehat{\mathbb{Z}}$-extension $\widehat{\mathbb{Q}}$. Many authors (Aoki, Fukuda, Horie, Ichimura, Inatomi, Komatsu, Miller, Morisawa, Nakajima, Okazaki, Washington, ...) analyse the behavior of the p-class groups $\mathscr{C}_K$. We revisit this problem, in a more conceptual form, since computations show that the p-torsion group $\mathscr{T}_K$ of the Galois groups of the maximal abelian p-ramified pro-p-extension of K (Tate–Shafarevich group of K) is often non-trivial; this raises questions since $\#\mathscr{T}_K = \#\mathscr{C}_K\,\#\mathscr{R}_K$ where $\mathscr{R}_K$ is the normalized p-adic regulator. We give a new method testing $\mathscr{T}_K \neq 1$ (Theorem 4.6, Table 6.2) and characterize the p-extensions F of K in $\widehat{\mathbb{Q}}$ with $\mathscr{C}_F \neq 1$ (Theorem 7.5 and Corollary 7.6). We publish easy to use programs, justifying again the eight known examples, and allowing further extensive computations.

CONTENTS

Date: November 5, 2020.
2020 *Mathematics Subject Classification.* 11R29, 11R37, 11Y40.
Key words and phrases. p-class groups, cyclotomic $\mathbb{Z}_\ell$-extensions, class field theory, p-adic regulators, p-ramification theory, PARI/GP programs.

1. Introduction

Let $\ell \geq 2$ be a prime number and let $\mathbb{Q}(\ell^n)$, $n \geq 0$, be the nth layer of the cyclotomic $\mathbb{Z}_\ell$-extension $\mathbb{Q}(\ell^\infty)$ of $\mathbb{Q}$ (with $[\mathbb{Q}(\ell^n) : \mathbb{Q}] = \ell^n$). We draw attention on the fact that we use ℓ (instead of p in the literature) since we need to apply the p-ramification theory to the fields $\mathbb{Q}(\ell^n)$, $p \neq \ell$, which is more convenient for our presentation and bibliographic references. The purpose of our study is to see in what circumstances the p-class group of $\mathbb{Q}(\ell^n)$ (then of any composite $\mathbb{Q}(N)$ of such fields) is likely to be non-trivial.

Indeed, one may ask if the arithmetic of these fields is as smooth as it is conjectured (for the class group $\mathscr{C}_{\mathbb{Q}(N)}$) by many authors after many verifications and partial proofs [2, 5, 10, 11, 12, 13, 14, 15, 34, 35, 36, 37, 38, 39, 40, 46, 47, 48, 49, 50, 51, 52, 59]. The triviality of $\mathscr{C}_{\mathbb{Q}(\ell^n)}$ has, so far, no counterexamples as ℓ, n, p vary, but that of the Tate–Shafarevich group $\mathscr{T}_{\mathbb{Q}(\ell^n)}$ (or more generally $\mathscr{T}_{\mathbb{Q}(N)}$) is, on the contrary, not true as we shall see numerically, and, for composite N, few $\mathscr{C}_{\mathbb{Q}(N)} \neq 1$ have been discovered.

1.1. History of the main progress and results.

The computation of the class number have been done in few cases because of limitation of the order of magnitude of the degree N and of p; for instance, the results given in [46, 47, Tables 1, 2] only concern $\ell^n = 2^7$, 3^4, 5^2, 11, 13, 17, 19, 23, 29, 31 (2^7, 3^4, 29, 31 under GRH). From PARI/GP [56], in a straightforward use, any computation needs the instruction bnfinit(P) (giving all the basic invariants of the field K defined via the polynomial P, whence the class group, a system of units, etc.); thus, by this way, few values of N may be carried out.

Approaches, by means of geometry of numbers, prove that some of these fields are euclidean (see, e.g., [6] about $\mathbb{Q}(2^2)$, $\mathbb{Q}(2^3)$); but this more difficult and broad aspect, needs other techniques and is hopeless for our goal.

Then some deep analytic studies of the class number were done by many authors (Aoki, Fukuda, Horie, Ichimura, Inatomi, Komatsu, Miller, Morisawa, Nakajima, Okazaki, Washington...) proving infinitely many cases of p-principality, high enough in the towers. New PARI functions, for abelian arithmetic, may be available (see [16] for more information) and deal with classical analytic formulas (cyclotomic units, Bernoulli numbers, etc.).

1.2. Method and main results.

Let K be any real abelian number field and let $\mathscr{T}_K$ be the torsion group of $\mathscr{G}_K := \mathrm{Gal}(H_K^{\mathrm{pr}}/K)$, where H_K^{pr} is the maximal abelian p-ramified (i.e., unramified outside p and ∞) pro-p-extension of K; this group is essentially the so-called Tate–Shafarevich group. The new aspects of our method is the use of p-adic measures which are more naturally attached to $\mathscr{T}_K$ or to the Jaulent logarithmic class groups $\widetilde{\mathscr{C}}_K$ related to Greenberg's conjecture.

Curiously, the computation of $\mathscr{T}_K$ is easier than that of $\mathscr{C}_K$ or of the normalized p-adic regulator $\mathscr{R}_K$, separately.

Let $\widehat{\mathbb{Q}}$ be the composite of the cyclotomic $\mathbb{Z}_\ell$-extensions of $\mathbb{Q}$. For $K = \mathbb{Q}(\ell^n)$, or more generally, for the subfields $\mathbb{Q}(\ell_1^{n_1}) \cdots \mathbb{Q}(\ell_t^{n_t}) \in \widehat{\mathbb{Q}}$, (denoted $\mathbb{Q}(N)$ where $N := \ell_1^{n_1} \cdots \ell_t^{n_t}$), we have the identity:

$$\#\mathscr{T}_K = \#\mathscr{C}_K \cdot \#\mathscr{R}_K \cdot \#\mathscr{W}_K,$$

where $\mathscr{C}_K$ is the p-class group, $\mathscr{R}_K$ the normalized p-adic regulator, $\mathscr{W}_K = 1$ for $p > 2$ and $\mathscr{W}_K \simeq \mathbb{F}_2^{\#S-1}$ for $p = 2$, where $S := \{\mathfrak{p},\ \mathfrak{p} \mid 2 \text{ in } K\}$ (Lemma 2.1). Since Leopoldt's conjecture holds in abelian fields, we have, for any prime p, $\mathscr{G}_K = \Gamma_K \oplus \mathscr{T}_K$ with $\Gamma_K \simeq \mathbb{Z}_p$.

So, as soon as $\mathscr{T}_K = 1$ (i.e., K is called p-rational), we are certain that $\mathscr{C}_K = 1$; otherwise, we may suspect a possible counterexample. We shall first compute § 2.5 the structure of some $\mathscr{T}_K$ by means of an indisputable reference program (but using bnfinit(P)) to show that this p-torsion group is non-trivial in many cases. The good new is that there exists a test for $\mathscr{T}_K \neq 1$ which does not need bnfinit(P) and allows large K and p, so that our programs are very elementary and written with basic instructions giving simpler faster computations in larger intervals; it will be explained Sections 3, 4, and yields Theorem 4.6 and Table 6.2.

Finally, we give programs to search non-trivial p-class groups using Chevalley's formula in p-extensions of K in $\widehat{\mathbb{Q}}$, in connection with a deep property of the p-adic regulator $\mathscr{R}_K$, as product of the form $\mathscr{R}_K = \mathscr{R}_K^{\rm nr} \cdot \mathscr{R}_K^{\rm ram}$ (diagrams of § 7.2), in relationship with studies of Taya [58] on Greenberg's conjecture. We prove (Lemma 7.3) that, without restricting the generality, one may assume p totally split in K, then $\mathscr{R}_K^{\rm ram} = 1$ (Lemma 7.2) and (Lemma 7.4) that $\mathscr{R}_K \neq 1$ is equivalent to $\mathscr{C}_{K_m} \neq 1$ for $K_m := K\mathbb{Q}(p^m)$, m large enough, hence the following fundamental criterion (Theorem 7.5):

Main Theorem. *Let $\widehat{\mathbb{Q}}$ be the composite of all the cyclotomic $\mathbb{Z}_\ell$-extensions of $\mathbb{Q}$ and let $K = \mathbb{Q}(N) \subset \widehat{\mathbb{Q}}$. Let $p > 2$ be a prime, totally split in K. Then, $\mathscr{C}_{K\mathbb{Q}(p^m)} = 1$ for all $m \geq 0$, if and only if $\mathscr{T}_K = 1$ (i.e., K is p-rational). For $p = 2$, the condition becomes $\mathscr{T}_K = \mathscr{W}_K$ (i.e., $\#\mathscr{T}_K = 2^{N-1}$).*

Despite of the huge intervals tested, we only find again (see Corollary 7.6) known cases (Fukuda–Komatsu–Horie–Morisawa), but with programs that may be used by anyone on more powerful computers than ours. This suggests an extreme rarity of non-trivial class groups in $\widehat{\mathbb{Q}}$.

1.3. **The p-torsion groups $\mathscr{T}_K$ in number theory.** These invariants were less (numerically) computed than class groups, which is unfortunate because they are of basic significance in Galois cohomology since for all number fields K (under Leopoldt's conjecture), $\mathscr{T}_K$ is the dual of $\mathrm{H}^2(\mathscr{G}_K, \mathbb{Z}_p)$ [55], where $\mathscr{G}_K$ is the Galois group of the maximal p-ramified pro-p-extension of K (ordinary sense); the freeness of $\mathscr{G}_K$ is then equivalent to $\mathscr{T}_K = 1$. Then, after the pioneering works of Haberland–Koch–Neumann–Schmidt and others, we have the local-global principle defining first and second Tate–Shafarevich groups in the framework of S-ramification when S is the set of p-places of K [45, Theorem 3.74]:

$$Ш^i_K := \mathrm{Ker}\Big[\mathrm{H}^i(\mathscr{G}_K, \mathbb{F}_p) \longrightarrow \bigoplus_{v \in S} \mathrm{H}^i(\mathscr{G}_{K_v}, \mathbb{F}_p)\Big],\ i = 1, 2;$$

then $Ш^1_K \simeq \mathscr{C}_K / cl_K(S)$ (the S-class group), and $Ш^2_K$ closely depends on $V_K := \{\alpha \in K^\times,\ (\alpha) = \mathfrak{a}^p,\ \alpha \in K_v^{\times p},\ \forall v \in S\}$, via the exact sequence:

$$0 \to V_K/K^{\times p} \longrightarrow \mathrm{H}^2(\mathscr{G}_K, \mathbb{F}_p) \longrightarrow \bigoplus_{v \in S} \mathrm{H}^2(\mathscr{G}_{K_v}, \mathbb{F}_p) \longrightarrow \mathbb{Z}/p\mathbb{Z} \text{ (resp. } 0) \to 0,$$

if $\mu_p \subset K$ (resp. $\mu_p \not\subset K$). Finally, the link with the invariant $\mathscr{T}_K$ is given by the rank formula $\mathrm{rk}_p(\mathscr{T}_K) = \mathrm{rk}_p(V_K/K^{\times p}) + \sum_{v \in S} \delta_v - \delta_K$, where δ_v (resp. δ_K) is 1 or 0 according as K_v (resp. K) contains μ_p or not [17, Corollary III.4.2.3], thus giving for $K \subset \widehat{\mathbb{Q}}$ (real fields):

$$\mathrm{rk}_p(\mathscr{T}_K) = \mathrm{rk}_p(V_K/K^{\times p}) + \delta_{p,2}\,(\#S - 1),$$

with an exceptional term, only when $p = 2$. Thus, $\mathrm{rk}_p(\text{Ш}^2_K)$ is essentially $\mathrm{rk}_p(\mathscr{T}_K)$. For generalizations, with ramification and decomposition giving Shafarevich formula, see [17, II.5.4.1] as well as [41], and for the reflection theorem on generalized class groups, see [17, II.5.4.5 and Theorem III.4.2].

If one replaces the notion of p-ramification (in pro-p-extensions) by that of Σ-ramification (in pro-extensions), *for any set of places* Σ, the corresponding Tate–Shafarevich groups have some relations with the corresponding torsion groups $\mathscr{T}_{K,\Sigma}$, but with many open questions and interesting phenomena when no assumption is done (see, e.g., [32, 33] for an up to date story about them and for numerical examples).

When $\mathscr{T}_K = 1$ under Leopoldt's conjecture (freeness of $\mathscr{G}_K$), one speaks of p-rational field K; in this case, the Tate–Shafarevich groups are trivial or obvious, which has deep consequences as shown for instance in [3] in relation with our conjectures in [21] on the p-adic properties of the units. For more information on the story of abelian p-ramification and for that of p-rationality, see [28, Appendix A] and its bibliography about the pioneering contributions: K-theory approach [20], p-infinitesimal approach [41], cohomological/pro-p-group approach [53, 54]. All basic material about p-rationality is overviewed in [17, III.2, IV.3, IV.4.8].

The orders and annihilations of the $\mathscr{T}_K$ are given by p-adic L-functions "at $s = 1$", the two theories (arithmetic and analytic) being equivalent and given by suitable p-adic pseudo-measures (see Theorem 4.6).

All these principles on Tate–Shafarevich groups exist for the theory of elliptic curves and other contexts as the arithmetic of abelian varieties over the composite of $\mathbb{Z}_\ell$-extensions of a fixed number field F, the case of $\widehat{\mathbb{Q}}$ ($F = \mathbb{Q}$) being at the origin of a question of Coates [9, Section 3] on the possible triviality of the $C_{\mathbb{Q}(N)}$ in $\widehat{\mathbb{Q}}$, or at least of their extreme rarity. [1]

1.4. **The logarithmic class group and Greenberg's conjecture.** We shall also consider another p-adic invariant, the Jaulent's logarithmic class group $\widetilde{\mathscr{C}\ell}_K$ [42] which governs Greenberg's conjecture [30] for totally real number fields K (i.e., $\lambda = \mu = 0$ for the cyclotomic $\mathbb{Z}_p$-extension of K), the result being that Greenberg's conjecture holds if and only $\widetilde{\mathscr{C}\ell}_K$ capitulates in $K_\infty := K\mathbb{Q}(p^\infty)$ [43]. Of course Greenberg's conjecture holds for $p = \ell$ in $\mathbb{Q}(\ell^\infty)$ for trivial reasons, but we have few information for the cyclotomic $\mathbb{Z}_p$-extensions of $K = \mathbb{Q}(N) \subset \widehat{\mathbb{Q}}$. As we shall see, in all attempts concerning subfields of $\widehat{\mathbb{Q}}$, Jaulent's logarithmic class group was trivial (but the instruction $\mathsf{bnflog(P,p)}$ needs $\mathsf{bnfinit(P)}$ limiting the intervals). See § 7.4 for more numerical information. In particular, $\mathscr{C}_K = \mathscr{R}_K^{\mathrm{nr}} = 1$ implies $\lambda = \mu = \nu = 0$ [29, Theorem 5].

2. Abelian p-ramification theory

Recall the context of abelian p-ramification theory when K is any totally real number field (under Leopoldt's conjecture for p in K).

2.1. **Main definitions and notations.**

(*a*) Let E_K be the group of p-principal global units $\varepsilon \equiv 1 \,(\mathrm{mod}\ \prod_{\mathfrak{p}|p} \mathfrak{p})$ of K. Let $U_K := \oplus_{\mathfrak{p}|p} U_\mathfrak{p}$ be the $\mathbb{Z}_p$-module of p-principal local units, where $U_\mathfrak{p}$ is the group of $\mathfrak{p}$-principal units of the $\mathfrak{p}$-completion $K_\mathfrak{p}$ of K. Let μ_K (resp. $\mu_\mathfrak{p}$) be the group of pth roots of unity of K (resp. $K_\mathfrak{p}$).

(*b*) Let $\iota : \{x \in K^\times \otimes \mathbb{Z}_p,\ x \text{ prime to } p\} \to U_K$ be the diagonal embedding. Let $\overline{E}_K = \iota(E_K \otimes \mathbb{Z}_p)$ be the closure of ιE_K in U_K and let H_K^{nr} be the p-Hilbert class field of K;

[1] I warmly thank John Coates for sending me his conference paper (loc.cit.), not so easy to find for me, but which contains very useful numerical and bibliographical information.

then we have $\mathrm{Gal}(H_K^{\mathrm{pr}}/H_K^{\mathrm{nr}}) \simeq U_K/\overline{E}_K$. The Leopoldt conjecture leads to the (not so trivial) exact sequence:

$$1 \to \mathscr{W}_K \longrightarrow \mathrm{tor}_{\mathbb{Z}_p}\big(U_K/\overline{E}_K\big) \xrightarrow{\log} \mathrm{tor}_{\mathbb{Z}_p}\big(\log(U_K)/\log(\overline{E}_K)\big) \to 0,$$

where $\mathscr{W}_K := \mathrm{tor}_{\mathbb{Z}_p}(U_K)/\iota\mu_K = \big[\oplus_{\mathfrak{p}|p}\,\mu_{\mathfrak{p}}\big]/\iota\mu_K$.

(*c*) Let $\mathscr{C}_K \simeq \mathrm{Gal}(H_K^{\mathrm{nr}}/K)$ be the p-class group of K and let $\widetilde{\mathscr{C}}_K$ be the logarithmic class group, isomorphic to $\mathrm{Gal}(H_K^{\mathrm{lc}}/K_\infty)$, where $H_K^{\mathrm{lc}} \subseteq H_K^{\mathrm{pr}}$ is the maximal abelian locally cyclotomic pro-p-extension of K.

(*d*) Let $\mathscr{R}_K := \mathrm{tor}_{\mathbb{Z}_p}(\log(U_K)/\log(\overline{E}_K))$ be the normalized p-adic regulator [24, § 5]; recall that for $p \neq 2$, $\#\mathscr{R}_K = \frac{R_K}{p^{d-1}}$ and $\#\mathscr{R}_K = \frac{1}{2^{s_2-1}}\frac{R_K}{2^{d-1}}$ for $p = 2$, where R_K is the classical p-adic regulator, $d = [K:\mathbb{Q}]$ and s_2 is the number of 2-places in K (see [8, Appendix] giving the link of $\mathscr{R}_K$ with the residue of the p-adic zeta function of K).

(*e*) Let $K_\infty := K\mathbb{Q}(p^\infty)$ be the cyclotomic $\mathbb{Z}_p$-extension of K and let H_K^{bp} (called the Bertrandias–Payan field) fixed by the subgroup $\mathscr{W}_K$ of $\mathscr{T}_K$; the field H_K^{bp} is the composite of all p-cyclic extensions of K embeddable in p-cyclic extensions of arbitrary large degree.

2.2. **The case of the fields $K = \mathbb{Q}(N)$.** In that case, $K_\infty \cap H_K^{\mathrm{nr}} = K$ and $\mathscr{W}_K$ is given as follows:

Lemma 2.1. *One has $\mathscr{W}_K = 1$ for $K = \mathbb{Q}(N)$, except for $p = 2$ in which case, $\mathscr{W}_K \simeq \mathbb{F}_2^{\#S-1}$ where S is the set of primes $\mathfrak{p} \mid 2$ in K.*

Proof. For $p \neq 2$, $K_{\mathfrak{p}}$ does not contain μ_p since $\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p$, of degree $p-1 > 1$, is totally ramified and not contained in $\mathbb{Q}_p(p^\infty)$; thus $\mathscr{W}_K = 1$. For $p = 2$, $K_{\mathfrak{p}}$ does not contain μ_4 and $\mathrm{tor}_{\mathbb{Z}_p}(U_K) \simeq \mathbb{F}_2^{\#S}$, thus $\mathscr{W}_K \simeq \mathbb{F}_2^{\#S-1}$. □

The case $\#S > 1$ is very rare and occurs when $2^{\ell-1} \equiv 1 \pmod{\ell^2}$ for some $\ell \mid N$, e.g., $\ell = 2093,\ 3511$ which are out of range of practical computations. Thus $\mathscr{W}_K$ is in general trivial. If moreover $\mathscr{C}_K = 1$, $\mathscr{T}_K = \mathscr{R}_K$, which is not always trivial as we shall see, even if we have conjectured in [21] that, for any number field K, $\mathscr{T}_K = 1$ for $p \gg 0$.

2.3. **Fixed points formulas.** Let C_K be the whole class group of a number field K (in the restricted or ordinary sense, which will be specified with the mentions $^{\mathrm{res}}$ or $^{\mathrm{ord}}$).

