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

GEORGES GRAS

ABSTRACT. Let $K := \mathbb{Q}(\ell^n)$ be the nth layer of the cyclotomic $\mathbb{Z}_\ell$-extension. It is conjectured that K is principal (Weber's conjecture for $\ell = 2$). Many studies (Ichimura–Miller–Morisawa–Nakajima–Okazaki) go in this direction. Nevertheless, we examine if a counterexample may be possible. For this, computations show that the p-torsion group $\mathscr{T}_K$ of the Galois group of the maximal abelian p-ramified pro-p-extension of K is not always trivial; whence the relevance of the conjecture since $\#\mathscr{T}_K = \#\mathscr{C}_K \cdot \#\mathscr{R}_K$ (up to a canonical 2-power if $p = 2$), where $\mathscr{C}_K$ is the p-class group, and $\mathscr{R}_K$ the normalized p-adic regulator. We give a new method (Theorem 4.6 testing $\#\mathscr{T}_K \neq 1$), allowing larger values of ℓ^n than those of the literature. Finally, we search in the cyclotomic $\widehat{\mathbb{Z}}$–extension, cases of non-trivial class groups using genus theory related to a deep property of $\mathscr{R}_K$ (Theorem 6.3); we only find again the three known cases (Fukuda–Komatsu–Horie).

CONTENTS

Date: September 30, 2020.
1991 *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 in 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 usual.

The purpose of our study is to see in what circumstances the p-class group of $\mathbb{Q}(\ell^n)$ is likely to be non-trivial for some prime p. Of course, the direct computation (and some deep analytic studies) of the class number have been done by many authors without complete success because of limitation of the order of magnitude of the degree ℓ^n and p; for instance, the results given in [43, 44, 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). Using PARI/GP [53], any "serious" computation needs the instruction $\mathsf{bnfinit}(\mathsf{P})$ (giving all the basic invariants of the field K defined via the polynomial P, whence the whole class group, a system of units, etc.), few values of ℓ, n, may be carried out. Some approaches, by means of geometry of numbers, prove that some of these fields are euclidian (see, e.g., [5] about $\mathbb{Q}(2^2)$, $\mathbb{Q}(2^3)$); but this more difficult and broad aspects, needs other techniques and we are in a class field theory context. For these reasons, we will use the following trick:

Let $\mathscr{T}_K$ be the torsion group of the Galois group $\mathscr{G}_K^{\rm pr} := {\rm Gal}(H_K^{\rm pr}/K)$, where $H_K^{\rm pr}$ is the maximal abelian p-ramified (i.e., unramified outside p and ∞) pro-p-extension of K; for $K = \mathbb{Q}(\ell^n)$, 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 of K, $\mathscr{R}_K$ its 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, $\mathscr{G}_K^{\rm pr} = \Gamma_K \oplus \mathscr{T}_K$ with $\Gamma_K \simeq \mathbb{Z}_p$.

So, as soon as $\mathscr{T}_K = 1$, we are certain that $\mathscr{C}_K = 1$; otherwise, we may suspect a possible counterexample. We shall compute, in § 2.3, the structure of some $\mathscr{T}_K$ by means of an indisputable reference program 2.3 (using $\mathsf{bnfinit}(\mathsf{P})$) to show that this p-torsion group is non-trivial in some cases of small degrees ℓ^n. The good new is that there exists a test about $\mathscr{T}_K$ which does not need $\mathsf{bnfinit}(\mathsf{P})$ and allows much larger fields K and primes p; it will be explained Section 3 and yields Theorem 4.6.

Finally, we consider the subfields of the composite $\widehat{\mathbb{Q}}$ of the $\mathbb{Z}_\ell$-extension of $\mathbb{Q}$ and give programs to search non-trivial p-class groups using instead genus theory in p-extensions F/K, $K \subset F \subset \widehat{\mathbb{Q}}$, in connection with a deep link with the p-adic regulator $\mathscr{R}_K$ of the base field (Theorem 6.3), as initiated by Taya [55]. Despite of the huge intervals tested, we only find again three known cases (Fukuda–Komatsu–Horie); then we propose some conjectures.

Now, recall some classical properties of these invariants.