Chevalley's formula [7, p. 406] for class groups C_K^{res} and C_k^{res}, in any cyclic extension K/k of number fields, of Galois group G, is given, in whole generality, by $\#(C_K^{\mathrm{res}})^G = \frac{\#C_k^{\mathrm{res}} \cdot \prod_{\mathfrak{l}} e_{\mathfrak{l}}}{[K:k]\cdot(E_k^{\mathrm{pos}} : E_k^{\mathrm{pos}} \cap \mathrm{N}_{K/k}(K^\times))}$, where $e_{\mathfrak{l}}$ is the ramification index in K/k of the prime ideal $\mathfrak{l}$ of k and E_k^{pos} is the group of totally positive units of k. When K/k is *totally ramified* at some prime ideal $\mathfrak{l}_0$, the formula becomes $\#(C_K^{\mathrm{res}})^G = \#C_k^{\mathrm{res}} \cdot \frac{\prod_{\mathfrak{l}\neq\mathfrak{l}_0} e_{\mathfrak{l}}}{(E_k^{\mathrm{pos}} : E_k^{\mathrm{pos}} \cap \mathrm{N}_{K/k}(K^\times))}$ (product of two integers).

Applied to $\mathbb{Q}(\ell^n)/\mathbb{Q}$ the formula gives $(C_{\mathbb{Q}(\ell^n)}^{\mathrm{res}})^G = 1$ since ℓ is the unique (totally) ramified prime and since $E_{\mathbb{Q}}^{\mathrm{pos}} = 1$. So, for $p = \ell$, $\mathscr{C}_{\mathbb{Q}(\ell^n)}^{\mathrm{res}} = 1$, a classical result. This fixed points formula is often attributed to Iwasawa (1956), Yokoi (1967) or others, instead of Chevalley (1933) (more precisely Herbrand–Chevalley, the "Herbrand quotient" of the group of units of K being the key for a general proof). The analogous "fixed points formula" for the *ℓ-torsion group* $\mathscr{T}_{\mathbb{Q}(\ell^n)}$, in $\mathbb{Q}(\ell^n)/\mathbb{Q}$ gives also $\mathscr{T}_{\mathbb{Q}(\ell^n)} = 1$ ([17, Theorem IV.3.3], [20, Proposition 6], [28, Appendix A.4.2]); which justifies once again the fact that the notation $\mathscr{T}$ always refers to a p-torsion group.

Nevertheless, Chevalley's formula is non-trivial in p-extensions K_m/K, $K_m := K\mathbb{Q}(p^m) \subset \widehat{\mathbb{Q}}$, as soon as p splits in part in K, and gives rare counterexamples (see Section 7).

2.4. **Galois action – Relative submodules.** Let p be a fixed prime. We recall some elementary principles for cyclic extensions of degree prime to p, to apply them to the fields $\mathbb{Q}(N)$, $p \nmid N$.

Let $K = \mathbb{Q}(N)$ and $k = \mathbb{Q}(N')$, $N'|N$. The transfer maps $\mathscr{T}_k \to \mathscr{T}_K$, $\mathscr{R}_k \to \mathscr{R}_K$, $\mathscr{C}_k \to \mathscr{C}_K$, are injective and the (arithmetic and algebraic) norms $\mathscr{T}_K \to \mathscr{T}_k$, $\mathscr{R}_K \to \mathscr{R}_k$, $\mathscr{C}_K \to \mathscr{C}_k$, are surjective since $p \nmid N$. More generally, let $(\mathscr{M}_{\mathbb{Q}(N)})_{N\geq 1}$ be a family of finite $\mathbb{Z}_p[G_N]$-modules, where $G_N = \mathrm{Gal}(\mathbb{Q}(N)/\mathbb{Q})$, provided with natural transfer and norm maps having the above properties when $N \not\equiv 0 \pmod p$ and let $\mathscr{M}^*_{\mathbb{Q}(N)}$ be the kernel of all the norms $\nu_{\mathbb{Q}(N)/\mathbb{Q}(N')}$, $N'|N$, $N' \neq N$, so that $\mathscr{M}_{\mathbb{Q}(N)} \simeq \big(\sum_{N'} \mathscr{M}_{\mathbb{Q}(N')}\big) \oplus \mathscr{M}^*_{\mathbb{Q}(N)}$.

Since G_N is cyclic of order N, the rational characters χ of K are in one-to-one correspondence with the fields $k \subseteq K$; we shall denote by $\theta \mid \chi$ the irreducible p-adic characters; each θ is above a character ψ of degree 1 and order a divisor of N.

We have $\mathscr{M}_K = \oplus_\chi \mathscr{M}_K^\chi = \oplus_\chi \mathscr{M}_k^* = \oplus_\chi \big[\oplus_{\theta|\chi} \mathscr{M}_k^\theta\big]$. Then $\mathscr{M}_K^*$ (or any of its component $\mathscr{M}_K^{\theta_N}$ for θ_N above ψ_N of order N) is a module over $\mathbb{Z}_p[\mu_N]$, hence isomorphic to a product of $\mathbb{Z}_p[\mu_N]$-modules of the form $\mathbb{Z}_p[\mu_N]/\mathfrak{p}_N^e$, for $\mathfrak{p}_N \mid p$ in $\mathbb{Q}_p(\mu_N)$, $e \geq 1$, whose p-rank is a multiple of the residue degree ρ_N of p in $\mathbb{Q}_p(\mu_N)/\mathbb{Q}_p$; thus $\rho_N \to \infty$ as $N \to \infty$, which is considered "incredible" for arithmetic invariants, as class groups, for totally real fields.

Indeed, interesting examples occur more easily when p totally splits in $\mathbb{Q}(\mu_N)$ (i.e., $p \equiv 1 \pmod N$) and this "explains" the result of [38] and [39] claiming that $\#C_{\mathbb{Q}(\ell^n)}$ is odd in $\mathbb{Q}(\ell^\infty)$ for all $\ell < 500$, that of [37, 51, 52] and explicit deep analytic computations in [5, 10, 11, 14, 36, 37, 38, 39, 48, 49, 51, 52, 59] (e.g., Washington's theorem [59] claiming that for ℓ and p fixed, $\#\mathscr{C}_K$ is constant for all n large enough, whence $\mathscr{C}_K^* = 1$ for all $n \gg 0$, then [14, Theorems 2, 3, 4, Corollary 1]); mention also the numerous pioneering Horie's papers proving results of the form: "let ℓ_0 be a small prime; then a prime p, totally inert in some $\mathbb{Q}(\ell_0^{n_0})$, yields $\mathscr{C}_{\mathbb{Q}(\ell_0^n)} = 1$ for all n". In [5], a conjecture (from "speculative extensions of the Cohen–Lenstra–Martinet heuristics") implies $\mathscr{C}^*_{\mathbb{Q}(\ell^n)} \neq 1$ for finitely many layers (possibly none).

Concerning the torsion groups $\mathscr{T}_K$, $K = \mathbb{Q}(\ell^n)$, we observe that in general the solutions p, for $\#\mathscr{T}_K^* \equiv 0 \pmod p$, also fulfill $p \equiv 1 \pmod{\ell^n}$, which is in some sense a strong form of Washington's result because the reflection theorem that we shall recall later in Section 5, in $L := K(\mu_p)$, the p-rank of $\mathscr{T}_K^*$ is bounded by that of a suitable component of $\mathscr{C}_L^*$. Thus Washington's theorem may be true for the torsion groups in K.

One can wonder what happens for the normalized regulators $\mathscr{R}_K$ and the relative components $\mathscr{R}_K^*$, due to the specific nature of a regulator as a Frobenius determinant and regarding the previous observations. So, recall some algebraic facts about the $\mathscr{R}_K^*$ that we can explain from heuristics and probabilistic studies given in [21, § 4.2.2]. For any real Galois extension $K/\mathbb{Q}$, of Galois group G, the normalized p-adic regulator $\mathscr{R}_K$ may be defined via the conjugates of the p-adic logarithm of a suitable Minkowski unit η and can be written, regarding G, as Frobenius determinant $\mathrm{R}_p^G(\eta) = \prod_\theta \mathrm{R}_p^\theta(\eta)$, where θ runs trough the irreducible p-adic characters, and $\mathrm{R}_p^\theta(\eta) = \prod_{\psi|\theta} \mathrm{R}_p^\psi(\eta)$ with absolutely irreducible characters ψ. Then, in a standard point of view, $\mathrm{Prob}\big(\mathscr{R}_K^\theta \equiv 0 \pmod p\big) = \frac{O(1)}{p^{\rho\,\delta^2}}$ (loc. cit.), where ρ is still the residue degree of p in the field of values of ψ and $\delta \geq 1$ is a suitable multiplicity of the absolutely irreducible θ-representation (in our case, $\rho = \rho_{\ell^n}$ and $\delta = 1$).

Contrary to the class group of K (for K fixed) which is *finite*, the primes p such that $\mathscr{R}_K \equiv 0 \pmod p$ may be, a priori, infinite in number (we have conjectured that it is not the case, but this is an out of reach conjecture). Nevertheless, some very large p with $\rho = 1$, may divide $\#\mathscr{R}_K^\theta$, which indicates other probabilities conjectured in [21, Théorème 1.1]. This analysis also confirms that, for ℓ and p fixed, $\mathscr{T}_{\mathbb{Q}(\ell^n)}$ may be constant for all n large enough.

We have computed the order $\#\widetilde{\mathscr{C}\ell}_K$ of the logarithmic class groups (from [4]), and we have no non-trivial example; this means that the logarithmic class group behaves, in some sense, as the ordinary p-class group in $\mathbb{Q}(\ell^\infty)$ or in any $K=\mathbb{Q}(N)$, but not as $\mathscr{T}_K$, as we have seen. This is not too surprising since if $\mathscr{C}\ell_K=1$ and if p is totally inert in K, then $\widetilde{\mathscr{C}\ell}_K=1$ (see [43, Schéma § 2.3] or [29, Diagram 4.2]).

2.5. **Computation of the structure of $\mathscr{T}_K$ for $K=\mathbb{Q}(\ell^n)$.** The following PARI/GP programs give the structure, of abelian group, of $\mathscr{T}_{\mathbb{Q}(\ell^n)}$, from the polynomial P defining $\mathbb{Q}(\ell^n)$: $\mathsf{P}=\mathsf{polsubcyclo}(\mathsf{el}^{\mathsf{n}+1},\mathsf{el}^{\mathsf{n}})$ for $p>2$ and: $\mathsf{P}=\mathsf{x};\mathsf{for}(\mathsf{j}=1,\mathsf{n},\mathsf{P}=\mathsf{P}^2-2)$, for $p=2$. These programs are the simplified form of the following general one written in [26, Program I, § 3.2], for *any monic irreducible polynomial in* $\mathbb{Z}[x]$, where r is the number of independent $\mathbb{Z}_p$-extensions:

```
PROGRAM I. FOR ANY NUMBER FIELD AND ANY p
{P=x^3-7*x+1;K=bnfinit(P,1);b=2;B=10^5;r=K.sign[2]+1;forprime(p=b,B,Ex=12;
KpEx=bnrinit(K,p^Ex);HpEx=KpEx.cyc;L=List;e=matsize(HpEx)[2];R=0;
for(k=1,e-r,c=HpEx[e-k+1];w=valuation(c,p);if(w>0,R=R+1;
listinsert(L,p^w,1)));if(R>0,print("p=",p," rk(T_p)=",R," T_p=",L)))}
p=7   rk(T_p)=1  T_p=List([7])       p=701 rk(T_p)=1  T_p=List([701])
```

The parameter Ex must be such that p^{Ex} is larger than the exponent of $\mathscr{T}_K$; taking $\mathsf{Ex}=2$ for $p>2$ (resp. $\mathsf{Ex}=3$ for $p=2$) gives the p-rank of $\mathscr{T}_K$.

```
PROGRAM II. STRUCTURE OF T_K, K=Q(el^n), FOR ANY el, n, p<Bp
{el=2;n=3;Bp=2*10^5;if(el==2,P=x;for(j=1,n,P=P^2-2));if(el!=2,
P=polsubcyclo(el^(n+1),el^n));Ex=6;K=bnfinit(P,1);forprime(p=2,Bp,
KpEx=bnrinit(K,p^Ex);HpEx=KpEx.cyc;L=List;e=matsize(HpEx)[2];R=0;
for(k=1,e-1,c=HpEx[e-k+1];w=valuation(c,p);
if(w>0,R=R+1;listinsert(L,p^w,1)));
if(R>0,print("el=",el," n=",n," p=",p," rk(T)=",R," T=",L)))}

el=2 n=1 p=13  rk(T)=1 T=[13]          el=2 n=3 p=29  rk(T)=1 T=[29]
el=2 n=1 p=31  rk(T)=1 T=[31]          el=2 n=3 p=521 rk(T)=1 T=[521]
el=2 n=2 p=13  rk(T)=2 T=[169,13]      el=3 n=1 p=7   rk(T)=1 T=[7]
el=2 n=2 p=31  rk(T)=1 T=[31]          el=3 n=1 p=73  rk(T)=1 T=[73]
el=2 n=2 p=29  rk(T)=1 T=[29]          el=3 n=2 p=7   rk(T)=1 T=[7]
el=2 n=2 p=37  rk(T)=1 T=[37]          el=3 n=2 p=73  rk(T)=1 T=[73]
el=2 n=3 p=3   rk(T)=2 T=[3,3]         el=5 n=1 p=11  rk(T)=2 T=[11,11]
el=2 n=3 p=31  rk(T)=1 T=[31]          el=5 n=2 p=11  rk(T)=2 T=[11,11]
el=2 n=3 p=13  rk(T)=2 T=[169,13]      el=5 n=2 p=101 rk(T)=1 T=[101]
el=2 n=3 p=37  rk(T)=1 T=[37]
```

Remark 2.2. *These partial results show that p-ramification aspects are more intricate since, for instance for $\ell=2$, the divisibility by $p=29$ only appears for $n=2$ and, for $p=13$, the 13-rank and the exponent increase from $n=1$ to $n=2$.*
Unfortunately, it is not possible in practice to compute beyond $\ell=17$ with the instruction bnfinit. *So, as we have explained in the Introduction, we shall give Section 3 another method to test $\mathscr{T}_{\mathbb{Q}(N)}\neq 1$ for larger N and p; this algorithm only uses elementary basic instructions and does not need any large computer memory contrary to* bnfinit *(see Table 6.2).*

3. Definition of p-adic measures

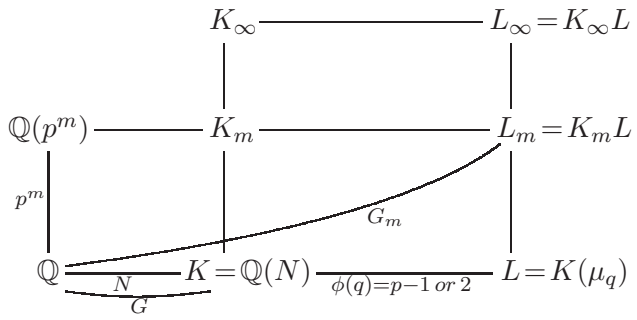
We recall the main classical principles to apply them to the fields $\mathbb{Q}(N)$, with any prime $p\geq 2$, $p\nmid N$.

3.1. **General definition of the Stickelberger elements.** Let $f>1$ be any abelian conductor and let $\mathbb{Q}(\mu_f)$ be the corresponding cyclotomic field.

We define $\mathscr{S}_{\mathbb{Q}(\mu_f)}:=-\sum_{a=1}^{f}\left(\frac{a}{f}-\frac{1}{2}\right)\cdot\left(\frac{\mathbb{Q}(\mu_f)}{a}\right)^{-1}$ (where the integers a are prime to f and where Artin symbols are taken over $\mathbb{Q}$).

The properties of annihilation need to multiply $\mathscr{S}_{\mathbb{Q}(\mu_f)}$ by a multiplier $1-c\cdot\big(\frac{\mathbb{Q}(\mu_f)}{c}\big)^{-1}$, for any odd c prime to f; this shall give integral elements in $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q})]$. If $p\cdot f$ is odd, one may take $c=2$ for annihilation in the $\mathbb{Z}_p$-algebra considered since $\frac{1}{2}\sum_{a=1}^{f}\big(\frac{\mathbb{Q}(\mu_f)}{a}\big)^{-1}$ can be neglected at the end.

Put $q=p$ (resp. 4) if $p\neq 2$ (resp. $p=2$). For $K=\mathbb{Q}(N)$, let $L=K(\mu_q)$; to simplify, put $K_m:=K\mathbb{Q}(p^m)$, $L_m:=K_mL=K(\mu_{qp^m})$ for all $m\geq 0$; so $\cup_m K_m=K_\infty$ and $\cup_m L_m=L_\infty$. All is summarized by the following diagram where $G_m\simeq\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/p^m\mathbb{Z}\times\mathbb{Z}/\phi(q)\mathbb{Z}$, ϕ being the Euler function:



3.2. **Multipliers of the Stickelberger elements.** Let f_N be the conductor of $K=\mathbb{Q}(N)$, $N=\ell_1^{n_1}\cdots\ell_t^{n_t}$. We have $f_N=\ell_1^{n_1+1}\cdots\ell_t^{n_t+1}$ if N is odd and $f_N=2^{n_1+2}\cdot\ell_2^{n_2+1}\cdots\ell_t^{n_t+1}$ if N is even. The conductor of L_m is $f_{L_m}=qp^m\cdot f_N$ for $2\nmid N$ and $p^{m+1}\cdot f_N$ otherwise.

Put $f_{L_m}=:f_N^m$ and let c be prime to f_N^m and, by restriction of $\mathscr{S}_{\mathbb{Q}(\mu_{f_N^m})}$ to L_m, let $\mathscr{S}^c_{L_m}:=\Big(1-c\Big(\frac{L_m}{c}\Big)^{-1}\Big)\cdot\mathscr{S}_{L_m}$; then $\mathscr{S}^c_{L_m}\in\mathbb{Z}[G_m]$. Indeed:

$$\mathscr{S}^c_{L_m}=\tfrac{-1}{f_N^m}\sum_a\Big[a\Big(\tfrac{L_m}{a}\Big)^{-1}-ac\Big(\tfrac{L_m}{a}\Big)^{-1}\Big(\tfrac{L_m}{c}\Big)^{-1}\Big]+\tfrac{1-c}{2}\sum_a\Big(\tfrac{L_m}{a}\Big)^{-1};$$

let $a'_c\in[1,f_N^m]$ be the unique integer such that $a'_c\cdot c\equiv a\pmod{f_N^m}$ and put $a'_c\cdot c=a+\lambda_a^m(c)f_N^m$, $\lambda_a^m(c)\in\mathbb{Z}$; using the bijection $a\mapsto a'_c$ in the summation of the second term in $[\ ]$ and $\Big(\frac{L_m}{a'_c}\Big)\Big(\frac{L_m}{c}\Big)=\Big(\frac{L_m}{a}\Big)$, this yields:

$$\begin{aligned}\mathscr{S}^c_{L_m}&=\tfrac{-1}{f_N^m}\Big[\sum_a a\Big(\tfrac{L_m}{a}\Big)^{-1}-\sum_a a'_c\cdot c\Big(\tfrac{L_m}{a'_c}\Big)^{-1}\Big(\tfrac{L_m}{c}\Big)^{-1}\Big]+\tfrac{1-c}{2}\sum_a\Big(\tfrac{L_m}{a}\Big)^{-1}\\&=\tfrac{-1}{f_N^m}\sum_a\Big[a-a'_c\cdot c\Big]\Big(\tfrac{L_m}{a}\Big)^{-1}+\tfrac{1-c}{2}\sum_a\Big(\tfrac{L_m}{a}\Big)^{-1}\\&=\sum_a\Big[\lambda_a^m(c)+\tfrac{1-c}{2}\Big]\Big(\tfrac{L_m}{a}\Big)^{-1}\in\mathbb{Z}[G_m].\end{aligned}$$

Lemma 3.1. *We have the relations* $\lambda^m_{f_N^m-a}(c)+\frac{1-c}{2}=-\big(\lambda_a^m(c)+\frac{1-c}{2}\big)$ *for all* $a\in[1,f_N^m]$ *prime to* f_N^m. *Then* $\mathscr{S}'^c_{L_m}:=\sum_{a=1}^{f_N^m/2}\big[\lambda_a^m(c)+\frac{1-c}{2}\big]\big(\frac{L_m}{a}\big)^{-1}\in\mathbb{Z}[G_m]$ *is such that* $\mathscr{S}^c_{L_m}=\mathscr{S}'^c_{L_m}\cdot(1-s_\infty)$.

Proof. By definition, $(f_N^m-a)'_c$ is in $[1,f_N^m]$ and congruent modulo f_N^m to $(f_N^m-a)\,c^{-1}\equiv -ac^{-1}\equiv -a'_c\pmod{f_N^m}$; thus $(f_N^m-a)'_c=f_N^m-a'_c$ and $\lambda^m_{f_N^m-a}(c)=\frac{(f_N^m-a)'_c\,c-(f_N^m-a)}{f_N^m}=\frac{(f_N^m-a'_c)\,c-(f_N^m-a)}{f_N^m}=c-1-\lambda_a^m(c)$, whence $\lambda^m_{f_N^m-a}(c)+\frac{1-c}{2}=-\big(\lambda_a^m(c)+\frac{1-c}{2}\big)$ and the result. □

3.3. **Spiegel involution.** Let $\kappa_m:G_m\to(\mathbb{Z}/qp^m\mathbb{Z})^\times\simeq\mathrm{Gal}(\mathbb{Q}(\mu_{qp^m})/\mathbb{Q})$ be the *cyclotomic character of level* m, of kernel $\mathrm{Gal}(L_m/\mathbb{Q}(\mu_{qp^m}))$, defined by $\zeta^s=\zeta^{\kappa_m(s)}$, for all $s\in G_m$ and all $\zeta\in\mu_{qp^m}$. The Spiegel involution is the involution of $(\mathbb{Z}/qp^m\mathbb{Z})[G_m]$ defined by $x:=\sum_{s\in G_m}a_s\cdot s\longmapsto\ x^*:=\sum_{s\in G_m}a_s\cdot\kappa_m(s)\cdot s^{-1}$.

Thus, if s is the Artin symbol $\left(\frac{L_m}{a}\right)$, then $\left(\frac{L_m}{a}\right)^* \equiv a \cdot \left(\frac{L_m}{a}\right)^{-1} \pmod{qp^m}$. From Lemma 3.1, we obtain $\mathscr{S}^{c\,*}_{L_m} = \mathscr{S}'^{c\,*}_{L_m} \cdot (1 + s_\infty)$ in $(\mathbb{Z}/qp^m\mathbb{Z})[G_m]$.

We shall use the case $m = 0$ for which we have $\kappa_m(s) \equiv \omega(s) \pmod{q}$, where ω is the usual Teichmüller character $\omega : G_0 = \mathrm{Gal}(L/\mathbb{Q}) \to \mathbb{Z}_p^\times$.

4. Annihilation theorem of $\mathscr{T}_K^*$

Recall that, for $K = \mathbb{Q}(N)$ we put $K_m := K\mathbb{Q}(p^m)$ and $L_m := K_m L$, where $L = K(\mu_q)$, $q = p$ or 4. For *the most precise and straightforward method*, the principle, which was given in the 60's and 70's, is to consider the annihilation, by means of the above Stickelberger twist, of the kummer radical in $L_m^\times$ defining the maximal sub-extension of $H^{\mathrm{pr}}_{K_m}$ whose Galois group is of exponent p^m, then to use the Spiegel involution giving a p-adic measure annihilating, for $m \to \infty$, the finite Galois group $\mathscr{T}_K$ (see [19, 23] for more history). The case $p = 2$ is particularly tricky; to overcome this difficulty, we shall refer to [18, 31].

In fact, this process is equivalent to get, elementarily, an explicit approximation of the p-adic L-functions "at $s = 1$", avoiding the ugly computation of Gauss sums and p-adic logarithms of cyclotomic units [59, Theorem 5.18]. We have the following result with a detailed proof in [23, Theorems 5.3, 5.5]:

Proposition 4.1. *For $p \geq 2$, let p^e be the exponent of $\mathscr{T}_K$ for $K = \mathbb{Q}(N)$. For all $m \geq e$, the $(\mathbb{Z}/qp^m\mathbb{Z})[G_m]$-module $\mathscr{T}_K$ is annihilated by $\mathscr{S}'^{c\,*}_{L_m}$.*

From the expression of $\mathscr{S}'^{c}_{L_m}$ (Lemma 3.1), the Spiegel involution yields:

$$\mathscr{S}'^{c\,*}_{L_m} \equiv \sum_{a=1}^{f_N^m/2} \left[\lambda_a^m(c) + \frac{1-c}{2}\right] a^{-1}\left(\frac{L_m}{a}\right) \pmod{qp^m}, \tag{1}$$

defining a coherent family in $\varprojlim_{m \geq e} (\mathbb{Z}/qp^m\mathbb{Z})[G_m]$. One obtains, by restriction of $\mathscr{S}'^{c\,*}_{L_m}$ to K, a coherent family of annihilators of $\mathscr{T}_K$, whose p-adic limit

$$\mathscr{A}'^{c}_K := \lim_{m\to\infty} \sum_{a=1}^{f_N^m/2} \left[\lambda_a^m(c) + \frac{1-c}{2}\right] a^{-1}\left(\frac{K}{a}\right) \text{ in } \mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})],$$

is a canonical annihilator of $\mathscr{T}_K$.

Remark 4.2. *Let $\alpha^*_{L_m} := \left[\sum_{a=1}^{f_N^m} \left(\frac{L_m}{a}\right)^{-1}\right]^* \equiv \sum_{a=1}^{f_N^m} a^{-1}\left(\frac{L_m}{a}\right) \pmod{qp^m}$; then: $\alpha^*_{L_m} := \sum_{a=1}^{f_N^m/2} a^{-1}\left(\frac{L_m}{a}\right) + (f_N^m - a)^{-1}\left(\frac{L_m}{f_N^m - a}\right) \equiv \sum_{a=1}^{f_N^m/2} a^{-1}\left(\frac{L_m}{a}\right)(1 - s_\infty) \bmod f_N^m$,*

which annihilates $\mathscr{T}_K$, modulo p, by restriction since K is real. We shall neglect $\frac{1-c}{2} \cdot \alpha^*_{L_m}$ and we still denote $\mathscr{A}'^{c}_K := \lim_{m\to\infty} \left[\sum_{a=1}^{f_N^m/2} \lambda_a^m(c)\, a^{-1}\left(\frac{K}{a}\right)\right]$.

Lemma 4.3. *For $K = \mathbb{Q}(N)$, ψ_N of order N and conductor f_N, one has $\psi_N(\mathscr{A}'^{c}_K) = (1 - \psi_N(c)) \cdot \frac{1}{2} L_p(1, \psi_N)$.*

Proof. Classical construction of p-adic L-functions (e.g., [19, Propositions II.2, II.3, Définition II.3, II.4, Remarques II.3, II.4], after Amice–Fresnel works, then [59, Chapters 5, 7]). For more details, see [23, § 7.1]. □

Proposition 4.4. *Let $K := \mathbb{Q}(N)$, $N = \ell_1^{n_1} \cdots \ell_t^{n_t}$, and let $p \nmid N$. Then, for the p-adic character θ_N above a character ψ_N of order N of K, the component $\mathscr{T}_K^{\theta_N}$ is annihilated by $(1 - \psi_N(c)) \cdot \frac{1}{2} L_p(1, \psi_N)$. Moreover, from the principal theorem of Ribet–Mazur–Wiles–Kolyvagin–Greither on abelian fields, $\frac{1}{2} L_p(1, \psi_N)$ gives its order.*

In the practice, taking $c = 2$ in the programs when N is odd and $p \neq 2$, we obtain the annihilation by $(1 - \psi_N(2)) \cdot \frac{1}{2} L_p(1, \psi_N)$, where $\psi_N(2)$ is a root of unity of order dividing N, hence prime to p; thus $(1 - \psi_N(2))$ is invertible modulo p, except when $\psi_N(2) = 1$ for $N = 1093, 3511, \ldots$ which are in fact unfeasible numerically. If $p = 2$ an odd c prime to N must be chosen.

Lemma 4.5. [23, Corollary 7.3 (iii)]. *We have* $\mathscr{A}_K^{\prime c} \equiv \sum_{a=1}^{q f_N/2} \lambda_a^0(c)\, a^{-1} \left(\frac{K}{a}\right)$ *(mod p), whence* $\psi_N(\mathscr{A}_K^{\prime c}) \equiv (1 - \psi_N(c)) \cdot \frac{1}{2} L_p(1, \psi_N) \pmod p$.

Thus, we have obtained a computable characterization of non-triviality of $\mathscr{T}_K$, for $K = \mathbb{Q}(N)$, $N = \ell_1^{n_1} \cdots \ell_t^{n_t}$, and for any $p \geq 2$, $p \nmid N$, where f_N is the conductor of K (see § 3.2):

Theorem 4.6. *Let $L = K(\mu_q)$, $q = p$ or 4 as usual. Let c be an integer prime to $q\, f_N$. For all $a \in [1, q\, f_N]$, prime to $q\, f_N$, let a'_c be the unique integer in $[1, q\, f_N]$ such that $a'_c \cdot c \equiv a \pmod{q\, f_N}$ and put $a'_c \cdot c - a = \lambda_a(c)\, q\, f_N$, $\lambda_a(c) \in \mathbb{Z}$. Let $\mathscr{A}_K^{\prime c} \equiv \sum_{a=1}^{q f_N/2} \lambda_a(c)\, a^{-1} \left(\frac{K}{a}\right) \pmod p$, let ψ_N be a character of K of order N and θ_N the p-adic character above ψ_N. Then, if c is chosen such that $\psi_N(c) \neq 1$, the θ_N-component of the $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-module $\mathscr{T}_K$ is non-trivial if and only if $\psi_N(\mathscr{A}_K^{\prime c})$ is not a p-adic unit.*

4.1. **Numerical test $\mathscr{T}^*_{\mathbb{Q}(\ell^n)} \neq 1$ for $\ell > 2$, $p > 2$.** We have, from § 2.4, $\mathscr{T}_{\mathbb{Q}(\ell^n)} = \mathscr{T}^*_{\mathbb{Q}(\ell^n)} \bigoplus \mathscr{T}_{\mathbb{Q}(\ell^{n-1})}$. For a character ψ of order ℓ^n of K, the condition $\psi(\mathscr{A}_{\mathbb{Q}(\ell^n)}^{\prime c}) \equiv 0 \pmod{\mathfrak{p}}$, for some $\mathfrak{p} \mid p$, is equivalent to the non-triviality of $\mathscr{T}^*_{\mathbb{Q}(\ell^n)}$, due to the p-adic character θ above ψ. We compute $\psi(\mathscr{A}_{\mathbb{Q}(\ell^n)}^{\prime c}) \pmod p$ and test if the norm of this element is divisible by p; this characterize the condition $\mathscr{T}^*_{\mathbb{Q}(\ell^n)} \neq 1$:

```
PROGRAM III. TEST #T*>1 WITH NORM COMPUTATIONS FOR el>2, p>2
{C=2;forprime(el=3,120,for(n=1,4,Q=polcyclo(el^n);
h=znprimroot(el^(n+1));H=lift(h);forprime(p=3,2500,if(p==el,next);
f=p*el^(n+1);cm=Mod(C,f)^-1;g=znprimroot(p);G=lift(g);gm=g^-1;
e=lift(Mod((1-H)*el^(-n-1),p));H=H+e*el^(n+1);h=Mod(H,f);
e=lift(Mod((1-G)*p^-1,el^(n+1)));G=G+e*p;g=Mod(G,f);
S=0;hh=1;gg=1;ggm=1;for(u=1,el^n*(el-1),hh=hh*h;
t=0;for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh*gg);A=lift(a*cm);
t=t+(A*C-a)/f*ggm);S=S+lift(t)*x^u);s=Mod(S,Q);vp=valuation(norm(s),p);
if(vp>0,print("el=",el," n=",n," p=",p)))))}
```

The program finds again very quickly the cases of Table 2.5: ($\ell^n = 3$, $p = 7$, $p = 73$), ($\ell^n = 27$, $p = 109$), ($\ell^n = 81$, $p = 487$, $p = 1621$), etc., ($\ell = 5$, $p = 11$), ($\ell = 25$, $p = 101$, $p = 1151$, $p = 2251$), ($\ell = 125$, $p = 2251$), etc.

Interesting cases are $\ell = 5$ giving $\mathscr{T}_{\mathbb{Q}(5^2)} \simeq \mathbb{Z}/2251\mathbb{Z}$ and $\mathscr{T}^*_{\mathbb{Q}(5^3)} \simeq \mathbb{Z}/2251\mathbb{Z}$; which implies that $\mathscr{T}_{\mathbb{Q}(5^3)}$ contains $(\mathbb{Z}/2251\mathbb{Z})^2$.

To verify, we have computed, with Program II of § 2.5, the structure of $\mathscr{T}_{\mathbb{Q}(\ell^n)}$ for $\ell^n = 27$, $p = 109$, which is much longer and needs an huge computer memory; we get as expected $\mathsf{el} = 3\ \mathsf{n} = 3\ \mathsf{p} = 109\ \ \mathsf{rk}(\mathsf{T}) = 1\ \ \mathsf{T} = [109]$.

Whence, we can propose the following program, only considering primes $p \equiv 1 \pmod{\ell^n}$, so that p splits completely in $\mathbb{Q}(\mu_{\ell^n})$ which allows to characterize, once for all, a prime $\mathfrak{p} \mid p$ by means of a congruence $\mathsf{z} \equiv \mathsf{r} \pmod{\mathfrak{p}}$, where z denotes, in the program, a generator of μ_{ℓ^n} and r a rational integer, then avoiding the computation of $\mathsf{N} = \mathsf{norm}(\mathsf{s})$ in some programs, which takes too much time. We then find supplementary examples.

```
PROGRAM IV. TEST #T*>1 MODULO (zeta-r) WHEN p=1 (mod el^n) FOR el>2, p>2
{C=2;forprime(el=3,250,for(n=1,6,Q=polcyclo(el^n);h=znprimroot(el^(n+1));
H=lift(h);forprime(p=3,5000,if(Mod(p,el^n)!=1,next);Qp=Mod(1,p)*Q;
m=(p-1)/el^n;r=znprimroot(p)^m;f=p*el^(n+1);cm=Mod(C,f)^-1;
g=znprimroot(p);G=lift(g);gm=g^-1;
```

```
e=lift(Mod((1-H)*el^(-n-1),p));H=H+e*el^(n+1);h=Mod(H,f);
e=lift(Mod((1-G)*p^-1,el^(n+1)));G=G+e*p;g=Mod(G,f);
S=0;hh=1;gg=1;ggm=1;for(u=1,el^n*(el-1)/2,hh=hh*h;
t=0;for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh*gg);A=lift(a*cm);
t=t+(A*C-a)/f*ggm);S=S+lift(t)*x^u);s=lift(Mod(S,Qp));
R=1;for(k=1,el^n,R=R*r;if(Mod(k,el)==0,next);t=Mod(s,x-R);
if(t==0,print("el=",el," n=",n," p=",p))))))}
```

```
PROGRAM V. VARIANT FOR ANY NUMBER d OF p-PLACES
USING THE FACTORIZATION OF Q mod p
d (a power of el) may be optionally specified (e.g. d=1,el,...):

{el=3;C=2;for(n=1,10,Q=polcyclo(el^n);h=znprimroot(el^(n+1));H=lift(h);
forprime(p=5,2*10^4,f=p*el^(n+1);cm=Mod(C,f)^-1;Qp=Mod(1,p)*Q;
F=factor(Q+O(p));R=lift(component(F,1));d=matsize(F)[1];
g=znprimroot(p);G=lift(g);gm=g^-1;
e=lift(Mod((1-H)*el^(-n-2),p));H=H+e*el^(n+2);h=Mod(H,f);
e=lift(Mod((1-G)*p^-1,el^(n+2)));G=G+e*p;g=Mod(G,f);
S=0;hh=1;gg=1;ggm=1;for(u=1,el^n*(el-1)/2,hh=hh*h;
t=0;for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh*gg);A=lift(a*cm);
t=t+(A*C-a)/f*ggm);S=S+lift(t)*x^u);s=lift(Mod(S,Qp));
for(k=1,d,t=Mod(s,R[k]);if(t==0,print("el=",el," n=",n," p=",p)))))}
```

The following table is the addition of that obtained with Programs III–V:

el=3	n=1	p=7	el=5	n=2	p=6701	el=67	n=1	p=269
el=3	n=1	p=73	el=5	n=3	p=2251	el=83	n=1	p=499
el=3	n=3	p=109	el=5	n=3	p=27751	el=101	n=1	p=607
el=3	n=3	p=17713	el=5	n=4	p=11251	el=107	n=1	p=857
el=3	n=4	p=487	el=17	n=1	p=239	el=109	n=1	p=50359
el=3	n=4	p=1621	el=23	n=1	p=47	el=131	n=1	p=2621
el=3	n=7	p=17497	el=29	n=1	p=59	el=131	n=1	p=8123
el=5	n=1	p=11	el=37	n=1	p=4441	el=131	n=1	p=34061
el=5	n=2	p=101	el=43	n=1	p=173	el=137	n=1	p=1097
el=5	n=2	p=1151	el=47	n=1	p=283	el=151	n=1	p=907
el=5	n=2	p=2251	el=61	n=1	p=1709	el=191	n=1	p=383

In the case $p = 2$, $\ell > 2$, we have the exceptional prime $\ell = 11$ for which 3 splits in $\mathbb{Q}(11)$, whence $1 - \psi_{11}(3) = 0$, giving a wrong solution with $C = 3$. Moreover, the 2-adic characters θ of $\mathbb{Q}(\ell^n)$ cannot be of degree 1 in practice since 2 is inert in $\mathbb{Q}(\ell)$ except for the two known cases of non-trivial Fermat quotients of 2 modulo ℓ; so we are obliged to test with the computation of a norm in $\mathbb{Q}(\mu_\ell)$. As expected, any program gives the solutions $\ell = 1093$, $n = 1$, $p = 2$ and $\ell = 3511$, $n = 1$, $p = 2$. For $\ell = 1093$, see Remarks 5.2.

4.2. **Numerical test $\mathscr{T}^*_{\mathbb{Q}(2^n)} \neq 1$ for $\ell = 2$, $p > 2$.** We have only to modify the conductor $p\,2^{n+2}$ of $L = K(\mu_p)$ where $K = \mathbb{Q}(2^n)$, then note that we must choose another multiplier for the Stickelberger element and the generator $\mathsf{h} = \mathsf{Mod}(5, \mathsf{el}^{(n+2)})$ (for $p = 3$ one must take $C = 5$ giving the solution $\mathsf{el} = 2 \;\; \mathsf{n} = 3 \;\; \mathsf{p} = 3$). To obtain a half-system S for $a \in [1, p\,2^{n+2}]$ we can neglect the subgroup generated by the generator of $\mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q}(2^n)(\mu_p))$ (will be proven in the general case in Lemma 6.1):

```
PROGRAM VI. TEST #T>1 WITH NORM COMPUTATIONS FOR el=2, p>3
{el=2;for(n=1,8,Q=polcyclo(el^n);h=Mod(5,el^(n+2));H=lift(h);C=3;
forprime(p=5,2*10^4,f=p*el^(n+2);cm=Mod(C,f)^-1;
g=znprimroot(p);G=lift(g);gm=g^-1;
e=lift(Mod((1-H)*el^(-n-2),p));H=H+e*el^(n+2);h=Mod(H,f);
e=lift(Mod((1-G)*p^-1,el^(n+2)));G=G+e*p;g=Mod(G,f);
S=0;hh=1;gg=1;ggm=1;for(u=1,el^n,hh=hh*h;
t=0;for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh*gg);A=lift(a*cm);
t=t+(A*C-a)/f*ggm);S=S+lift(t)*x^u);s=Mod(S,Q);
vp=valuation(norm(s),p);if(vp>0,print("el=",el," n=",n," p=",p))))}
```

For instance the results $\mathsf{el}=2\ \mathsf{n}=1\ \mathsf{p}=13$, $\mathsf{el}=2\ \mathsf{n}=2\ \mathsf{p}=13$ correspond to the following cases of Table 2.5: $\mathsf{el}^{\mathsf{n}}=2\ \mathsf{p}=13\ \mathsf{rk}(\mathsf{T})=1\ \mathsf{T}=[13]$ and $\mathsf{el}^{\mathsf{n}}=4\ \mathsf{p}=13\ \mathsf{rk}(\mathsf{T})=2\ \mathsf{T}=[169,13]$.