1.1. **Class groups and torsion groups of abelian p-ramification, in $\mathbb{Q}(\ell^\infty)$.** The invariants $\mathscr{C}_{\mathbb{Q}(\ell^n)}$ and $\mathscr{T}_{\mathbb{Q}(\ell^n)}$, for all $p \neq \ell$, are the fundamental invariants of $\mathbb{Q}(\ell^n)$ and one may ask if the arithmetic of $\mathbb{Q}(\ell^n)$ is as smooth as it is conjectured (for the class group) by many authors after many verifications and partial proofs [4, 10, 11, 12, 13, 32, 33, 34, 35,

36, 37, 43, 44, 45, 46, 47, 48, 49]. The triviality of $\mathscr{C}_{\mathbb{Q}(\ell^n)}$ has no counterexamples as ℓ, n, p vary, but that of $\mathscr{T}_{\mathbb{Q}(\ell^n)}$ is, on the contrary, not true as we shall see numerically.

Denote by C_K the whole class group (in the restricted or ordinary sense, which will be precised with the mentions $^{\rm res}$ or $^{\rm ord}$).

Chevalley's formula [6, p. 406] (1933) for class groups $C_K^{\rm res}$, $C_k^{\rm res}$, in any cyclic extension K/k of Galois group G, is given, in whole generality, by $\#(C_K^{\rm res})^G = \frac{\#C_k^{\rm res}\cdot\prod_{\mathfrak{l}} e_{\mathfrak{l}}}{[K:k]\cdot(E_k^{\rm pos}:E_k^{\rm pos}\cap {\rm N}_{K/k}(K^\times))}$, where $e_{\mathfrak{l}}$ is the ramification index in K/k of the prime ideal $\mathfrak{l}$ of k and $E_k^{\rm pos}$ 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 the product of two integers:

$$\#(C_K^{\rm res})^G = \#C_k^{\rm res}\cdot\frac{\prod_{\mathfrak{l}\neq\mathfrak{l}_0} e_{\mathfrak{l}}}{(E_k^{\rm pos}:E_k^{\rm pos}\cap {\rm N}_{K/k}(K^\times))}.$$

Applied to $\mathbb{Q}(\ell^n)/\mathbb{Q}$ the formula gives $(C^{\rm res}_{\mathbb{Q}(\ell^n)})^G = 1$ since ℓ is the unique (totally) ramified prime and since $E^{\rm pos}_{\mathbb{Q}} = 1$. So, for $p=\ell$, $\mathscr{C}^{\rm res}_{\mathbb{Q}(\ell^n)} = 1$, a classical result often attributed to Iwasawa instead of Chevalley (or more precisely Herbrand–Chevalley, the Herbrand quotient of the group of units of K being the key for the proof). In the sequel, we implicitly assume $p\neq\ell$.

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 $\mathscr{T}_{\mathbb{Q}(\ell^n)} = 1$ for all n ([15, Theorem IV.3.3], [18, Proposition 6], [27, Appendix A.4.2]); which justifies once again the assumption $p\neq\ell$ and that the notation $\mathscr{T}$ always refers to a p-torsion group.

1.2. **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 field K (under Leopoldt's conjecture), $\mathscr{T}_K$ is the dual of ${\rm H}^2(\mathscr{G}_K,\mathbb{Z}_p)$ [52], 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 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 Shafarevich–Tate groups in the framework of S-ramification when S is the set of p-places (and real ones if $p=2$) [42, Theorem 3.74]:

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

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

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

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, ${\rm rk}_p(\mathscr{T}_K) = {\rm rk}_p(V_K/K^{\times p}) + \sum_{v\in S}\delta_v - \delta_K$, where $\delta_v = 1$ or 0 according as K_v contains μ_p or not, $\delta_K = 1$ or 0 according as K contains μ_p or not [15, Corollary III.4.2.3]. For generalizations, with ramification and decomposition giving Shafarevich formula, see [15, II.5.4.1] as well as [38], and for the reflection theorem on generalized class groups, see [19], [15, II.5.4.5 and Theorem III.4.2]. Thus, ${\rm rk}_p(Ш^2_K)$ depends essentially on ${\rm rk}_p(\mathscr{T}_K)$.