As for $\ell>2$, we have a faster program using only primes $p\equiv 1\,(\mathrm{mod}\ 2^n)$, which gives new solutions (e.g., $\ell^n=2^{10}$, $p=114689$). The table below is the addition of that obtained with these two programs:

```
PROGRAM VII. TEST #T*>1 MODULO (zeta-r) WHEN p=1 (mod el^n) FOR el=2, p>3
{el=2;for(n=1,12,Q=polcyclo(el^n);h=Mod(5,el^(n+2));H=lift(h);C=3;
forprime(p=5,2*10^5,if(Mod(p,el^n)!=1,next);f=p*el^(n+2);cm=Mod(C,f)^-1;
Qp=Mod(1,p)*Q;m=(p-1)/el^n;r=znprimroot(p)^m;
g=znprimroot(p);G=lift(g);gm=g^-1;
e=lift(Mod((1-H)*el^(-n-2),p));H=H+e*el^(n+2);h=Mod(H,f);
e=lift(Mod((1-G)*p^-1,el^(n+2)));G=G+e*p;g=Mod(G,f);
S=0;hh=1;gg=1;ggm=1;for(u=1,el^n,hh=hh*h;
T=0;for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh*gg);A=lift(a*cm);
T=T+(A*C-a)/f*ggm);S=S+lift(T)*x^u);s=lift(Mod(S,Qp));
R=1;for(k=1,el^n,R=R*r;if(Mod(k,el)==0,next);t=Mod(s,x-R);
if(t==0,print("el=",el," n=",n," p=",p)))))}
```

el=2	n=1	p=13	el=2	n=3	p=3	el=2	n=7	p=257
el=2	n=1	p=31	el=2	n=3	p=521	el=2	n=7	p=641
el=2	n=2	p=13	el=2	n=5	p=3617	el=2	n=8	p=18433
el=2	n=2	p=29	el=2	n=5	p=4513	el=2	n=10	p=114689
el=2	n=2	p=37	el=2	n=6	p=193			

```
PROGRAM VIII. VARIANT USING THE FACTORIZATION OF Q (mod p)
for any number d of p-places of K
{el=2;for(n=1,12,Q=polcyclo(el^n);h=Mod(5,el^(n+2));H=lift(h);C=3;
forprime(p=5,2*10^5,f=p*el^(n+2);cm=Mod(C,f)^-1;Qp=Mod(1,p)*Q;
F=factor(Q+O(p));R=lift(component(F,1));d=matsize(F)[1];
\\d (a power of 2) may be optionally specified (e.g. d=1, d=2)
g=znprimroot(p);G=lift(g);gm=g^-1;
e=lift(Mod((1-H)*el^(-n-2),p));H=H+e*el^(n+2);h=Mod(H,f);
e=lift(Mod((1-G)*p^-1,el^(n+2)));G=G+e*p;g=Mod(G,f);
S=0;hh=1;gg=1;ggm=1;for(u=1,el^n,hh=hh*h;
T=0;for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh*gg);A=lift(a*cm);
T=T+(A*C-a)/f*ggm);S=S+lift(T)*x^u);s=lift(Mod(S,Qp));
for(k=1,d,t=Mod(s,R[k]);if(t==0,print("el=",el," n=",n," p=",p)))))}
```

4.3. **Test on the normalized p-adic regulator.** A *sufficient condition* to get the divisibility of $\#\mathscr{C}_K$ by p, when we have obtained $\mathscr{T}_K\neq 1$, is to establish that the normalized p-adic regulator $\mathscr{R}_K$ is a p-adic unit; otherwise, this only gives that very probably $\#\mathscr{C}_K=1$. Since with PARI/GP the computation of units implies that of the class number (due to $\mathsf{K}=\mathsf{bnfinit}(\mathsf{P})$), there is no interest to test the p-divisibility of the regulator instead of looking at $\mathsf{K.no}$ (the class number), except to obtain some verifications and to get the p-adic relations between the units.

The following program computes the p-rank of the matrix M obtained by approximation (modulo p) of the p-adic expressions $\frac{1}{p}\log_p(\varepsilon_i)$, written on a $\mathbb{Z}$-basis of K (via $\mathsf{nfalgtobasis}$), for a system of fundamental units ε_i given by PARI/GP; then $\mathscr{R}_K$ is a p-adic unit if and only if $\mathrm{rank}(M)=\ell^n-1$:

```
PROGRAM IX. TEST ON THE REGULATOR R FOR el>2, n>=1
{el=17;n=1;p=239;N=el^n;if(el==2,P=x;for(j=1,n,P=P^2-2));
if(el!=2,P=polsubcyclo(el^(n+1),el^n));Pp=P*Mod(1,p^2);
K=bnfinit(P,1);E=K.fu;L=List;for(k=1,N-1,e=E[k];
ep=Mod(lift(e),Pp);epm=Mod(lift(e^-1),Pp);
Ep=ep;for(u=1,N,Ep=Ep^p);Ep=Ep*epm;le=lift(Ep-1);Le=0;
for(j=0,N,c=polcoeff(le,j);c=lift(c);Le=Le+c*x^j);
Le=nfalgtobasis(K,Le)/p;LogE=Mod(Le,p);listinsert(L,LogE,1));
```

```
M=matrix(N-1,N,i,j,polcoeff(L[i],j));rk=matrank(M);
if(rk==N-1,print("N =",N," p=",p," rk(M)=",rk," R_K invertible"));
if(rk<N-1,print("N =",N," p=",p," rk(M)=",rk," R_K=0 mod (p)"))}

N=3 p=7  rk(M)=1 R_K=0 mod (p)    N=17 p=239 rk(M)=15 R_K=0 mod (p)
N=3 p=73 rk(M)=1 R_K=0 mod (p)    N=23 p=47  rk(M)=21 R_K=0 mod (p)
N=5 p=11 rk(M)=2 R_K=0 mod (p)    N=29 p=59  rk(M)=27 R_K=0 mod (p)

N=2 p=13 rk(M)=0 R_K=0 mod (p)    N=4 p=29   rk(M)=2  R_K=0 mod (p)
N=2 p=31 rk(M)=0 R_K=0 mod (p)    N=4 p=37   rk(M)=2  R_K=0 mod (p)
N=4 p=13 rk(M)=1 R_K=0 mod (p)    N=8 p=521  rk(M)=6  R_K=0 mod (p)
```

4.4. **Conjecture about the p-torsion groups $\mathscr{T}_{\mathbb{Q}(N)}$.** The annihilation Theorem 4.6 allows us to test the non-triviality of the integer $\#\mathscr{T}_K = \#\mathscr{C}_K \cdot \#\mathscr{R}_K \cdot \#\mathscr{W}_K$, for $K := \mathbb{Q}(N)$, giving possible non-trivial class groups (see Lemma 2.1 about $\mathscr{W}_K$, in general trivial). More precisely, all computations or experiments depend on the relative components $\mathscr{T}_K^*$ whose orders are given by $\frac{1}{2}\,L_p(1,\psi_N)$, for ψ_N of order N of K.

Indeed, we do not see why $\#\mathscr{C}_K$ should be always trivial for an"algebraic reason", even if it is known that $\mathscr{R}_K$ may be, a priori, non-trivial whatever the order of magnitude of p. Moreover, an observation made in other contexts shows that, when $\#\mathscr{C}_K^* \cdot \#\mathscr{R}_K^*$ is non-trivial, the probability of $\#\mathscr{R}_K^* \neq 1$ is, roughly, p times that of $\#\mathscr{C}_K^* \neq 1$. The Cohen–Lenstra–Martinet heuristics (see [5, 46, 47] for large developments) give low probabilities for non-trivial p-class groups, even in the case of residue degree 1 of p in $\mathbb{Q}(\mu_N)$.

As for the question of p-rationality of number fields, when $K \subset \widehat{\mathbb{Q}}$ is fixed, the number of p such that $\#\mathscr{T}_K^* \equiv 0 \pmod p$ may be finite as we have conjectured; whence the rarity of these cases. Nevertheless, we propose the following conjecture claiming the infiniteness of non-trivial relative groups $\mathscr{T}_K^*$ when all parameters vary (i.e., the infiniteness of Table 6.2):

Conjecture 4.7. *There exist infinitely many pairs (N,p), $N \geq 2$, p prime, $p \nmid N$, such that $\frac{1}{2}\,L_p(1,\psi_N) \equiv 0 \pmod{\mathfrak{p}_N}$, for some $\mathfrak{p}_N \mid p$ in $\mathbb{Q}(\mu_N)$, where ψ_N is a character of $\mathbb{Q}(\mu_N)$ of order N (whence $\mathscr{T}_{\mathbb{Q}(N)}^* \neq 1$).*

We have seen that the solutions p to $\mathscr{T}_K^* \neq 1$, in the case $K = \mathbb{Q}(\ell^n)$, are mostly of the form $p = 1 + \lambda\,\ell^n$ giving, possibly, a class group of K roughly of order $O(\ell^n)$, which is very reasonable since the discriminant of K is such that $\sqrt{D_K} = (\ell^n)^{O(\ell^n)}$, whereas the class number fulfills the following general property $\#C_K \leq c_{\ell^n,\epsilon} \cdot (\sqrt{D_K})^{1+\epsilon}$ [1] and the ϵ-conjecture $\#C_K \leq c'_{\ell^n,\epsilon} \cdot (\sqrt{D_K})^{\epsilon}$.

Finally, if we assume that the p-class group $\mathscr{C}_K$ and the regulator $\mathscr{R}_K$ are random and independent, the Weber class number conjecture is possibly false for some $\ell_0^{n_0}$, p_0, the prime $\ell = 2$ being not specific.

5. Reflection theorem for p-class groups and p-torsion groups

Reflection theorem compares the p-class group $\mathscr{C}_K$ of K with a suitable component of the p-torsion group $\mathscr{T}_L$ of $L := K(\mu_p)$.

Put $\mathrm{rk}_p(A) := \dim_{\mathbb{F}_p}(A/A^p)$ for any abelian group A of finite type.

5.1. **Case $p = 2$.** Consider, once for all, the case $p = 2$ with $2 \nmid N$. The reflection theorem works in $K = \mathbb{Q}(N)$, with the trivial character; applied with the set S of prime ideals of K above 2, it is given by [17, Proposition III.4.2.2, § II.5.4.9.2], where $\mathfrak{m}^* = (4)$ and where $\mathscr{C}_K^{(4)}$ denotes a ray class group modulo (4). We have, in reflection theorems, the relation $\mathscr{T}_K^{\mathrm{res}} \simeq \mathscr{T}_K^{\mathrm{ord}} \bigoplus \mathbb{F}_2^N$ [17, Theorem III.4.1.5], valid under Leopoldt's conjecture for $p = 2$.

Theorem 5.1. *We have, in $K=\mathbb{Q}(N)$, for any odd $N>1$ and $p=2$:*

$$\begin{aligned}\mathrm{rk}_2(\mathscr{T}_K^{\mathrm{ord}}) &= \mathrm{rk}_2\big[\mathscr{C}_K^{\mathrm{res}}/cl_K^{\mathrm{res}}(S)\big]+\#S-1,\\ \mathrm{rk}_2(\mathscr{T}_K^{\mathrm{ord}}) &= \mathrm{rk}_2\big[\mathscr{C}_K^{\mathrm{ord}}/cl_K^{\mathrm{ord}}(S)\big]+\#S-1,\\ \mathrm{rk}_2(\mathscr{C}_K^{(4)\,\mathrm{ord}}) &= \mathrm{rk}_2(\mathscr{C}_K^{\mathrm{res}}),\end{aligned}$$

Thus, $\mathscr{T}_K^{\mathrm{ord}}=1$ (i.e., $\mathscr{C}_K^{\mathrm{ord}}=\mathscr{R}_K^{\mathrm{ord}}=\mathscr{W}_K^{\mathrm{ord}}=1$) if and only if 2 is inert in $K/\mathbb{Q}$ and $\mathscr{C}_K^{\mathrm{ord}}=1$ (or 2 is inert and $\mathscr{C}_K^{\mathrm{res}}=1$).

Remark 5.2. *Let $K=\mathbb{Q}(N)$, N odd. If $p=2$ is inert in K, $\mathrm{rk}_2(\mathscr{T}_K^{\mathrm{ord}})=\mathrm{rk}_2(\mathscr{C}_K^{\mathrm{res}})=\mathrm{rk}_2(\mathscr{C}_K^{\mathrm{ord}})$ (second and third formulas). This does not apply if N is divisible by $\ell=1093$, 3511 and primes ℓ such that $2^{\ell-1}\equiv 1 \pmod{\ell^2}$. For $\ell=1093$ and from $\mathrm{rk}_2(\mathscr{T}_K^{\mathrm{ord}})=\mathrm{rk}_2(\mathscr{C}_K^{\mathrm{ord}}/cl_K^{\mathrm{ord}}(S))+1092$, we have verified that the norm of $(1-\psi(3))\cdot\frac{1}{2}L_p(1,\psi)$ is exactly 2^{1092}; this means that 2 annihilates $\mathscr{T}_K^{\mathrm{ord}}$, whence that $\mathscr{C}_K^{S\,\mathrm{ord}}=1$ and that $\mathscr{T}_K^{\mathrm{ord}}\simeq(\mathbb{Z}/2\mathbb{Z})^{1092}$.*

5.2. **Case $p\neq 2$.** The application of the reflection theorem needs to consider $L=K\mathbb{Q}(\mu_p)$ for $K=\mathbb{Q}(N)$, $p\nmid N$, with the group $\mathrm{Gal}(L/K)$. Let $\omega_p=:\omega$ be the Teichmüller character. We denote by $\mathrm{rk}_\chi(A)$ the $\mathbb{F}_p$-dimension of the χ-component of A/A^p, $\chi\in\langle\omega\rangle$; whence $\mathrm{rk}_1(A)=\mathrm{rk}_p(A)$.
Since p is totally ramified in L/K one may denote S, by abuse, the sets of p-places of K and L, respectively; we then have $cl_L(S)\simeq cl_K(S)$.

Theorem 5.3. [17, § II.5.4.2 and Theorem II.5.4.5] *Let $p>2$ be a prime not dividing N and let $K:=\mathbb{Q}(N)$, $L:=K(\mu_p)$; put $\mathfrak{P}^*=(p)\cdot(1-\zeta_p)$ in L, where $\mathscr{C}_L^{\mathfrak{P}^*}$ is the ray class group of modulus $\mathfrak{P}^*$. We have:*

$$\begin{aligned}\mathrm{rk}_p(\mathscr{T}_K) &= \mathrm{rk}_\omega(\mathscr{C}_L),\\ \mathrm{rk}_p\big[\mathscr{C}_K/cl_K(S_K)\big] &= \mathrm{rk}_\omega(\mathscr{T}_L)+1-\#S_K,\\ \mathrm{rk}_p(\mathscr{C}_K) &= \mathrm{rk}_\omega(\mathscr{C}_L^{\mathfrak{P}^*})+1-N,\end{aligned}$$

5.3. **Illustration of reflection theorem for $N=\ell^n$, $p\neq 2$.** The parameter #zp gives the number $\ell^n(p-1)/2+1$ of $\mathbb{Z}_p$-extensions of L, but the cyclotomic extension of $\mathbb{Q}$ does not intervene because the conductor of $\mathbb{Q}(p)$ is p^2 larger that $\mathfrak{P}^*$; thus, #zp − 1 − rk(Hp) is the p-rank of the torsion part, where Hp is the ray class group $\mathscr{C}_L^{\mathfrak{P}^*}$ (e.g., $\ell=2$, $p=11,13,19$).

```
PROGRAM X. ILLUSTRATION OF FORMULA (8)
{el=2;for(n=1,3,print("el=",el," n=",n);if(el==2,P=x;for(j=1,n,P=P^2-2));
if(el!=2,P=polsubcyclo(el^(n+1),el^n));forprime(p=2,23,if(p==el,next);
Q=polcompositum(P,polcyclo(p))[1];L=bnfinit(Q,1);
r=el^n*(p-1)/2+1;A=idealfactor(L,p);d=matsize(A)[1];a=1;
for(k=1,d,a=idealmul(L,a,component(A,1)[k]));ap=idealpow(L,a,p);
Lp=bnrinit(L,ap);Hp=Lp.cyc;LT=List;e=matsize(Hp)[2];
R=0;for(k=1,e,c=Hp[e-k+1];w=valuation(c,p);if(w>0,R=R+1;
listinsert(LT,p^w,1)));print("p=",p," rk(Hp)=",R," #zp=",r," Hp=",LT)))}
el=2  n=1
p=3  rk(Hp)=2  #zp=3  Hp=[3,3]
p=5  rk(Hp)=4  #zp=5  Hp=[5,5,5,5]
p=7  rk(Hp)=6  #zp=7  Hp=[7,7,7,7,7,7]
p=11 rk(Hp)=11 #zp=11 Hp=[121,11,11,11,11,11,11,11,11,11,11]
p=13 rk(Hp)=13 #zp=13 Hp=[169,13,13,13,13,13,13,13,13,13,13,13,13]
p=17 rk(Hp)=16 #zp=17 Hp=[17,17,17,17,17,17,17,17,17,17,17,17,17,17,17,17]
p=19 rk(Hp)=19 #zp=19 Hp=[361,19,19,19,19,19,19,19,19,19,19,19,19,19,19,
                                                          19,19,19,19]
p=23 rk(Hp)=22 #zp=23 Hp=[23,23,23,23,23,23,23,23,23,23,23,23,23,23,23,
                                                    23,23,23,23,23,23,23]
el=2  n=2
p=3  rk(Hp)=4  #zp=5  Hp=[3,3,3,3]
```

```
p=5  rk(Hp)=9  #zp=9  Hp=[25,5,5,5,5,5,5,5,5]
p=7  rk(Hp)=12 #zp=13 Hp=[7,7,7,7,7,7,7,7,7,7,7,7]
p=11 rk(Hp)=21 #zp=21 Hp=[121,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,
                                                        11,11,11,11,11,11]
p=13 rk(Hp)=26 #zp=25 Hp=[169,169,13,13,13,13,13,13,13,13,13,13,13,13,13,13,
                                          13,13,13,13,13,13,13,13,13,13,13]
el=3  n=1
p=5  rk(Hp)=6  #zp=7  Hp=[5,5,5,5,5,5]
p=7  rk(Hp)=10 #zp=10 Hp=[49,7,7,7,7,7,7,7,7,7]
p=11 rk(Hp)=15 #zp=16 Hp=[11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11]
p=13 rk(Hp)=18 #zp=19 Hp=[13,13,13,13,13,13,13,13,13,13,13,13,13,13,13,13,
                                                              13,13,13]
p=17 rk(Hp)=24 #zp=25 Hp=[17,17,17,17,17,17,17,17,17,17,17,17,17,
                                       17,17,17,17,17,17,17,17,17,17,17,17]
p=19 rk(Hp)=27 #zp=28 Hp=[19,19,19,19,19,19,19,19,19,19,19,19,19,19,19,19,19,
                                       19,19,19,19,19,19,19,19,19,19,19,19]
el=3  n=2
p=5  rk(Hp)=18 #zp=19 Hp=[5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5]
p=7  rk(Hp)=28 #zp=28 Hp=[49,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,
                                                          7,7,7,7,7,7,7]
el=5 n=1
p=3  rk(Hp)=5  #zp=6  Hp=[3,3,3,3,3]
p=7  rk(Hp)=15 #zp=16 Hp=[7,7,7,7,7,7,7,7,7,7,7,7,7,7,7]
```

5.4. **Probabilistic analysis for $p > 2$.** Consider the following reflection theorem [17, II.5.4.9.2, formula (4)]:

Proposition 5.4. *Let $L = K(\mu_p)$, $p \nmid N$; we have $\mathrm{rk}_p(\mathscr{C}_K) = \mathrm{rk}_p(Y^\omega_{L,\mathrm{prim}})$, where $Y^\omega_{L,\mathrm{prim}} \subseteq Y^\omega_L := \big(\{\alpha \in L^\times, (\alpha) = \mathfrak{A}^p\} \cdot L^{\times p}/L^{\times p}\big)^\omega$ is the ω-component of the subset of p-primary elements α (i.e., such that $L(\sqrt[p]{\alpha})/L$ is unramified of degree p and decomposed into a cyclic extension of K in H^{nr}_K). Thus $\mathrm{rk}_p(\mathscr{C}_K) = \mathrm{rk}_p(\mathscr{C}^\omega_L)$ or $\mathrm{rk}_p(\mathscr{C}^\omega_L) - 1$.*

Proof. We have, from the general formula (loc. cit.):

$$\mathrm{rk}_p(\mathscr{C}_K) = \mathrm{rk}_p(\mathscr{C}^\omega_L) + 1 - \mathrm{rk}_p(Y^\omega_L) + \mathrm{rk}_p(Y^\omega_{L,\mathrm{prim}}).$$

Put $Y^\omega_L = \{\alpha_1, \ldots, \alpha_r\} \cup \{\zeta_p\}$ modulo $L^{\times p}$, the α_i being non-units and independent modulo $L^{\times p}$, and where r is the p-rank of $\mathscr{C}^\omega_L$. Since ζ_p is not p-primary, one gets $\mathrm{rk}_p(\mathscr{C}_K) = \mathrm{rk}_p(Y^\omega_{L,\mathrm{prim}}) = \mathrm{rk}_p(\langle \alpha_1, \ldots, \alpha_r\rangle_{\mathrm{prim}})$. Due to the p-adic action of ω on the α_i, it is immediate to deduce the last claim. □

The condition $\mathrm{rk}_p(\mathscr{C}_K) \geq 1$ is then equivalent to the existence of a p-primary $\alpha \in Y^\omega_L$ such that $(\alpha) = \mathfrak{A}^p$, with a non-principal $\mathfrak{A}$. Program X gives cases where necessarily $\mathrm{rk}_p(\mathscr{C}_L) = r \geq 1$ (probably $r = 1$, otherwise we should have $\mathrm{rk}_p(\mathscr{C}_K) = r$ or $r - 1 \neq 0$); one computes easily that the probability to have α p-primary (in a standard point of view) is $\frac{1}{p}$.