If one replaces the notion of p-ramification (in pro-p-extensions) by that of S-ramification (in pro-extensions), *for any set of places S*, the corresponding Shafarevich–Tate groups have some relations with the corresponding torsion groups $\mathscr{T}_{K,S}$, but with many open questions when no assumption is done on S (see [31] 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 Shafarevich–Tate groups are trivial or obvious, which has deep consequences as shown for instance in [2] in relation with our conjectures in [20] on the p-adic properties of the units. For more information on the story of abelian p-ramification and p-rationality, see [27, Appendix A] and its bibliography about the pioneering contributions: K-theory approach [18], p-infinitesimal approach [38], cohomological/pro-p-group approach [50, 51]. All basic material about p-rationality is overviewed in [15, III.2, IV.3, IV.4.8].

In another point of view, the orders and annihilations of the $\mathscr{T}_{\mathbb{Q}(\ell^n)}$ are given by p-adic L-functions, the two theories (arithmetic and analytic) being equivalent (this will give the testing of $\mathscr{T}_{\mathbb{Q}(\ell^n)} \neq 1$ from Theorem 4.6).

All these principles on Shafarevich–Tate groups exist for the theory of elliptic curves and this is at the origin of a question of Coates [8, Section 3] on the possible triviality of the $C_{\mathbb{Q}(\ell^n)}$ and more generally on the behavior of the class groups in the composite $\widehat{\mathbb{Q}}$ of the $\mathbb{Z}_\ell$-extensions of $\mathbb{Q}$.[1]

1.3. **The logarithmic class group and Greenberg's conjecture.** We may also consider another p-adic invariant, the Jaulent's logarithmic class group $\widetilde{\mathscr{C}\ell}_K$ [39] which governs Greenberg's conjecture [29] 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 $K(p^\infty)$ [40]. 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 $K = \mathbb{Q}(\ell^n)$ for $p \neq \ell$. As we shall see, in all attempts concerning subfields of $\mathbb{Q}(\ell^\infty)$, Jaulent's logarithmic class group for $p \neq \ell$ was trivial .

2. Abelian p-ramification theory for totally real fields

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 – The p-invariants of K.**

(*a*) Let E_K^1 be the group of p-principal global units $\varepsilon \equiv 1 \pmod{\prod_{\mathfrak{p}|p} \mathfrak{p}}$ of K. Let $U_K^1 := \oplus_{\mathfrak{p}|p} U_{K_\mathfrak{p}}^1$ be the $\mathbb{Z}_p$-module of p-principal local units, where $U_{K_\mathfrak{p}}^1$ is the group of $\mathfrak{p}$-principal units of the $\mathfrak{p}$-completion $K_\mathfrak{p}$ of K. Denote by μ_κ the group of pth roots of unity of any field κ and put $\mathscr{W}_K := \mathrm{tor}_{\mathbb{Z}_p}(U_K^1)/\mu_K = \big[\oplus_{\mathfrak{p}|p} \mu_{K_\mathfrak{p}}\big]/\mu_K$.

(*b*) Let $\iota : \{x \in K^\times \otimes \mathbb{Z}_p,\ x \text{ prime to } p\} \to U_K^1$ be the diagonal embedding. Let $\overline{E_K^1}$ be the closure of ιE_K^1 in U_K^1 and let H_K^{nr} be the p-Hilbert class field of K; then we have $\mathrm{Gal}(H_K^{\mathrm{pr}}/H_K^{\mathrm{nr}}) \simeq U_K^1/\overline{E_K^1}$. The Leopoldt conjecture leads to the (not so trivial) exact sequence:

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

(*c*) Let $\mathscr{C}_K$ be the p-class group of K, isomorphic to $\mathrm{Gal}(H_K^{\mathrm{nr}}/K)$.

(*d*) Let $\mathscr{R}_K := \mathrm{tor}_{\mathbb{Z}_p}(\log(U_K^1)/\log(\overline{E_K^1}))$ be the normalized p-adic regulator [23, § 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 [7, Appendix] giving the link of $\mathscr{R}_K$ with the residue of the p-adic zeta function 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.

(e) Let $K(p^\infty) = K\mathbb{Q}(p^\infty)$ be the cyclotomic $\mathbb{Z}_p$-extension of K and let $H_K^{\rm bp}$ (called the Bertrandias–Payan field) fixed by the subgroup $\mathscr{W}_K$ of $\mathscr{T}_K$; the field $H_K^{\rm bp}$ 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 $K = \mathbb{Q}(\ell^n)$.** In that case, some simplifications arise:

Lemma 2.1. *One has $\mathscr{W}_K = 1$ for all $K = \mathbb{Q}(\ell^n)$, except for the case $p = 2$ 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 $p \neq 2$, the p-completions $K_\mathfrak{p}$ (unramified of ℓ-power degree, $\ell \neq p$) do not contain μ_p since $\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p$, of degree $p-1 > 1$, is totally ramified at p; thus $\mathscr{W}_K = 1$. For $p = 2$, $K_\mathfrak{p}$ does not contain μ_4 but μ_2 and $\mathrm{tor}_{\mathbb{Z}_p}(U_K^1) \simeq \mathbb{F}_2^{\#S}$, thus $\mathscr{W}_K \simeq \mathbb{F}_2^{\#S-1}$. □

For $p = 2$, the case $\#S > 1$ is very rare and occurs only when $2^{\ell-1} \equiv 1 \pmod{\ell^2}$, e.g., $\ell = 2093, 3511$, but these values of ℓ are out of range of practical computations. Thus $\mathscr{W}_K$ is in general trivial. Since for $K = \mathbb{Q}(\ell^n)$, $K(p^\infty) \cap H_K^{\rm nr} = K$, we have the following diagram:

$$\begin{array}{ccccccc} & & & \overset{\mathscr{T}_K}{\frown} & & & \\ K(p^\infty) & \xrightarrow[\mathscr{C}_K]{} & K(p^\infty)H_K^{\rm nr} & \xrightarrow[\mathscr{R}_K]{} & H_K^{\rm bp} & \xrightarrow[\mathscr{W}_K]{} & H_K^{\rm pr} \end{array}$$

Remarks 2.2. *Assume to be in the non-exceptional cases where $\mathscr{W}_K = 1$.*

(*i*) *If $\mathscr{C}_K = 1$, $\mathscr{T}_K = \mathscr{R}_K$, the normalized p-adic regulator, which is not always trivial as we shall see, even if we have conjectured in* [20] *that, for any number field K, $\mathscr{T}_K = 1$ for $p \gg 0$.*

(*ii*) *One may think that interesting examples occur more easily when p totally splits in $\mathbb{Q}(\mu_{\ell^n})$ (i.e., $p \equiv 1 \pmod{\ell^n}$). This explains the result of* [36] *and* [37] *clamming that $\#C_{\mathbb{Q}(\ell^n)}$ is odd in $\mathbb{Q}(\ell^\infty)$ for all $\ell < 500$ and that of* [35, 48, 49]. *Indeed, for $p = 2$ or any very small p, the residue degree ρ_n of p in $\mathbb{Q}(\mu_{\ell^n})$ fulfills the condition $p^{\rho_n} \equiv 1 \pmod{\ell^n}$, giving $\rho_n > \dfrac{n\log(\ell)}{\log(p)}$, unbounded as $n \to \infty$, which means that if the order of the relative class group $\mathscr{C}^*_{\mathbb{Q}(\ell^n)} = \mathrm{Ker}(\mathrm{N}_{\mathbb{Q}(\ell^n)/\mathbb{Q}(\ell^{n-1})})$ is non-trivial for n large enough, then it is divisible by p^{ρ_n} due to the Galois action on a non-trivial p-class of $\mathscr{C}^*_{\mathbb{Q}(\ell^n)}$, which becomes oversized; see § 2.4 for more details showing that $\mathscr{C}^*_{\mathbb{Q}(\ell^n)} = 1$ for $n \gg 0$ does exist for any prime $p \geq 2$ from a non-trivial result of Washington* [56] *and explicit deep analytic computations in* [4, 9, 10, 13, 34, 35, 36, 37, 45, 46, 48, 49] *(e.g.,* [13, Corollary 1]*).* [2]