The computation of the class group of L is rapidly out of reach and we have only been able to compute $\mathscr{C}_L$ for $N = 3$ with $p = 7$ giving $\mathscr{C}_L \simeq \mathbb{Z}/7\mathbb{Z}$; we do not know α so that we cannot verify that it is not 7-primary (which is indeed the case since we know, from § 4.3, that $\mathscr{R}_K$ is not a 7-adic unit).

6. The p-torsion groups in the cyclotomic $\widehat{\mathbb{Z}}$-extension $\widehat{\mathbb{Q}}$

Since there exist many fields $k = \mathbb{Q}(\ell^n)$ with non-trivial p-torsion groups $\mathscr{T}_k$, these groups remain subgroups of $\mathscr{T}_K$ for any $K = \mathbb{Q}(N)$, extension of k in $\widehat{\mathbb{Q}}$, $N = \ell_1^{n_1} \cdots \ell_t^{n_t}$, and give larger groups. So we have essentially to compute $\mathscr{T}^*_K$ (the relative submodule), product of the components $\mathscr{T}^\theta_K$ for p-adic characters θ given by the characters ψ of order N of K (see § 2.4).

6.1. **General program.** The following completely general program uses the method of p-adic measure associated to the computation of Stickelberger's element for the composite conductor $f := pf_N$ of $K\mathbb{Q}(\mu_p)$, or $f = 4f_N$ if $p = 2$; the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q})$ is described by the program as direct product deduced from that of $(\mathbb{Z}/f\mathbb{Z})^\times$ as usual, using a half system of representatives Σ distinct from $[1, f/2]$ since it is not efficient to determine the Artin automorphism of a representative $a \in [1, f/2]$. All primes p are tested, which will give some cases of annihilators of degree > 1 (hence primes p of residue degree > 1 in $\mathbb{Q}(\mu_N)$).

The choice of c, defining the multiplier $1-c\cdot\left(\frac{\mathbb{Q}(\mu_f)}{c}\right)^{-1}$, gives some difficulty for N even since for N odd, $c = 2$ is always suitable (except in the rare known cases where 2 totally splits in $\mathbb{Q}(N)$, giving integers N out of reach). But c must be chosen for each p so that $\psi(c) \neq 1$, ψ of order N, which increases dramatically the computing time since the Artin symbol of c is not immediate; so, in the program, we only assume c prime to f. Doing this, the case $\psi(c) = 1$ may occur, giving $(1-\psi(c))\cdot\frac{1}{2}L_p(1,\psi) = 0$ in the relation of Lemma 4.3, while $L_p(1,\psi) \neq 0$; but $\psi(c)$ is a Nth root of unity and, by assumption, $p \nmid N$, so $1-\psi(c)$ non-invertible modulo p is equivalent to $\psi(c) = 1$; a unique example occurs for $N = 10$ (line * of the table) to be dropped since a direct verification via Program I (§ 2.5) does not give any solution p in the selected interval.

The p-adic characters θ are defined using a factorization modulo p of the Nth cyclotomic polynomial Q in polynomials $\mathsf{Rp[k]}$ in the list Rp; then the program tests the condition $\mathsf{S(x)} \equiv \mathsf{0} \pmod{\mathsf{Rp[k]}}$, where $\mathsf{S(x)}$ represents $\mathscr{A}_K'^c$ in the group algebra $\mathbb{Z}_p[x]$, x generating the Galois group.

Lemma 6.1. *When $\ell_1 = 2 \mid N$, let $f =: 2^{n_1+2}\cdot\ell_2^{n_2+1}\cdots\ell_t^{n_t+1}\cdot p =: 2^{n_1+2}\cdot f'$ be the conductor of $K(\mu_p)$. One can neglect, in the summation over $a \in [1, f]$ defining $\mathscr{A}^c_{\mathbb{Q}(\mu_f)} = (1+s_{-1})\,\mathscr{A}'^c_{\mathbb{Q}(\mu_f)}$, the component $\mathrm{Gal}(\mathbb{Q}(\mu_f)/k)$, where $k = \mathbb{Q}(2^{n_1})\mathbb{Q}(\mu_{f'})$. When N is odd one can use the representatives of $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell_1^{n_1+1}})/\mathbb{Q})$ modulo its complex conjugation.*

Proof. Let s be the generator of $\mathrm{Gal}(\mathbb{Q}(\mu_f)/k)$, s_{-1} the complex conjugation and $\sigma_a := \left(\frac{\mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q}}{a}\right)$. Let $\Sigma := \{a \in [1, f],\ \sigma_a \in \mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_4))\}$ be the set of representatives in $[1, f]$ used by the program, so that $[1, f] = \Sigma\cup\overline{\Sigma}$, where $\overline{\Sigma}$ represents $s\mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_4))$; then $\mathscr{A}^c_{\mathbb{Q}(\mu_f)} = \sum_{a\in\Sigma\cup\overline{\Sigma}}\lambda_a(c)a^{-1}\sigma_a$. Then $\Sigma\cup(f-\Sigma)$ is a partition of $[1, f]$ (s and s_{-1} project on $\mathrm{Gal}(\mathbb{Q}(\mu_4)/\mathbb{Q})$); thus $\mathscr{A}^c_{\mathbb{Q}(\mu_f)} = \sum_{a\in\Sigma\cup(f-\Sigma)}\lambda_a(c)a^{-1}\sigma_a$. Put $\mathscr{B}' := \sum_{a\in\Sigma}\lambda_a(c)a^{-1}\sigma_a$; then $(1+s_{-1})\cdot\mathscr{B}' \equiv \mathscr{A}^c_{\mathbb{Q}(\mu_f)} \pmod p$ (Lemma 3.1). Since $\mathscr{A}^c_{\mathbb{Q}(\mu_f)} = (1+s_{-1})\,\mathscr{A}'^c_{\mathbb{Q}(\mu_f)}$, one deduces that $\mathscr{A}'^c_{\mathbb{Q}(\mu_f)} \equiv \mathscr{B}'$ modulo the ideal $((1-s_{-1}), p)$; whence the claim since ψ is even. The case of odd N is obvious. □

Then we shall perform some verifications by using the basic Programs I, II, § 2.5, when computation via $\mathsf{K} = \mathsf{bnfinit(P)}$ is possible, which holds only for small conductors contrary to the present method allowing computations up to $N = 400$ and beyond, with large primes p without any more memory. But the standard method gives the structure of $\mathscr{T}_K$ contrary to the present one, only giving the annihilator of $\mathscr{T}_K^*$ modulo p.

The instruction $\mathsf{if(Mod(p, N)! = 1, next)}$ only considers primes p totally split in $\mathbb{Q}(\mu_N)$ (faster, but eliminates cases with annihilators of degree > 1); the instructions which follows only consider primes p totally split in K (these parts have been suppressed in the writing but may be restored). Otherwise, the program tests all primes (case of the table obtained below). The program may give the polynomial P defining $K = \mathbb{Q}(N)$.

To simplify the use by the reader and to reduce the execution time, the program considers two cases (N even and N odd) and deals with 4 possibilities corresponding to the number dim of divisors of N so that the program can work for $2 \le N \le 2309$. The bound $\mathsf{Bp} = \mathsf{floor}(2 * 10^5/\mathsf{N})$ for p may be modified at will. The variables fN and $\mathsf{f} = \mathsf{p} * \mathsf{fN}$ denote the conductors of K and $K(\mu_p)$, respectively.

```
PROGRAM XI. ANNIHILATORS OF T*, FOR ALL N >1
{BN=500;for(N=2,BN,Bp=floor(2*10^5/N);dim=omega(N);Q=polcyclo(N);
Lq=List;LQ=List;Lh=List;LH=List;LN=List;divN=factor(N);
D=component(divN,1);Exp=component(divN,2);
if(Mod(N,2)==0,delta=1;fN=1;
q1=D[1]^Exp[1];listput(Lq,q1,1);Q1=4*q1;listput(LQ,Q1,1);
N1=N/q1;listput(LN,N1,1);fN=fN*Q1;
h1=Mod(5,Q1);listput(Lh,h1,1);listput(LH,lift(h1),1);
for(i=2,dim,qi=D[i]^Exp[i];listput(Lq,qi,i);Qi=qi*D[i];
listput(LQ,Qi,i);fN=fN*Qi;Ni=N/qi;listput(LN,Ni,i);
hi=znprimroot(Qi);listput(Lh,hi,i);listput(LH,lift(Lh[i]),i)));
if(Mod(N,2)!=0,C=2;delta=2;fN=1;
for(i=1,dim,qi=D[i]^Exp[i];listput(Lq,qi,i);Qi=qi*D[i];
listput(LQ,Qi,i);fN=fN*Qi;Ni=N/qi;listput(LN,Ni,i);
hi=znprimroot(LQ[i]);listput(Lh,hi,i);listput(LH,lift(hi),i)));
\\polynomial of Q(N):
\\if(Mod(N,2)==0,P=x;for(i=1,Exp[1],P=P^2-2);for(i=2,dim,
\\P=polcompositum(P,polsubcyclo(LQ[i],Lq[i]))[1]);print("N=",N," P=",P));
\\if(Mod(N,2)!=0,P=x;for(i=1,dim,
\\P=polcompositum(P,polsubcyclo(LQ[i],Lq[i]))[1]);print("N=",N," P=",P));
if(dim>=1,E1=eulerphi(LQ[1])/delta);if(dim>=2,E2=eulerphi(LQ[2]));
if(dim>=3,E3=eulerphi(LQ[3]));if(dim>=4,E4=eulerphi(LQ[4]));
forprime(p=3,Bp,if(Mod(N,p)==0,next);
\\Specifies the primes p totally split in Q(mu_N):
\\if(Mod(p,N)!=1,next);
\\Specifies the primes p totally split in Q(N):
\\if(Mod(N,2)==0,w1=valuation(p^2-1,2);if(Exp[1]+3>w1,next);
\\for(j=2,dim,wj=valuation(p^(D[j]-1)-1,D[j]);if(Exp[j]+1>wj,next(2))));
\\if(Mod(N,2)!=0,
\\for(j=1,dim,wj=valuation(p^(D[j]-1)-1,D[j]);if(Exp[j]+1>wj,next(2))));
g=znprimroot(p);G=lift(g);gm=g^-1;
f=p*fN;M=f/p;E=lift(Mod((1-G)*p^-1,M));G=G+E*p;g=Mod(G,f);
for(j=1,dim,M=f/LQ[j];E=lift(Mod((1-LH[j])*LQ[j]^-1,M));
H=LH[j]+E*LQ[j];listput(Lh,Mod(H,f),j));
if(Mod(N,2)==0,Cc=2;while(gcd(Cc,f)!=1,Cc=Cc+1);C=Cc;cm=Mod(C,f)^-1);
if(Mod(N,2)!=0,C=2;cm=Mod(C,f)^-1);
F=factor(Q+O(p));R=lift(component(F,1));d=matsize(F)[1];Rp=List;
for(j=1,d,listput(Rp,R[j]*Mod(1,p),j));Qp=Q*Mod(1,p);gg=1;ggm=1;hh=1;S=0;
if(dim==1,
for(u1=1,E1,hh=hh*Lh[1];t=0;
for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh*gg);A=lift(a*cm);
t=t+(A*C-a)/f*ggm);e=lift(Mod(u1*LN[1],N));
S=S+lift(t)*x^e);S=S*Mod(1,p);S=lift(Mod(S,Qp));for(k=1,d,Rk=Rp[k];
if(Mod(S,Rk)==0,print("N=",N," p=",p," annihilator = ",Rk))));
if(dim==2,
for(u1=1,E1,hh=hh*Lh[1];for(u2=1,E2,hh=hh*Lh[2];
t=0;for(v=1,p-1,gg=gg*g;ggm=ggm*gm;
a=lift(hh*gg);A=lift(a*cm);
t=t+(A*C-a)/f*ggm);e=lift(Mod(u1*LN[1]+u2*LN[2],N));
S=S+lift(t)*x^e));S=S*Mod(1,p);S=lift(Mod(S,Qp));for(k=1,d,Rk=Rp[k];
if(Mod(S,Rk)==0,print("N=",N," p=",p," annihilator = ",Rk))));
if(dim==3,
for(u1=1,E1,hh=hh*Lh[1];for(u2=1,E2,hh=hh*Lh[2];
for(u3=1,E3,hh=hh*Lh[3];t=0;
for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh*gg);A=lift(a*cm);
t=t+(A*C-a)/f*ggm);e=lift(Mod(u1*LN[1]+u2*LN[2]+u3*LN[3],N));
S=S+lift(t)*x^e)));S=S*Mod(1,p);S=lift(Mod(S,Qp));for(k=1,d,Rk=Rp[k];
if(Mod(S,Rk)==0,print("N=",N," p=",p," annihilator = ",Rk))));
if(dim==4,
for(u1=1,E1,hh=hh*Lh[1];for(u2=1,E2,hh=hh*Lh[2];
for(u3=1,E3,hh=hh*Lh[3];for(u4=1,E4,hh=hh*Lh[4];t=0;
```

```
for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh*gg);A=lift(a*cm);
t=t+(A*C-a)/f*ggm);e=lift(Mod(u1*LN[1]+u2*LN[2]+u3*LN[3]+u4*LN[4],N));
S=S+lift(t)*x^e))));S=S*Mod(1,p);S=lift(Mod(S,Qp));for(k=1,d,Rk=Rp[k];
if(Mod(S,Rk)==0,print("N=",N," p=",p," annihilator = ",Rk))))))}
```

6.2. **Table of non-trivial $\mathscr{T}^{\theta}_{\mathbb{Q}(N)}$.** Let σ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$, $K := \mathbb{Q}(N)$, $N \geq 2$. To simplify notations, (a,p) means $\mathsf{Mod}(\mathsf{a},\mathsf{p})$; an annihilator $f(x)$ gives the Galois action $\tau^{f(\sigma)} = 1$ in $\mathscr{T}_K/\mathscr{T}_K^p$ and defines a p-adic character θ (θ above ψ of order N) for which $\mathscr{T}_K^{\theta} \neq 1$ (recall that the order and the annihilation of $\mathscr{T}_K^{\theta}$ is given by $\frac{1}{2}L_p(1,\psi)$). For instance, the two informations:

$$\mathsf{N}=2,\ \mathsf{p}=13,\ (1,13)*\mathsf{x}+(1,13) \text{ and } \mathsf{N}=4,\ \mathsf{p}=13,\ (1,13)*\mathsf{x}+(5,13)$$