2.3. **General computation of the structure of $\mathscr{T}_{\mathbb{Q}(\ell^n)}$.** We shall first use the following PARI/GP programs giving the structure of abelian group, of $\mathscr{T}_{\mathbb{Q}(\ell^n)}$, for small values of n, from the given polynomial $\mathsf{P} = \mathsf{polsubcyclo}(\mathsf{el}^{\mathsf{n}+1}, \mathsf{el}^{\mathsf{n}})$ for $p > 2$ (the case of degree 2^n being different for the polynomial), P defining the real field $\mathbb{Q}(\ell^n)$ (these programs are simplified forms of the general one written in [25, Programme I, § 3.2]). The parameter N must be such that p^N is larger than the exponent of $\mathscr{T}_{\mathbb{Q}(\ell^n)}$; taking $N = 2$ for $p > 2$ (resp. $N = 3$ for $p = 2$) gives the p-rank of the group.

```
PROGRAM I. STRUCTURE OF T FOR el=2, p>2
{el=2;N=12;for(n=1,3,print("el=",el," n=",n);P=x;for(j=1,n,P=P^2-2);
K=bnfinit(P,1);forprime(p=3,2*10^5,KpN=bnrinit(K,p^N);HpN=KpN.cyc;
L=List;e=matsize(HpN)[2];R=0;for(k=1,e-1,c=HpN[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)=",R," T=",L))))}
```

[2] See 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 $\mathbb{Q}(\ell^{n_0})$, yields $\mathscr{C}_{\mathbb{Q}(\ell^n)} = 1$ for all n.

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

FASTER PROGRAM, FOR el=2, p>2, ONLY COMPUTING #T
{el=2;n=3;P=x;for(k=1,n,P=P^2-2);K=bnfinit(P,1);
forprime(p=3,2*10^5,HpN=bnrclassno(K,p^2);w=valuation(HpN,p)-1;
if(w>0,print("el=",el," n=",n," p=",p," #T=", p^w)))}

PROGRAM II. STRUCTURE OF T FOR el>2, p!=el
{el=3;N=8;for(n=1,2,print("el=",el," n=",n);P=polsubcyclo(el^(n+1),el^n);
K=bnfinit(P,1);forprime(p=2,200,KpN=bnrinit(K,p^N);HpN=KpN.cyc;
L=List;e=matsize(HpN)[2];R=0;for(k=1,e-1,c=HpN[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)=",R," T=",L))))}

el=3 n=1 p=7   rk(T)=1 T=[7]           el=3 n=1 p=73  rk(T)=1 T=[73]
el=3 n=2 p=7   rk(T)=1 T=[7]           el=3 n=2 p=73  rk(T)=1 T=[73]
el=5 n=1 p=11  rk(T)=2 T=[11,11]
el=5 n=2 p=11  rk(T)=2 T=[11,11]       el=5 n=2 p=101 rk(T)=1 T= [101]