are related to characters θ of orders 2 and 4, for which the $\mathscr{T}^{\theta}_{\mathbb{Q}(N)}$ are non-trivial (see the complete structure of $\mathscr{T}_{\mathbb{Q}(4)}$ in the table of Program II, § 2.5).

```
            ANNIHILATORS mod p
 N=2   p=13   (1,13)*x+(1,13)
 N=2   p=31   (1,31)*x+(1,31)
 N=3   p=7    (1,7)*x+(5,7)
 N=3   p=73   (1,73)*x+(9,73)
 N=4   p=13   (1,13)*x+(5,13)
 N=4   p=29   (1,29)*x+(12,29)
 N=4   p=37   (1,37)*x+(31,37)
 N=5   p=11   (1,11)*x+(7,11)
 N=5   p=11   (1,11)*x+(8,11)
 N=6   p=7    (1,7)*x+(2,7)
 N=6   p=13   (1,13)*x+(9,13)
 N=6   p=43   (1,43)*x+(36,43)
 N=8   p=3    (1,3)*x^2+(1,3)*x+(2,3)
 N=8   p=521  (1,521)*x+(206,521)
*N=10  p=3    (1,3)*x^4+(2,3)*x^3
             +(1,3)*x^2+(2,3)*x+(1,3)
 N=12  p=13   (1,13)*x+(7,13)
 N=14  p=113  (1,113)*x+(106,113)
 N=15  p=31   (1,31)*x+(11,31)
 N=15  p=31   (1,31)*x+(22,31)
 N=15  p=241  (1,241)*x+(81,241)
 N=15  p=1291 (1,1291)*x+(958,1291)
 N=17  p=239  (1,239)*x+(172,239)
 N=18  p=37   (1,37)*x+(33,37)
 N=22  p=397  (1,397)*x+(16,397)
 N=22  p=2729 (1,2729)*x+(1268,2729)
 N=23  p=47   (1,47)*x+(19,47)
 N=25  p=101  (1,101)*x+(21,101)
 N=25  p=1151 (1,1151)*x+(744,1151)
 N=25  p=2251 (1,2251)*x+(1033,2251)
 N=27  p=109  (1,109)*x+(20,109)
 N=28  p=701  (1,701)*x+(338,701)
 N=29  p=59   (1,59)*x+(56,59)
 N=30  p=1831 (1,1831)*x+(261,1831)
 N=33  p=397  (1,397)*x+(136,397)
 N=38  p=2357 (1,2357)*x+(659,2357)
 N=39  p=157  (1,157)*x+(44,157)
 N=40  p=41   (1,41)*x+(22,41)
 N=40  p=41   (1,41)*x+(30,41)
 N=40  p=41   (1,41)*x+(35,41)
 N=43  p=173  (1,173)*x+(41,173)
 N=45  p=541  (1,541)*x+(336,541)
 N=47  p=283  (1,283)*x+(27,283)
 N=48  p=193  (1,193)*x+(28,193)
 N=50  p=101  (1,101)*x+(88,101)

                ANNIHILATORS mod p
 N=128 p=641  (1,641)*x+(287,641)
 N=129 p=257  (1,257)*x^2
               +(81,257)*x+(1,257)
 N=136 p=137  (1,137)*x+(35,137)
 N=138 p=139  (1,139)*x+(31,139)
 N=140 p=29   (1,29)*x^2
                +(3,29)*x+(5,29)
 N=144 p=433  (1,433)*x+(292,433)
 N=153 p=307  (1,307)*x+(178,307)
 N=155 p=311  (1,311)*x+(203,311)
 N=156 p=157  (1,157)*x+(80,157)
 N=172 p=173  (1,173)*x+(143,173)
 N=174 p=349  (1,349)*x+(16,349)
 N=178 p=179  (1,179)*x+(129,179)
 N=190 p=761  (1,761)*x+(94,761)
 N=191 p=383  (1,383)*x+(315,383)
 N=191 p=383  (1,383)*x+(360,383)
 N=192 p=193  (1,193)*x+(115,193)
 SOLUTIONS p<10*N SPLIT IN Q(mu_N):
 N=210 p=211  (1,211)*x+(59,211)
 N=210 p=211  (1,211)*x+(154,211)
 N=215 p=431  (1,431)*x+(74,431)
 N=215 p=1721 (1,1721)*x+(162,1721)
 N=225 p=1801 (1,1801)*x+(1536,1801)
 N=226 p=227  (1,227)*x+(160,227)
 N=230 p=691  (1,691)*x+(345,691)
 N=230 p=1381 (1,1381)*x+(144,1381)
 N=234 p=1171 (1,1171)*x+(988,1171)
 N=236 p=1181 (1,1181)*x+(939,1181)
 N=240 p=241  (1,241)*x+(110,241)
 N=242 p=2179 (1,2179)*x+(1976,2179)
 N=249 p=499  (1,499)*x+(242,499)
 N=261 p=2089 (1,2089)*x+(1080,2089)
 N=265 p=1061 (1,1061)*x+(919,1061)
 N=276 p=277  (1,277)*x+(272,277)
 N=281 p=563  (1,563)*x+(551,563)
 N=284 p=2557 (1,2557)*x+(1876,2557)
 N=288 p=1153 (1,1153)*x+(428,1153)
 N=288 p=1153 (1,1153)*x+(577,1153)
 N=290 p=1451 (1,1451)*x+(135,1451)
 N=292 p=877  (1,877)*x+(405,877)
 N=293 p=587  (1,587)*x+(323,587)
 N=296 p=593  (1,593)*x+(447,593)
 N=296 p=1481 (1,1481)*x+(444,1481)
 N=303 p=607  (1,607)*x+(59,607)
```

```
N=50  p=251  (1,251)*x+(123,251)
N=50  p=1201 (1,1201)*x+(493,1201)
N=52  p=53   (1,53)*x+(12,53)
N=52  p=53   (1,53)*x+(21,53)
N=52  p=53   (1,53)*x+(27,53)
N=52  p=157  (1,157)*x+(128,157)
N=54  p=163  (1,163)*x+(21,163)
N=56  p=13   (1,13)*x^2
              +(5,13)*x+(5,13)
N=60  p=61   (1,61)*x+(43,61)
N=63  p=379  (1,379)*x+(302,379)
N=64  p=193  (1,193)*x+(160,193)
N=66  p=1321 (1,1321)*x+(617,1321)
N=67  p=269  (1,269)*x+(176,269)
N=67  p=269  (1,269)*x+(208,269)
N=69  p=829  (1,829)*x+(532,829)
N=70  p=71   (1,71)*x+(40,71)
N=70  p=211  (1,211)*x+(76,211)
N=72  p=73   (1,73)*x+(28,73)
N=80  p=241  (1,241)*x+(124,241)
N=81  p=487  (1,487)*x+(287,487)
N=83  p=499  (1,499)*x+(312,499)
N=84  p=757  (1,757)*x+(685,757)
N=86  p=431  (1,431)*x+(145,431)
N=87  p=349  (1,349)*x+(157,349)
N=87  p=523  (1,523)*x+(62,523)
N=88  p=353  (1,353)*x+(17,353)
N=93  p=373  (1,373)*x+(307,373)
N=95  p=191  (1,191)*x+(132,191)
N=95  p=191  (1,191)*x+(137,191)
N=99  p=991  (1,991)*x+(91,991)
N=99  p=991  (1,991)*x+(818,991)
N=100 p=199  (1,199)*x^2
            +(173,199)*x+(1,199)
N=101 p=607  (1,607)*x+(277,607)
N=101 p=607  (1,607)*x+(514,607)
N=102 p=103  (1,103)*x+(83,103)
N=102 p=103  (1,103)*x+(97,103)
N=104 p=937  (1,937)*x+(609,937)
N=106 p=107  (1,107)*x+(39,107)
N=106 p=107  (1,107)*x+(61,107)
N=107 p=857  (1,857)*x+(263,857)
N=108 p=109  (1,109)*x+(24,109)
N=111 p=223  (1,223)*x+(176,223)
N=115 p=461  (1,461)*x+(87,461)
N=115 p=461  (1,461)*x+(103,461)
N=118 p=709  (1,709)*x+(27,709)
N=124 p=5    (1,5)*x^3+(2,5)*x^2
                 +(2,5)*x+(3,5)
N=124 p=373  (1,373)*x+(139,373)
N=124 p=373  (1,373)*x+(340,373)
N=126 p=379  (1,379)*x+(165,379)
N=128 p=257  (1,257)*x+(113,257)
N=303 p=607  (1,607)*x+(564,607)
N=306 p=307  (1,307)*x+(7,307)
N=306 p=919  (1,919)*x+(81,919)
N=307 p=1229 (1,1229)*x+(121,1229)
N=309 p=619  (1,619)*x+(32,619)
N=315 p=631  (1,631)*x+(346,631)
N=321 p=643  (1,643)*x+(520,643)
N=324 p=2269 (1,2269)*x+(1878,2269)
N=324 p=2593 (1,2593)*x+(1526,2593)
N=328 p=2953 (1,2953)*x+(2160,2953)
N=330 p=331  (1,331)*x+(46,331)
N=330 p=331  (1,331)*x+(110,331)
N=335 p=2011 (1,2011)*x+(919,2011)
N=340 p=1021 (1,1021)*x+(417,1021)
N=340 p=1021 (1,1021)*x+(993,1021)
N=340 p=2381 (1,2381)*x+(1143,2381)
N=344 p=1721 (1,1721)*x+(939,1721)
N=345 p=1381 (1,1381)*x+(502,1381)
N=346 p=2423 (1,2423)*x+(2301,2423)
N=348 p=349  (1,349)*x+(132,349)
N=352 p=353  (1,353)*x+(238,353)
N=358 p=359  (1,359)*x+(111,359)
N=358 p=359  (1,359)*x+(240,359)
N=362 p=1087 (1,1087)*x+(172,1087)
N=363 p=1453 (1,1453)*x+(1416,1453)
N=363 p=2179 (1,2179)*x+(18,2179)
N=368 p=3313 (1,3313)*x+(2536,3313)
N=375 p=751  (1,751)*x+(335,751)
N=382 p=383  (1,383)*x+(23,383)
N=386 p=1931 (1,1931)*x+(1315,1931)
N=388 p=389  (1,389)*x+(233,389)
N=388 p=1553 (1,1553)*x+(421,1553)
N=388 p=1553 (1,1553)*x+(464,1553)
N=395 p=2371 (1,2371)*x+(2137,2371)
N=400 p=401  (1,401)*x+(294,401)
N=401 p=3209 (1,3209)*x+(154,3209)
N=401 p=4813 (1,4813)*x+(3529,4813)
N=405 p=811  (1,811)*x+(645,811)
N=407 p=3257 (1,3257)*x+(894,3257)
N=407 p=3257 (1,3257)*x+(2268,3257)
N=408 p=409  (1,409)*x+(370,409)
N=412 p=1237 (1,1237)*x+(387,1237)
N=420 p=421  (1,421)*x+(367,421)
N=422 p=2111 (1,2111)*x+(615,2111)
N=427 p=1709 (1,1709)*x+(922,1709)
N=428 p=857  (1,857)*x+(31,857)
N=429 p=3433 (1,3433)*x+(702,3433)
N=430 p=1291 (1,1291)*x+(1091,1291)
N=431 p=863  (1,863)*x+(406,863)
N=431 p=863  (1,863)*x+(754,863)
N=432 p=3889 (1,3889)*x+(2110,3889)
N=442 p=443  (1,443)*x+(325,443)
N=443 p=887  (1,887)*x+(226,887)
```

Remark 6.2. *One knows a unique example of the form* $p \mid \#\mathscr{C}_{\mathbb{Q}(N)}$ *for* $p \nmid N$ *with the data* $p = 107$, $N = 2 \cdot 53$ *(Aoki–Fukuda [2]). This value of* N *does appear in the table with two annihilators* $\mathsf{Mod}(1, 107) * \mathsf{x} + \mathsf{Mod}(39, 107)$, $\mathsf{Mod}(1, 107) * \mathsf{x} + \mathsf{Mod}(61, 107)$*; we ignore the contributions for* $\mathscr{C}_K$ *and* $\mathscr{R}_K$.

We observe that many values of N give more than one annihilator; they are perhaps good candidates for similar examples, even if all combinations are possible (including the cases of a unique annihilator).

For instance, the fields $K=\mathbb{Q}(5)$ and $\mathbb{Q}(15)$ give rise to two annihilators, which is specified by the structure $\mathscr{T}_K\simeq(\mathbb{Z}/11\mathbb{Z})^2$ and $\mathscr{T}_K\simeq(\mathbb{Z}/31\mathbb{Z})^2$, but we compute that $\mathscr{C}_K=1$ in these cases. In [37] it is proved that for $\ell<131,109,101$, the 3-class group of $\mathbb{Q}(\ell^\infty)$ is trivial for $p=7,11,13$, respectively. This confirms that for $N=5$, $p=11$, $\mathscr{T}_K=\mathscr{R}_K\simeq(\mathbb{Z}/11\mathbb{Z})^2$. The next examples in the table are $(N,p)=(40,41)$, $(52,53)$, $(67,269)$, $(95,191)$, $(99,991)$, etc. It would be interesting to test these fields.

Let's give some verifications, using Program I § 2.5, computing independently the structure of $\mathscr{T}_K$; only very small N can be tested because of the instructions $\mathsf{K}=\mathsf{bnfinit}(\mathsf{P})$ and $\mathsf{KpEx}=\mathsf{bnrinit}(\mathsf{K},\mathsf{p}^{\mathsf{Ex}})$, where the defining polynomial P may be obtained with Program XI above; the structure obtained for $\mathscr{T}_K$ depends on that of the subfields of K, while Program XI only gives the p-rank of $\mathscr{T}_K^*$.

For instance, the case $N=8$, $p=3$, with the annihilator $3\,x^2+x+2 \pmod p$ is the first annihilator of degree >1; since (from the table) $\mathscr{T}_K$ is annihilated by the relative norm $x^4+1\equiv(x^2+x+2)(x^2+2x+2)\,(\mathrm{mod}\ 3)$ and since 3 is totally inert, the result gives at least a 3-rank 2. This is validated as $\mathsf{N}=8,\ \mathsf{p}=3,\ \mathsf{rk}(\mathsf{T})=2,\ \mathsf{T}=\mathsf{List}([3,3])$.

```
PROGRAM XII. STRUCTURE OF T IN SOME Q(N) AND VERIFICATIONS WITH PROGRAM I:
Field K=Q(5)  T=[11,11]
Field K=Q(6)  T=[7,7] T=[13,13] T=[31] T=[43] T=[73]
Field K=Q(12) T=[9,9] T=[7,7] T=[169,169,13,13] T=[29] T=[31] T=[37]
                                                T=[43] T=[73]
Field K=Q(14) T=[13] T=[31] T=[113]
Field K=Q(15) T=[7] T=[11,11] T=[31,31] T=[73]
Field K=Q(21) T=[49,7]
Field K=Q(30) T=[7,7] T=[11,11] T=[13,13] T=[31,31,31] T=[43] T=[73]
Field K=Q(42) T=[49,49,7,7] T=[13,13]
```

The composite $K=\mathbb{Q}(42)$ has some interest for $p=7$ since $\mathscr{T}_K\simeq(\mathbb{Z}/7\mathbb{Z})^2$; so we know that $\mathscr{T}_K^{\mathrm{Gal}(K/k)}\simeq\mathscr{T}_k$, where $k=\mathbb{Q}(6)$; but with $\mathscr{T}_K\simeq(\mathbb{Z}/7\mathbb{Z})^2\times(\mathbb{Z}/7^2\mathbb{Z})^2$, showing that for p-ramification aspects, genus theory gives often increasing p-torsion groups contrary to p-class groups as we shall see in the next Section. Since $\mathrm{N}_{K/k}(\mathscr{T}_K)=\mathscr{T}_k$, we have $\mathscr{T}_K^*\simeq(\mathbb{Z}/7^2\mathbb{Z})^2$. Note that the case $N=42$ does not appear in the table because of the condition $p\nmid N$ which will be the framework of genus theory in $\mathbb{Q}(N)\mathbb{Q}(p^\infty)$.

7. Genus theory and p-class groups in $\widehat{\mathbb{Q}}$

We consider, in the cyclotomic $\widehat{\mathbb{Z}}$-extension $\widehat{\mathbb{Q}}$, any subfield of finite or infinite degree, and fix a prime p (see [50] for analytic results of non-divisibility in this context).

7.1. **Definition of $\widehat{\mathbb{Q}}^*$.** The pro-cyclic extension $\widehat{\mathbb{Q}}$ is the direct composite over $\mathbb{Q}$ of $\mathbb{Q}(p^\infty)$ and the composite $\widehat{\mathbb{Q}}^*$ of all the $\mathbb{Q}(\ell^\infty)$, for $\ell\neq p$. Two cases then arise: that of the p-class groups of $K=\mathbb{Q}(N)$ when $p\nmid N$ and the case of fields written as composite $K_m=K\mathbb{Q}(p^m)$, $K\subset\widehat{\mathbb{Q}}^*$, $m\geq1$.

In the first case, we are in a generalization of Weber's problem. In the second one the problem is related to genus theory, whence to Greenberg's conjecture [30], for which one very strongly admits that $\#\mathscr{C}_{K\mathbb{Q}(p^m)}$ is constant for all $m\gg0$ (i.e., the invariants λ,μ of K for the prime p are zero); see for instance [10, 29, 43] for some developments. But we have:

Proposition 7.1. *Let $K=\mathbb{Q}(N)\subset\widehat{\mathbb{Q}}^*$ (i.e., $p\nmid N$); let $K_m=K\mathbb{Q}(p^m)$ for any $m\geq0$. Then, under Leopoldt's conjecture, $\mathscr{T}_{K_m}=1$, if and only if $\mathscr{T}_K=1$. Thus, a necessary condition to get $\mathscr{C}_{K_m}\neq1$ (for some $m\geq0$) is $\mathscr{T}_K\neq1$, which brings into play the general Table 6.2.*

Proof. Since K_m/K is a p-ramified p-extension, the claim comes from the fixed points formula giving $\mathscr{T}_{K_m}^{\mathrm{Gal}(K_m/K)} \simeq \mathscr{T}_K$ ([17, Theorem IV.3.3], [20, Proposition 6], [28, Appendix A.4.2]). □

We shall study the reciprocal aspects in the next subsection to result ultimately in Theorem 7.5.

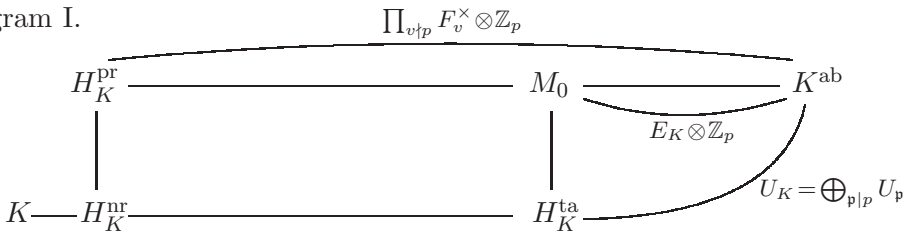
7.2. **The p-class group of K_m – Fundamental relation with $\mathscr{R}_K$.** The analog of Weber's problem in $\widehat{\mathbb{Q}}$ is, a priori, doubtful because of Chevalley's formula in an extension K_m/K, $K \subset \widehat{\mathbb{Q}}^*$, $K_m = K\mathbb{Q}(p^m)$:

$$\#(\mathscr{C}\ell_{K_m}^{\mathrm{res}})^{\mathrm{Gal}(K_m/K)} = \#\mathscr{C}\ell_K^{\mathrm{res}} \cdot \frac{p^{m\,(s_p-1)}}{(E_K^{\mathrm{pos}} : E_K^{\mathrm{pos}} \cap \mathrm{N}_{K_m/K}(K_m^\times))},$$

where $s_p := \#S$, the number of p-places. So $\mathscr{C}\ell_{K_m}^{\mathrm{res}} = 1$ as soon as $\mathscr{C}\ell_K^{\mathrm{res}} = 1$ and $s_p = 1$. If $s_p > 1$, the right factor may be a power of p only depending on the normic properties of E_K^{pos} in K_m/K.

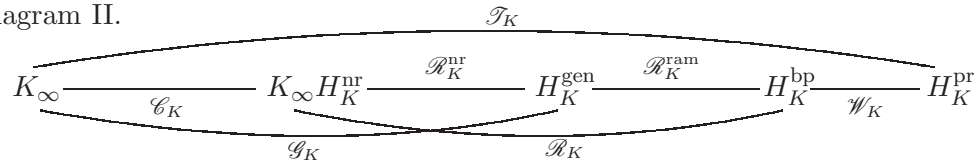
Consider the two diagrams [17, § III.4.4.1] and [29, Diagrams 2 and 3] (under the Leopoldt conjecture), where K^{ab} is the maximal abelian pro-p-extension of K:

Diagram I.



where F_v is the residue field of the tame place v (finite or infinite). We know that, in an idelic framework, the fixed field of $U_K = \bigoplus_{\mathfrak{p}|p} U_{\mathfrak{p}}$ is the maximal tame sub-extension H_K^{ta}, since each $U_{\mathfrak{p}}$ is the inertia group of $\mathfrak{p}$ in K^{ab}/K. From Diagram I, the restriction of U_K to $\mathrm{Gal}(H_K^{\mathrm{pr}}/K)$ is $\mathrm{Gal}(H_K^{\mathrm{pr}}/H_K^{\mathrm{nr}}) \simeq U_K/\iota_p(E_K \otimes \mathbb{Z}_p)$ whose torsion group is $\mathrm{Gal}(H_K^{\mathrm{pr}}/K_\infty H_K^{\mathrm{nr}})$.

Diagram II.



with $\mathscr{G}_K := \mathrm{Gal}(H_K^{\mathrm{gen}}/K_\infty)$, where H_K^{gen} is the union, over m, of the genus fields $H_{K_m/K}$ (maximal abelian p-extensions of K, unramified over K_m; then $[H_{K_m/K} : K_m] = \#\mathscr{C}\ell_{K_m}^g$ for $g := \mathrm{Gal}(K_m/K)$); it follows that H_K^{gen} is the maximal unramified extension of K_∞ in H_K^{pr} [29, Proposition 3.6] and that:

$$\#\mathscr{G}_K = \#\mathscr{C}\ell_K \frac{p^{m\,(s_p-1)}}{(E_K^{\mathrm{pos}} : E_K^{\mathrm{pos}} \cap \mathrm{N}_{K_m/K}(K_m^\times))} = \#\mathscr{C}\ell_{K_m}^g, \text{ for } m \text{ large enough} \tag{2}$$

The inertia groups, in $H_K^{\mathrm{pr}}/K_\infty$, of the p-places are the torsion parts of the images of the $U_{\mathfrak{p}}$, then are isomorphic to $\mathrm{tor}_{\mathbb{Z}_p}(U_{\mathfrak{p}}/\iota_p(E_K \otimes \mathbb{Z}_p) \cap U_{\mathfrak{p}})$. So, the subgroup $\mathscr{I}_K$ of $\mathscr{T}_K$ generated by these inertia groups fixes H_K^{gen}. We then have the following result (under Leopoldt's conjecture) which will be fundamental for the search of non-trivial $\mathscr{C}\ell_{K_m}^{\mathrm{res}}$:

Lemma 7.2. *Let p be totally split in $K = \mathbb{Q}(N)$, $N \neq 1$. The Galois group $\mathscr{I}_K$ generated by the inertia groups $\mathrm{tor}_{\mathbb{Z}_p}(U_{\mathfrak{p}}/\iota_p(E_K \otimes \mathbb{Z}_p) \cap U_{\mathfrak{p}})$ is isomorphic to $\mathscr{W}_K$, trivial for $p \neq 2$, isomorphic to $\mathbb{F}_2^{N-1}$ for $p = 2$ (Lemma 2.1). Thus $\mathscr{R}_K^{\mathrm{ram}} = 1$, $\mathscr{R}_K^{\mathrm{nr}} = \mathscr{R}_K$ and $\#\mathscr{G}_K = \#\mathscr{C}\ell_K \#\mathscr{R}_K$ (cf. Diagram II).*

Proof. Let $\varepsilon \in E_K \otimes \mathbb{Z}_p$ be such that the diagonal image $\iota_p(\varepsilon)$ in U_K is $\iota_p(\varepsilon) = (\iota_{\mathfrak{p}}(\varepsilon), 1, \ldots, 1)$. Since the global norm $\mathrm{N}_{K/\mathbb{Q}}$ is the product of the local norms at the p-places (thus identities), and since $\mathrm{N}_{K/\mathbb{Q}}(\varepsilon) = \pm(1, \ldots, 1)$, this yields $\iota_{\mathfrak{p}}(\varepsilon) = 1$ (since $N > 1$), then $\iota_p(\varepsilon) = 1$ and $\varepsilon = 1$ (Leopoldt's conjecture) and the claim for $p \neq 2$. For $p = 2$, $\mathrm{tor}_{\mathbb{Z}_2}(U_{\mathfrak{p}}/\iota_2(E_K \otimes \mathbb{Z}_2) \cap U_{\mathfrak{p}}) = \mathrm{tor}_{\mathbb{Z}_2}(U_{\mathfrak{p}}) = \mu_2$; since the image of $\mathrm{tor}_{\mathbb{Z}_2}(U_K)$ is $\mathscr{W}_K$, we have $\mathscr{I}_K \supseteq \mathscr{W}_K$ but since the image of -1 in U_K (as global unit) is trivial, this gets the equality $\mathscr{I}_K = \mathscr{W}_K$. □

The following result gives an important simplification in the context of Greenberg's conjecture in the totally split case [30, Theorem 2, § 4], and explains why examples with $\mathscr{C}_{K_m} \neq 1$ will take place in the above totally split case of p in K (Theorem 7.5 and Corollary 7.6):

Lemma 7.3. *Let p be a prime and let $K = \mathbb{Q}(N) \subset \widehat{\mathbb{Q}}^*$ (i.e., $p \nmid N$). We assume that $\mathscr{C}_K = 1$. Let $K' \subseteq K$ be the splitting field of p in K.*
Let $K_m := K\mathbb{Q}(p^m)$, $K'_m := K'\mathbb{Q}(p^m)$, $m \geq 0$. Then $\mathscr{C}_{K_m} = 1$ if and only if $\mathscr{C}_{K'_m} = 1$. Therefore, $\lambda = \mu = \nu = 0$ if and only if $\lambda' = \mu' = \nu' = 0$ in terms of Iwasawa's invariants in K_∞ and K'_∞, respectively.

Proof. Let $g := \mathrm{Gal}(K_m/K)$; since $\mathscr{C}_K = 1$, the Chevalley formulas become:

$$\#\mathscr{C}_{K_m}^{\,g} = \frac{p^{m\,(s_p-1)}}{(E_K^{\mathrm{pos}} : E_K^{\mathrm{pos}} \cap \mathrm{N}_{K_m/K}(K_m^\times))} \text{ and } \#\mathscr{C}_{K'_m}^{\,g} = \frac{p^{m\,(s_p-1)}}{(E_{K'}^{\mathrm{pos}} : E_{K'}^{\mathrm{pos}} \cap \mathrm{N}_{K'_m/K'}(K_m'^\times))}$$

since $s_p = [K' : \mathbb{Q}]$ is the same in the two formulas.
The map $E_{K'}^{\mathrm{pos}}/E_{K'}^{\mathrm{pos}} \cap \mathrm{N}_{K'_m/K'}(K_m'^\times) \to E_K^{\mathrm{pos}}/E_K^{\mathrm{pos}} \cap \mathrm{N}_{K_m/K}(K_m^\times)$ is injective; indeed, with obvious notations, if $\varepsilon' = \mathrm{N}_{K_m/K}(y)$, $y \in K_m^\times$, then using N_{K_m/K'_m}, one gets $\varepsilon'^{[K:K']} = \mathrm{N}_{K'_m/K'}(y')$, $y' \in K_m'^\times$. The result follows since $[K : K']$ is prime to p.
So $(E_{K'}^{\mathrm{pos}} : E_{K'}^{\mathrm{pos}} \cap \mathrm{N}_{K'_m/K'}(K_m'^\times)) \leq (E_K^{\mathrm{pos}} : E_K^{\mathrm{pos}} \cap \mathrm{N}_{K_m/K}(K_m^\times))$, whence $\#\mathscr{C}_{K'_m}^{\,g} \geq \#\mathscr{C}_{K_m}^{\,g}$; but the map $\mathscr{C}_{K'_m} \to \mathscr{C}_{K_m}$ is injective since $[K_m : K'_m]$ is prime to p, and we get $\mathscr{C}_{K_m}^{\,g} \simeq \mathscr{C}_{K'_m}^{\,g}$. Whence easily the claims. □

The following result may be considered as a corollary to Lemma 7.2 (cf. [22, Theorem 4.7], [27, Section 3], [29, Proposition 3.3, Theorem 1] for more information after the pioneering work of Taya [58, Theorem 1.1]):

Lemma 7.4. *Let $K = \mathbb{Q}(N) \subset \widehat{\mathbb{Q}}^*$ (i.e., $p \nmid N$) and let $K_m := K\mathbb{Q}(p^m)$. Then the integer $\dfrac{p^{m\,(s_p-1)}}{(E_K^{\mathrm{pos}} : E_K^{\mathrm{pos}} \cap \mathrm{N}_{K_m/K}(K_m^\times))}$ divides $\#\mathscr{R}_K^{\mathrm{nr}}$. If p totally splits in K, then for all m large enough there is equality with $\#\mathscr{R}_K^{\mathrm{nr}} = \#\mathscr{R}_K$ (cf. Diagram II).*

From Lemma 7.2, 7.3, 7.4, we get the following genus theory characterization, of practical use, in the framework of the notion of p-rationality:

Theorem 7.5. *Let $p > 2$ be totally split in $K = \mathbb{Q}(N)$. Then, there exists $m \geq 0$, such that $\mathscr{C}_{K_m} \neq 1$, if and only if $\mathscr{T}_K \neq 1$ (i.e., K is not p-rational). For $p = 2$, the condition becomes $\mathscr{T}_K/\mathscr{W}_K \neq 1$.*

Proof. Let $g = \mathrm{Gal}(K_m/K)$. If $\mathscr{C}_{K_m} \neq 1$ for some m, then $\mathscr{C}_{K_m}^{\,g} \neq 1$, whence $\mathscr{T}_K \neq 1$ from (2) and Diagram II. Assume $\mathscr{T}_K \neq 1$; if $\mathscr{C}_K \neq 1$, then $\mathscr{C}_{K_m}^{\,g} \neq 1$, otherwise, if $\mathscr{C}_K = 1$, then $\mathscr{R}_K \neq 1$ and for m large enough, $\#\mathscr{C}_{K_m}^{\,g} = \#\mathscr{G}_K = \#\mathscr{R}_K^{\mathrm{nr}} = \#\mathscr{R}_K = \#\mathscr{T}_K$. □

Corollary 7.6. *The table 6.2, restricted to primes p totally split in K, gives the following list of $\mathscr{C}_{K_1} \neq 1$, in the selected intervals for N, p:*

```
N=2     p=31       annihilator = Mod(1,31)*x+Mod(1,31)
N=2     p=1546463  annihilator = Mod(1,1546463)*x+Mod(1,1546463)
N=2^8   p=18433    annihilator = Mod(1, 18433)*x + Mod(9723, 18433)
N=2^10  p=114689   annihilator = Mod(1,114689)*x+Mod(66688,114689)
N=3     p=73       annihilator = Mod(1,73)*x+Mod(9,73)
```

```
N=3^4   p=487      annihilator = Mod(1,487)*x+Mod(287,487)
N=3^4   p=238627   annihilator = Mod(1,238627)*x+Mod(106366,238627)
N=5^2   p=2251     annihilator = Mod(1,2251)*x+Mod(1033,2251)
```

In fact the literature does contain these few counterexamples (see Coates [9, Section 3], relating results from Fukuda–Komatsu, Horie [34, 35, 13, 14]). Note that $N = 3^4$, $p = 238627$, needs, with Program XI, $\mathsf{time} = 52,869\mathsf{ms}$ and that $N = 2^{10}$, $p = 114689$, needs $\mathsf{time} = 5\mathsf{min}, 30, 507\mathsf{ms}$. We shall examine these cases and try to find others or to become aware of the rarity of them. We will also do checks, using another process, even if it's useless, by computing Hasse's normic symbols, in K_m/K, of the units of K, using the "product formula" of class field theory, since (assuming $\mathscr{C}\ell_K^{\rm res} = 1$), the condition $\mathscr{C}\ell_{K_m}^{\rm res} \neq 1$ is equivalent to $\dfrac{p^{m\,(s_p-1)}}{(E_K^{\rm pos} : E_K^{\rm pos} \cap {\rm N}_{K_m/K}(K_m^\times))} \neq 1$. This will be equivalent to the computation of the rank of a $\mathbb{F}_p$-matrix.

7.3. **Non-p-principalities in p-extensions.** Let $K = \mathbb{Q}(N)$ and let $p \nmid N$ totally split in $K/\mathbb{Q}$; since the case $p = 2$, totally split in K, is out of reach of the programs we implicitly assume $p > 2$ with the ordinary senses for classes and units. Let $K_1 := K\mathbb{Q}(p)$; we have to compute $(E_K : E_K \cap {\rm N}_{K_1/K})$. To avoid the instruction $\mathsf{bnfinit(P)}$, unfeasible for $N > 17$, we shall use the cyclotomic units [59, Lemma 8.1 (a)] giving E_K assuming the base field K principal, then use the local normic Hasse's symbols. Then, following the practical method described in [17, II.4.4.3], the normic symbol $(\varepsilon, K_1/K)_{\mathfrak{p}}$ for a unit $\varepsilon \in E_K$ and a ramified p-place $\mathfrak{p}$, requires to find α such that (the conductor being p^2):

$$\alpha \equiv \varepsilon \pmod{\mathfrak{p}^2}, \quad \alpha \equiv 1 \pmod{(p\,\mathfrak{p}^{-1})^2}. \tag{3}$$

Then (α) is an ideal, prime to p, whose Artin symbol in ${\rm Gal}(K_1/K)$ characterizes the normic symbol; its image in ${\rm Gal}(\mathbb{Q}(p)/\mathbb{Q})$ is given by the Artin symbol of ${\rm N}_{K_1/\mathbb{Q}(p)}(\alpha)$, seen in $(\mathbb{Z}/p^2\mathbb{Z})^\times$.

The program, written with $N = \ell^n$, may be generalized using Program XI. One must precise el and n; if the rank is strictly less than $\ell^n - 1$ (taking into account the "product formula") then $(E_K : E_K \cap {\rm N}_{K_1/K}(K_1^\times)) < p^{\ell^n-1}$, whence $\mathscr{C}\ell_{K_1}$ non-trivial. The variables $\mathsf{m1}, \mathsf{m2}$ denote the modulus $\mathfrak{p}^2$ and $(p\,\mathfrak{p}^{-1})^2$, the variable $\mathsf{m} = \mathsf{m1} + \mathsf{m2}$ allows congruence (3) for α (in Z). Thus one computes the $\mathbb{F}_p$-rank (in rkM) of the matrix M. A sufficient precision must be chosen to compute P as irreducible polynomial of the generating real cyclotomic unit deduced from $\mathsf{u} = \mathsf{z} + \mathsf{z}^{-1}$, where $\mathsf{z} = \mathsf{exp}(2 * \mathsf{I} * \mathsf{Pi}/\mathsf{f})$; thus the instruction $\mathsf{e} = \mathsf{nfgaloisconj(P)}$ gives the conjugates as polynomials of u.

```
PROGRAM XIII. RANK OF THE MATRIX OF NORMIC SYMBOLS FOR el^n ODD
{el=3;n=3;N=el^n;f=el^(n+1);z=exp(2*I*Pi/f);
rho=znprimroot(f);h=rho^N;H=rho^(el-1);
P=1;for(k=1,N,c=lift(H^k);u=1;for(j=1,(el-1)/2,a=lift(c*h^j);
u=u*(z^a+z^-a));P=P*(x-u));P=round(P);e=nfgaloisconj(P);
\\p=487;\\ Choice of a special prime p or of an interval:
forprime(p=2,2*10^5,w=valuation(p^(el-1)-1,el);if(w<n+1,next);
g=znprimroot(p^2);
for(aa=1,p-1,t=norm(Mod(x-aa,P));vt=valuation(t,p);if(vt==1,a=aa;break));
A=List;for(k=1,N,listput(A,e[k]-a,k));W=List;for(j=1,N,E=Mod(e[j],P);
V=List;for(k=1,N,m1=Mod(A[k],P);m2=norm(m1)/m1;
m1=m1^2;m2=m2^2;m=m1+m2;Z=E+(1-E)*m1/m;ZZ=lift(Z);
\\This part replace Z (very huge) by a suitable integer residue:
Num=numerator(ZZ);Num0=0;for(i=0,N-1,c=polcoeff(Num,i);if(c==0,next);
v=valuation(c,p);if(v>=0,c=lift(Mod(c,p^2)));
if(v<0,c=p^v*lift(Mod(c*p^-v,p^(2-v))));
Num0=Num0+c*x^i);Num=Num0;Den=denominator(ZZ);if(Den!=1,
Den0=0;for(i=0,N-1,c=polcoeff(Den,i);if(c==0,next);
v=valuation(c,p);if(v>=0,c=lift(Mod(c,p^2)));
if(v<0,c=p^v*lift(Mod(c*p^-v,p^(2-v))));
```

```
Den0=Den0+c*x^i);Den=Den0);Z=Mod(Num,P)*Mod(Den,P)^-1;
No=Mod(norm(Z),p^2);Ln=Mod(znlog(No,g),p);
listput(V,Ln));listput(W,V));M=matrix(N,N,u,v,W[u][v]);rk=matrank(M);
if(rk<N-1,print("N=",N," p=",p," rk(M)=",rk));if(rk==N-1,
print("N=",N," control: ","p=",p," vt=",vt," root=",a," rk(M)=",rk))
)\\ End of interval p
}
PROGRAM XIV. RANK OF THE MATRIX OF NORMIC SYMBOLS FOR 2^n
{el=2;n=4;N=el^n;f=el^(n+2);z=exp(2*I*Pi/f);H=Mod(5,f);
P=1;for(j=1,N,c=lift(H^j);u=z^(-2*c)*(1-z^(5*c))/(1-z^c);P=P*(x-u));
P=round(P);e=nfgaloisconj(P);
\\p=18433;\\ Choice of a special prime p or of an interval:
forprime(p=2,2*10^5,w=valuation(p^2-1,2);if(w<n+3,next);
g=znprimroot(p^2);
for(aa=1,p-1,t=norm(Mod(x-aa,P));vt=valuation(t,p);if(vt==1,a=aa;break));
A=List;for(k=1,N,listput(A,e[k]-a,k));W=List;for(j=1,N,E=Mod(e[j],P);
V=List;for(k=1,N,m1=Mod(A[k],P);m2=norm(m1)/m1;
m1=m1^2;m2=m2^2;m=m1+m2;Z=E+(1-E)*m1/m;ZZ=lift(Z);
\\ This part replace Z (very huge) by a suitable integer residue:
Num=numerator(ZZ);Num0=0;for(i=0,N-1,c=polcoeff(Num,i);if(c==0,next);
v=valuation(c,p);if(v>=0,c=lift(Mod(c,p^2)));
if(v<0,c=p^v*lift(Mod(c*p^-v,p^(2-v))));
Num0=Num0+c*x^i);Num=Num0;Den=denominator(ZZ);if(Den!=1,
Den0=0;for(i=0,N-1,c=polcoeff(Den,i);if(c==0,next);
v=valuation(c,p);if(v>=0,c=lift(Mod(c,p^2)));
if(v<0,c=p^v*lift(Mod(c*p^-v,p^(2-v))));
Den0=Den0+c*x^i);Den=Den0);Z=Mod(Num,P)*Mod(Den,P)^-1;
No=Mod(norm(Z),p^2);Ln=Mod(znlog(No,g),p);listput(V,Ln));
listput(W,V));M=matrix(N,N,u,v,W[u][v]);rk=matrank(M);
if(rk<N-1,print("N=",N," p=",p,"  rk(M)=",rk));if(rk==N-1,
print("N=",N," control: ","p=",p," vt=",vt," root=",a," rk(M)=",rk))
)\\ End of interval p
}
N=2  p=31      rk(M)=0     N=3    p=73  rk(M)=1     N=5^2  p=2251 rk(M)=23
N=2  p=1546463 rk(M)=0     N=3^4  p=487 rk(M)=79
```

For these known counterexamples, $\#\mathscr{T}_K = p$, which indicates that $\#\mathscr{R}_K = p$ since $\mathscr{C}_K = 1$. The case $\ell = 3$, $n = 1$, $p = 73$ may be elucidate in more details: the units are $(\varepsilon_1 = x^2 + x - 1, \varepsilon_2 = x - 1)$ and fulfill the relation $(\varepsilon_1^{33} \cdot \varepsilon_2^5)^{72} \equiv 1 + 73^2 \cdot (2\,x^2 + 59\,x + 69) \pmod{73^3}$, with $2\,x^2 + 59\,x + 69 \in \mathfrak{p} \mid 73$. Thus the inertia groups $\mathrm{tor}_{\mathbb{Z}_{73}}(U_{\mathfrak{p}_i}/\overline{E}_K \cap U_{\mathfrak{p}_i})$, $i = 1, 2, 3$, are trivial, giving $\mathscr{R}_K^{\mathrm{ram}} = 1$, $\mathscr{R}_K^{\mathrm{nr}} = \mathscr{R}_K = \mathscr{T}_K$, as expected. In the case $\ell = 5$, $n = 2$, $p = 2251$ totally splits in $K/\mathbb{Q}$; some computations in E_K/E_K^{2251} (of order 2251^{24}) indicate, as expected, that $(\varepsilon_i)^{2250} = 1 + 2251 \cdot \alpha_i$, with non-independent α_i modulo 2251, which implies, as above, the existence of a unit local pth power (hence local norm), but not in E_K^p.

This shows that a direct p-adic computation on the units is hopeless contrary to that of local norm symbols. We have performed such computations in large intervals without finding new solutions. This enforces [9, Conjecture D] in $\widehat{\mathbb{Q}}$ and our philosophy about the p-rationality in general.

More precisely, if one considers heuristics in the Borell–Cantelli style, using standard probabilities $\frac{1}{p}$, we have, possibly, infinitely many examples, but this does not seem realistic; in [21, Conjecture 8.4.], we have given extensive calculations and justifications of an opposite situation giving, as for the well-known Fermat quotients of small integers 2, 3,... some other probabilities, for any regulator of algebraic numbers, suggesting solutions finite in number with the particularity of giving very few solutions.

7.4. **Behavior of the logarithmic class groups in $\widehat{\mathbb{Q}}$.** The following results of Jaulent is perhaps a key to understand some phenomena in $\widehat{\mathbb{Q}}$, regarding Greenberg's conjecture:

Theorem 7.7. [42, Theorem 4.5, Remarques]. *Let $K = \mathbb{Q}(N) \subset \widehat{\mathbb{Q}}^*$, for some prime p, let $m \geq 0$ and $K_m = K\mathbb{Q}(p^m)$. Under the Leopoldt and Gross–Kuz'min conjectures for p, $\widetilde{\mathscr{C}}_{K_m} = 1$ if and only if $\widetilde{\mathscr{C}}_K = 1$.*

Theorem 7.8. [44, Théorème 17], [22, Théorème 3.4]. *Let p be totally split in K. A sufficient condition to have $\widetilde{\mathscr{C}}_K = 1$ is that $\mathscr{C}_K = cl_K(S)$ and $(E_K^S : E_K^S \cap \mathrm{N}_{K_1/K}(K_1^\times)) = p^{N-1}$, where E_K^S is the group of S-units of K.*

Remark 7.9. *Assume moreover that $\mathscr{C}_K = 1$ and to simplify that $\mathscr{R}_K = p$, in other words $(E_K : E_K \cap \mathrm{N}_{K_1/K}(K_1^\times)) = p^{N-2}$ (thus $\#\mathscr{C}_{K_1}^g = p$) as are the known numerical examples. Then E_K^S is of the form $E_K \bigoplus \langle \pi_1, \ldots, \pi_N \rangle$, the π_i being the generators of the $\mathfrak{p}_i \mid p$. This supposes that the group of norm symbols of $\langle \pi_1, \ldots, \pi_N \rangle$ is contained in that of E_K (of $\mathbb{F}_p$-dimension $N-2$), which is of low probability.*

These results give many cases of triviality and we know that $\widetilde{\mathscr{C}}_K = 1$ implies that Greenberg's conjecture holds true in K_∞ for obvious reason. We have no counterexamples (for all $N < 30$ and $p \in [2, 2 \cdot 10^5]$; one may use the following program (give ℓ, n, p):

```
PROGRAM XV. COMPUTATION OF LOGARITHMIC CLASS GROUPS
{el=3;n=1;p=73;if(el==2,P=x;for(i=1,n,P=P^2-2));
if(el!=2,P=polsubcyclo(el^(n+1),el^n));K=bnfinit(P,1);cl=K.no;
clog=bnflog(K,p);print("N=",el^n," p=",p," cl=",cl," clog=",clog)}

el=2  p=31  cl=1 clog=[[],[],[]]        el=3  p=73  cl=1 clog=[[],[],[]]
```

So, even if for $K_1 = K\,\mathbb{Q}(31) = \mathbb{Q}(2)\,\mathbb{Q}(31)$ $(p = 31)$ and $K_1 = K\,\mathbb{Q}(73) = \mathbb{Q}(3)\,\mathbb{Q}(73)$ $(p = 73)$, the class groups $\mathscr{C}_{K_1}$ are non-trivial, the logarithmic class groups $\widetilde{\mathscr{C}}_{K_1}$ are trivial.