FASTER PROGRAM, FOR el>2, p!=el, ONLY COMPUTING #T
{el=3;n=1;P=polsubcyclo(el^(n+1),el^n);K=bnfinit(P,1);
forprime(p=5,2*10^5,HpN=bnrclassno(K,p^2);w=valuation(HpN,p)-1;
if(w>0,print("el=",el," n=",n," p=",p," #T=", p^w)))}
```

These partial results show that the p-ramification aspects are more intricate since, for instance, for the case $\ell = 2$, 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 $n = 2$ (see the next § 2.4 for more explanations). Unfortunately, it is not possible in practice to compute easily beyond $\ell = 17$ for various p with the bnfinit instruction. So, as we have explained in the Introduction, we shall give Section 3 another method to test $\mathscr{T}_{\mathbb{Q}(\ell^n)} \neq 1$ for larger ℓ and p.

2.4. **Algebraic and analytic aspects.** Let $K = \mathbb{Q}(\ell^n)$ and $k = \mathbb{Q}(\ell^{n-1})$ with $p \neq \ell$ fixed. Then 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 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 $p \neq \ell$; so $\#\mathscr{T}_K$, $\#\mathscr{R}_K$, $\#\mathscr{C}_K$ increase as soon as appear relative submodules in K/k.

Let $\mathscr{T}_K^*$, $\mathscr{R}_K^*$, $\mathscr{C}_K^*$, be the corresponding kernels of the arithmetic norm $\mathrm{N}_{K/k}$ (or of the algebraic norm $\nu_{K/k} := \sum_{\sigma \in \mathrm{Gal}(K/k)} \sigma$); then we get the relation $\#\mathscr{T}_K^* = \#\mathscr{R}_K^* \cdot \#\mathscr{C}_K^*$, since $\#\mathscr{W}_K^* = 1$, except in the case $p = 2$ when 2 splits beyond k, giving $\#\mathscr{W}_K^* = 2$ (Lemma 2.1).

2.4.1. *Galois action – Relative submodules.* Let $(\mathscr{M}_{\mathbb{Q}(\ell^n)})_{n \geq 0}$ be a family of finite $\mathbb{Z}_p[G_n]$-modules, $G_n = \mathrm{Gal}(\mathbb{Q}(\ell^n)/\mathbb{Q})$, provided with natural transfer and norm maps having the above properties (this will apply to $\mathscr{T}$, $\mathscr{C}$, $\mathscr{R}$, $\mathscr{W}$), and let $\mathscr{M}^*_{\mathbb{Q}(\ell^n)}$ be the kernel of the algebraic norm $\nu_{\mathbb{Q}(\ell^n)/\mathbb{Q}(\ell^{n-1})}$ so that:

$$\mathscr{M}_{\mathbb{Q}(\ell^n)} \simeq \mathscr{M}_{\mathbb{Q}(\ell^{n-1})} \bigoplus \mathscr{M}^*_{\mathbb{Q}(\ell^n)}.$$

Let $K = \mathbb{Q}(\ell^n)$, $n \geq 1$, and $k_i := \mathbb{Q}(\ell^i)$, $0 \leq i \leq n$; since G_n is cyclic of order ℓ^n, the rational characters χ_i of K are in one-to-one correspondence with the k_i; we shall denote by $\theta_i \mid \chi_i$ the irreducible p-adic characters; each θ_i is above a character ψ_i of degree 1 and order ℓ^i. We have the decomposition $\mathscr{M}_K = \bigoplus_{i=1}^{n} \mathscr{M}_K^{\chi_i} = \bigoplus_{i=1}^{n} \mathscr{M}^*_{k_i} = \bigoplus_{i=1}^{n} \Big[\bigoplus_{\theta_i \mid \chi_i} \mathscr{M}^{\theta_i}_{k_i} \Big]$. Then $\mathscr{M}_K^*$

(or any of its component $\mathscr{M}_K^{\theta_n}$) is a module over $\mathbb{Z}_p[\mu_{\ell^n}]$, hence isomorphic to a product of $\mathbb{Z}_p[\mu_{\ell^n}]$-modules of the form $\mathbb{Z}_p[\mu_{\ell^n}]/\mathfrak{p}_n^e$, $\mathfrak{p}_n \mid p$ in $\mathbb{Q}_p(\mu_{\ell^n})$, $e \geq 1$, whose p-rank is a multiple of the residue degree ρ_n of p in the extension $\mathbb{Q}_p(\mu_{\ell^n})/\mathbb{Q}_p$ (i.e., $\rho_n \geq 1$ minimal such that $p^{\rho_n} \equiv 1 \pmod{\ell^n}$) and whose order is $p^{e\,\rho_n}$; thus $\rho_n \to \infty$ as $n \to \infty$, which is considered as incredible for classical arithmetic invariants that we shall investigate below, and leads to analytic proofs of the triviality of $\mathscr{C}_K^*$ for some p if $\ell^n \gg 0$ (Remark 2.2).