8. Conclusion and questions

Genus theory (Theorem 7.5, Corollary 7.6) have succeeded to give few non-trivial p-class groups of *composite subfields* $\mathbb{Q}(pN)$ of $\widehat{\mathbb{Q}}$, but there are not enough computations to give more precise heuristics. This invites to ask for some questions about the arithmetic properties of $\widehat{\mathbb{Q}}$:

(i) Let p be a fixed prime number. It is clear that p is totally ramified in $\widehat{\mathbb{Q}}/\widehat{\mathbb{Q}}^*$; thus the Frobenius of p in $\widehat{\mathbb{Q}}^*/\mathbb{Q}$ fixes a field D_p such that p totally splits in $D_p/\mathbb{Q}$. An out of reach question is the finiteness (or not) of D_p which can be written $\mathbb{Q}(\mathscr{L}^{\mathscr{N}})$, $\mathscr{L} = \{\ell_1, \ldots, \ell_t, \ldots\}$, $\mathscr{N} = \{n_1, \ldots, n_t, \ldots\}$, with an obvious meaning. Since the number ℓ^{g_p} of prime ideals above p in a single $\mathbb{Z}_\ell$-extension $\mathbb{Q}(\ell^\infty)$ is finite, the integers $n_\ell \in \mathscr{N}$ are finite but not necessarily $\mathscr{L}$.

For example, if $p = 2$, the only known primes ℓ such that 2 splits in part in $\mathbb{Q}(\ell^\infty)$ are 1093 and 3511; so if there is no other case, the decomposition field of 2 in $\widehat{\mathbb{Q}}/\mathbb{Q}$ should be $D_2 = \mathbb{Q}(1093 \cdot 3511)$.

Is the decomposition group of p in $\widehat{\mathbb{Q}}/\mathbb{Q}$ of finite index in $\mathrm{Gal}(\widehat{\mathbb{Q}}/\mathbb{Q})$? This is the conjecture given in [21, Conjecture 8.4]. Of course, taking a prime of the form $p = 1 + \lambda\, q_1^{a_1} \cdots q_s^{a_s}$, with primes q_i, $a_i \geq 2$, gives unbounded indices since p splits in $\mathbb{Q}(q_1^{a_1-1} \cdots q_s^{a_s-1})$.

(ii) Let $K = \mathbb{Q}(N)$ and for any $p \nmid N$, let $s_p = \#S$. Let $K_m = K\,\mathbb{Q}(p^m)$ for $m \gg 0$ such that $\dfrac{p^{m\,(s_p-1)}}{(E_K^{\mathrm{pos}} : E_K^{\mathrm{pos}} \cap \mathrm{N}_{K_m/K}(K_m^\times))} = \#\mathscr{R}_K^{\mathrm{nr}}$ (Lemma 7.4); is the set of p, such that $\mathscr{R}_K^{\mathrm{nr}} \neq 1$, finite in number ? If so, this gives new feature about the units in $\widehat{\mathbb{Q}}$ and is also related to Greenberg's conjecture in $\widehat{\mathbb{Q}}$.

(iii) In the two cases, $\ell^n = 2^8$, $p = 18433 \equiv 1 \pmod{2^{11}}$ and $\ell = 2^{10}$, $p = 114689 \equiv 1 \pmod{2^{14}}$, then $\mathscr{C}_K = 1$, $\mathscr{T}_K \neq 1$ (Programs of § 4.1 and § 4.2), p totally splits in K and then

$\#\mathscr{C}_{K_1}$ is non-trivial from Theorem 7.5; it is divisible by $\dfrac{p^{\ell^n-1}}{(E_K : E_K \cap \mathrm{N}_{K_1/K}(K_1^\times))}$ and it will be useful to verify, but this takes too much time to compute the norm index. The computations have been done in [2, 40, 14, 15], but, to our knowledge, no program is available. [2] What is the order of the logarithmic class group $\widetilde{\mathscr{C}}_K$ for these cases of too large degrees ?

(iv) Let $K = \mathbb{Q}(N)$ and $K_m = K\mathbb{Q}(p^m)$, for all $m \geq 0$; what are the Iwasawa invariants of $\varprojlim_m \mathscr{T}_{K_m}$?

(v) In [57] Silverman proves, after some other contributions (Cusick, Pohst, Remak), a general inequality between R_K (classical real regulator) and D_K (discriminant) of the form $R_K > c_K(\log(\gamma_K|D_K|))^{O([K:\mathbb{Q}])}$. A p-adic equivalent would give a solution of many questions in number theory, as a proof of Leopoldt's conjecture! However, we have proposed, in [25, Conjecture 8.2] a "folk conjecture" about $\#\mathscr{T}_K$, which applies to $\mathscr{R}_K$, equal to $\mathscr{T}_K$ for all p large enough, and justified by extensive computations:

Conjecture 8.1. *Let $\mathscr{K}$ be the set of totally real number fields; for $K \in \mathscr{K}$, let D_K be its discriminant and let $\mathscr{R}_K := \mathrm{tor}_{\mathbb{Z}_p}(\log(U_K)/\log(\overline{E}_K))$ be its normalized p-adic regulator (see § 2.1). There exists a constant $C_p > 0$ such that $\log_\infty(\#\mathscr{R}_K) \leq \log_\infty(\#\mathscr{T}_K) \leq C_p \cdot \log_\infty(\sqrt{|D_K|})$, for all $K \in \mathscr{K}$, where $\log_\infty$ is the complex logarithm. Possibly, C_p is independent of p.*

References

[1] N.C. Ankeny, R. Brauer, S. Chowla, A note on the class numbers of algebraic number fields, Amer. J. Math. **78** (1956), 51–61. https://doi.org/10.2307/2372483 13

[2] M. Aoki, T. Fukuda, An algorithm for computing p-class groups of abelian number fields, Lecture Notes in Computer Science, **4076** (2006), 56–71. https://doi.org/10.1007/11792086_5 2, 19, 26

[3] G. Boeckle, D.-A. Guiraud, S. Kalyanswamy, C. Khare, Wieferich Primes and a mod p Leopoldt Conjecture (2018). https://arxiv.org/pdf/1805.00131 4

[4] K. Belabas, J.-F. Jaulent, The logarithmic class group package in PARI/GP, Pub. Math. Besançon (Théorie des Nombres) (2016), 5–18. http://pmb.univ-fcomte.fr/2016/pmb_2016.pdf 7

[5] J. Buhler, C. Pomerance, L. Robertson, Heuristics for class numbers of prime-power real cyclotomic fields, In: High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of H.C. Williams, Fields Inst. Commun. **41**, Amer. Math. Soc., Providence, RI (2004), pp. 149–157.2, 6, 13 http://dx.doi.org/10.1090/fic/041

[6] J.-P. Cerri, De l'Euclidianité de $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ et $\mathbb{Q}(\sqrt{2+\sqrt{2+\sqrt{2}}})$ pour la norme, Journal de Théorie des Nombres de Bordeaux **12**(1) (2000), 103–126.2 http://www.numdam.org/item/JTNB_2000__12_1_103_0/

[7] C. Chevalley, Sur la théorie du corps de classes dans les corps finis et les corps locaux. Thèse no. 155, Jour. of the Faculty of Sciences Tokyo **2** (1933), 365–476.5 http://www.numdam.org/issue/THESE_1934__155__365_0.pdf

[8] J. Coates, p-adic L-functions and Iwasawa's theory, Algebraic number fields: L-functions and Galois properties, In: Sympos., Univ. Durham, Durham 1975, pp. 269-353. Academic Press, London, 1977. 5

[9] J. Coates, The enigmatic Tate–Shafarevich group, In: Fifth International Congress of Chinese Mathematicians, Parts 1, AMS/IP Stud. Adv. Math., vol. 2, 51(1), Amer. Math. Soc., Providence, RI, 2012, pp. 43–50. https://doi.org/10.1090/amsip/051.1 4, 23, 24

[10] T. Fukuda, K. Komatsu, On $\mathbb{Z}_p$-extensions of real quadratic fields, J. Math. Soc. Japan **38**(1) (1986), 95–102. https://doi.org/10.2969/jmsj/03810095 2, 6, 20

[11] T. Fukuda, K. Komatsu, Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, Experiment. Math. **18** (2009), 213–222. https://doi.org/10.1080/10586458.2009.10128896 2, 6

[12] T. Fukuda, K. Komatsu, Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, II, Journal de Théorie des Nombres de Bordeaux **22**(2) (2010), 359–368. https://doi.org/10.5802/jtnb.720 2

[2] I warmly thank Takayuki Morisawa for sending me his conference paper (loc.cit.), not so easy to find for me, but which contains all the bibliographical and numerical information that we revisit in our paper, especially summarized in Fukuda's lecture [15]. The results, $31 \mid h(2\cdot 31)$, $73 \mid h(3\cdot 73)$ (Horie 2001), $31 \mid h(2\cdot 31)$, $1546463 \mid h(2\cdot 1546463)$, $73 \mid h(3\cdot 73)$ (Fukuda, Komatsu 2011), $18433 \mid h(2^8\cdot 18433)$, $114689 \mid h(2^{10}\cdot 114689)$, $487 \mid h(3^4\cdot 487)$, $238627 \mid h(3^4\cdot 238627)$, $2251 \mid h(5^2\cdot 2251)$ (Fukuda, Komatsu, Morisawa 2011), $107 \mid h(2\cdot 53)$ (Fukuda 2011) were announced in various articles and conferences.

[13] T. Fukuda, K. Komatsu, Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, III, Int. J. Number Theory **7**(6) (2011), 1627–1635. https://doi.org/10.1142/S1793042111004782 2, 23
[14] T. Fukuda, K. Komatsu, T. Morisawa, Weber's class number one problem: Iwasawa Theory 2012, In: Contrib. Math. Comput. Sci., vol. **7**, Springer, Heidelberg, 2014.2, 6, 23, 26 https://doi.org/10.1007/978-3-642-55245-8_6
[15] T. Fukuda, Class Number Calculation of Special Number Fields, Exposé au Séminaire de Théorie des nombres de Bordeaux (2018).2, 26 https://lfant.math.u-bordeaux.fr/seminar/slides/2018-03-06T10:00--Takashi_Fukuda.pdf
[16] T. Fukuda, New PARI functions around abelian number fields 12th Atelier PARI/GP, University of Bordeaux (2019). https://pari.math.u-bordeaux.fr/Events/PARI2019/talks/takashi.pdf 2
[17] G. Gras, *Class Field Theory: from theory to practice*, corr. 2nd ed. Springer Monographs in Mathematics, Springer, xiii+507 pages (2005). 3, 4, 5, 13, 14, 15, 21, 23
[18] G. Gras, Sur l'annulation en 2 des classes relatives des corps abéliens, C.R. Math. Rep. Acad. Sci. Canada **1**(2) (1978), 107–110. https://mr.math.ca/article/sur-lannulation 9
[19] G. Gras, Sur la construction des fonctions L p-adiques abéliennes, Sém. Delange–Pisot–Poitou (Théorie des nombres) **20**(2) (1978–1979), Exposé no. 22, 1–20.9 http://www.numdam.org/item?id=SDPP_1978-1979__20_2_A1_0
[20] G. Gras, Remarks on K_2 of number fields, J. Number Theory **23**(3) (1986), 322–335.4, 5, 21 https://doi.org/10.1016/0022-314X(86)90077-6
[21] G. Gras, Les θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques, Canadian J. Math. **68**(3) (2016), 571–624. http://dx.doi.org/10.4153/CJM-2015-026-3 4, 5, 6, 24, 25
English translation: Local θ-regulators of an algebraic number: p-adic Conjectures (2017). https://arxiv.org/pdf/1701.02618
[22] G. Gras, Approche p-adique de la conjecture de Greenberg pour les corps totalement réels, Ann. Math. Blaise Pascal, **24**(2) (2017), 235–291. http://ambp.cedram.org/item?id=AMBP_2017__24_2_235_0 22, 25
[23] G. Gras, Annihilation of $\mathrm{tor}_{\mathbb{Z}_p}(\mathscr{G}_{K,S}^{\mathrm{ab}})$ for real abelian extensions $K/\mathbb{Q}$, Communications in Advanced Mathematical Sciences **I**(1) (2018), 5–34.9, 10 https://dergipark.org.tr/en/download/article-file/543993
[24] G. Gras, The p-adic Kummer–Leopoldt Constant: Normalized p-adic Regulator, Int. J. of Number Theory **14**(2) (2018), 329–337. https://doi.org/10.1142/S1793042118500203 5
[25] G. Gras, Heuristics and conjectures in the direction of a p-adic Brauer–Siegel theorem, Math. Comp. **88**(318) (2019), 1929–1965. https://doi.org/10.1090/mcom/3395 26
[26] G. Gras, On p-rationality of number fields. Applications–PARI/GP programs, Pub. Math. Besançon (Théorie des Nombres) (2019). https://pmb.centre-mersenne.org/article/PMB_2019___2_29_0.pdf 7
[27] G. Gras, Normes d'idéaux dans la tour cyclotomique et conjecture de Greenberg, Annales mathématiques du Québec (Online: 17 October 2018), **43** (2019), 249–280.22 https://doi.org/10.1007/s40316-018-0108-3
[28] G. Gras, Practice of the Incomplete p-Ramification Over a Number Field – History of Abelian p-Ramification, Communications in Advanced Mathematical Sciences **2**(4) (2019), 251–280. https://doi.org/10.33434/cams.573729 4, 5, 21
[29] G. Gras, Greenberg's conjecture for totally real number fields in terms of algorithmic complexity. https://arxiv.org/abs/2004.06959 4, 7, 20, 21, 22
[30] R. Greenberg, On the Iwasawa invariants of totally real number fields, Amer. J. Math. **98**(1) (1976), 263–284. https://doi.org/10.2307/2373625 4, 20, 22
[31] C. Greither, Class groups of abelian fields, and the Main Conjecture, Ann. Inst. Fourier (Grenoble) **42**(3) (1992), 449–499. https://doi.org/10.5802/aif.1299 9
[32] F. Hajir, C. Maire, R. Ramakrishna, On the Shafarevich Group of Restricted Ramification Extensions of Number Fields in the Tame Case, Indiana University Math Journal (to appear).4 https://arxiv.org/abs/1909.03689
[33] F. Hajir, C.Maire, R. Ramakrishna, Cutting towers of number fields.https://members.femto-st.fr/sites/femto-st.fr.christian-maire/files/content/fichiers/cutting_towers_june01 4
[34] K. Horie, A note on the $\mathbb{Z}_p \times \mathbb{Z}_q$-extension over $\mathbb{Q}$, Proc. Japan Acad. **77**, Ser. A (2001), 84–86. https://doi.org/10.3792/pjaa.77.84 2, 23
[35] K. Horie, Triviality in ideal class groups of Iwasawa-theoretical abelian number fields, J. Math. Soc. Japan **57**(3) (2005), 827–857. https://doi.org/10.2969/jmsj/1158241937 2, 23
[36] K. Horie, Certain primary components of the ideal class group of the $\mathbb{Z}_p$-extensions over the rationals, Tohoku Math. J. **59**(2) (2007), 259–291. https://doi.org/10.2748/tmj/1182180736 2, 6
[37] K. Horie, M. Horie, The ℓ-class group of the $\mathbb{Z}_p$-extension over the rational field, J. Math. Soc. Japan **64**(4) (2012), 1071–1089. https://doi.org/10.2969/jmsj/06441071 2, 6, 20

[38] H. Ichimura, On the parity of the class number of the 7^nth cyclotomic field, Math. Slovaca **59**(3) (2009), 357–364. https://doi.org/10.2478/s12175-009-0132-5 2, 6
[39] H. Ichimura, S. Nakajima, On the 2-part of the ideal class group of the cyclotomic $\mathbb{Z}_p$-extension over the rationals, Abh. Math. Semin. Univ. Hamburg **80**(2) (2010), 175–182.2, 6 https://doi.org/10.1007/s12188-010-0036-x
[40] A. Inatomi, On $\mathbb{Z}_p$-extensions of real abelian fields, Kodai Math. J. **12** (1986), 420–422.2, 26 https://projecteuclid.org/euclid.kmj/1138039105
[41] J.-F. Jaulent, S-classes infinitésimales d'un corps de nombres algébriques, Ann. Sci. Inst. Fourier (Grenoble) **34**(2) (1984), 1–27. https://doi.org/10.5802/aif.960 4
[42] J.-F. Jaulent, Classes logarithmiques des corps de nombres, Journal de Théorie des Nombres de Bordeaux **6** (1994), 301–325. https://jtnb.centre-mersenne.org/item/JTNB_1994__6_2_301_0 4, 25
[43] J.-F. Jaulent, Note sur la conjecture de Greenberg, J. Ramanujan Math. Soc. **34** (2019), 59–80. http://www.mathjournals.org/jrms/2019-034-001/2019-034-001-005.html 4, 7, 20
[44] J.-F. Jaulent, Annulateurs de Stickelberger des groupes de classes logarithmiques (2020). https://arxiv.org/abs/2003.05768 25
[45] H. Koch, Galois theory of p-extensions (English translation of *"Galoissche Theorie der p-Erweiterungen"*, 1970), Springer Monographs in Math., Springer, 2002. 3
[46] J.C. Miller, Class numbers of totally real fields and applications to the Weber class number problem, Acta Arith. **164**(4) (2014), 381–398. https://arxiv.org/pdf/1405.1094.pdf2, 13 https://doi.org/10.4064/aa164-4-4
[47] J.C. Miller, Class numbers in cyclotomic $\mathbb{Z}_p$-extensions, J. of Number Theory **150** (2015), 47–73.2, 13 https://doi.org/10.1016/j.jnt.2014.11.008
[48] T. Morisawa, Mahler measure of the Horie unit and Weber's class number problem in the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}$, AIP Conference Proceedings **1264**, 52 (2010).2, 6 https://doi.org/10.1063/1.3478179
[49] T. Morisawa, On Weber's class number problem, PhD thesis, Waseda University, 2012.2, 6 http://hdl.handle.net/2065/37750
[50] T. Morisawa, On the ℓ-part of the $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$-extension of $\mathbb{Q}$, J. Number Theory **133**(6) (2013), 1814–1826. https://doi.org/10.1016/j.jnt.2012.09.017 2, 20
[51] T. Morisawa, R. Okazaki, Height and Weber's Class Number Problem, Journal de Théorie des Nombres de Bordeaux **28**(3) (2016), 811–828. https://doi.org/10.5802/jtnb.965 2, 6
[52] T. Morisawa, R. Okazaki, Mahler measure and Weber's class number problem in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ for odd prime number p, Tohoku Math. J. **65**(2) (2013), 253–272.2, 6 https://doi.org/10.2748/tmj/1372182725
[53] A. Movahhedi, Sur les p-extensions des corps p-rationnels, Thèse, Univ. Paris VII, 1988. http://www.unilim.fr/pages_perso/chazad.movahhedi/These_1988.pdf 4
[54] A. Movahhedi, T. Nguyen Quang Do, Sur l'arithmétique des corps de nombres p-rationnels, Séminaire de Théorie des Nombres, Paris 1987–88, Progress in Math. **81** (1990), 155–200.4 https://doi.org/10.1007/978-1-4612-3460-9_9
[55] T. Nguyen Quang Do, Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens, Ann. Inst. Fourier (Grenoble) **36**(2) (1986), 27–46. https://doi.org/10.5802/aif.1045 3
[56] The PARI Group, PARI/GP, version 2.9.0, Université de Bordeaux (2016). 2 http://pari.math.u-bordeaux.fr/
[57] J.H. Silverman, An inequality Relating the Regulator and the Discriminant of a Number Field, J. Number Theory **19**(3) (1984), 437–442. https://doi.org/10.1016/0022-314X(84)9008 26
[58] H. Taya, On p-adic zêta functions and $\mathbb{Z}_p$-extensions of certain totally real number fields, Tohoku Math. J. **51**(1) (1999), 21–33. https://doi.org/10.2748/tmj/1178224850 3, 22
[59] L.C. Washington, The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension, Invent. Math. **49**(1) (1978), 87–97. https://doi.org/10.1007/BF01399512 2, 6, 9, 23

Villa la Gardette, 4 Chemin Château Gagnière, F-38520 Le Bourg d'Oisans
Email address: g.mn.gras@wanadoo.fr