2.4.2. *The p-class groups in $\mathbb{Q}(\ell^\infty)$.* We still put $K := \mathbb{Q}(\ell^n)$. Washington's theorem [56] gives a limitation of the increasing of $\mathscr{C}_K$, as $n \to \infty$; it claims (with our notations) that for ℓ and p fixed, $\#\mathscr{C}_K$ is constant for all n large enough, whence $\mathscr{C}_K^* = 1$ for all $n \gg 0$. This only applies to the p-class groups, but in all the tower. Other analytical studies, as we have mentioned, give some principalities (or p-principalities), for all n, under some limitations of the parameters. In [4], a conjecture (from "speculative extensions of the Cohen–Lenstra–Martinet heuristics") implies $\mathscr{C}_K^* \neq 1$ for finitely many layers K (possibly none).

These theorems may be easily understandable from the previous observation on the p-ranks. Thus it is natural (but non-trivial) that $\mathscr{C}_K^* = 1$ (hence $\mathscr{C}_K$ constant) for all $n \gg 0$.

2.4.3. *The torsion groups in $\mathbb{Q}(\ell^\infty)$.* Concerning the case of the torsion groups $\mathscr{T}_K$, 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 the layers $L := K(\mu_p)$, the p-rank of $\mathscr{T}_K^*$ is bounded by that of $\mathscr{C}_L^*$ (in fact of the ω-component where ω is the Teichmüller character). Thus Washington's theorem may be true for the torsion groups in $\mathbb{Q}(\ell^\infty)$.

2.4.4. *The normalized regulators in $\mathbb{Q}(\ell^\infty)$.* One can wonder what happens for the 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 [20, § 4.2.2]. Indeed, 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 $\mathrm{R}_p^\theta(\eta) = \prod_{\psi \mid \theta} \mathrm{R}_p^\psi(\eta)$ with absolutely irreducible characters ψ. Then, in a standard point of view, $\mathrm{Prob}\left(\mathscr{R}_K^\theta \equiv 0 \,(\mathrm{mod}\ p)\right) = \frac{O(1)}{p^{\rho\,\delta^2}}$ (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, $\rho = \rho_n$ 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 $\rho_n = 1$, may divide $\#\mathscr{R}_K^{\theta_n}$, which indicates other probabilities conjectured in [20, Théorème 1.1]. Thus, this analysis also confirms that, for ℓ and p fixed, $\mathscr{T}_K$ may be constant for all n large enough. So, we have forced some programs to search only primes $p \equiv 1 \pmod{\ell^n}$ hoping more examples of non-trivial $\mathscr{T}_K$.

2.4.5. *The logarithmic class groups in $\mathbb{Q}(\ell^\infty)$.* We have computed (for $\ell^n \in \{2^6, 3^3, 5^3, 7, 11, 13, 17, 19, 23, 29\}$) the order of $\widetilde{\mathscr{C}}_K$ for all $p \in [2, 2 \cdot 10^5]$ (from [3]), and we have no non-trivial example; this means that the logarithmic class group behaves as the ordinary p-class group in $\mathbb{Q}(\ell^\infty)$, but not as $\mathscr{T}_K$, as we have seen. So it is possible to state the conjecture that, for all p, the logarithmic class groups $\widetilde{\mathscr{C}}_K$ are all trivial. This is not too surprising since if $\mathscr{C}_K = 1$ and if p is totally inert in K, then $\widetilde{\mathscr{C}}_K = 1$ for obvious reasons (see [40, Schéma § 2.3] or [28, Diagram 4.2]); and this is almost the case in our computations.

We refer to [41, Théorème 4] giving the property of annihilation of $\widetilde{\mathscr{C}_K}$ by means of the Stickelberger pseudo measure and its image by the Spiegel involution that we shall recall and use for the annihilation of $\mathscr{T}_K$.

3. Definition of p-adic measures

We recall the main classical principles to apply them to the fields $\mathbb{Q}(\ell^n)$, $\ell \geq 2$ prime, $n \geq 1$, with $p \geq 2$ prime distinct from ℓ, then to composite of such fields $\mathbb{Q}(\ell_1^{n_1}) \cdots \mathbb{Q}(\ell_t^{n_t})$, denoted $\mathbb{Q}(N)$, where $N = \ell_1^{n_1} \cdots \ell_t^{n_t}$, and by taking $p \nmid N$.

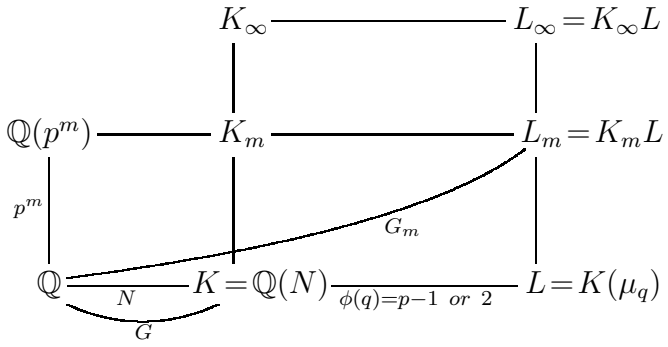
3.1. **General definition of the Stickelberger elements.** Let $f > 1$ be any abelian conductor and let $\mathbb{Q}(\mu_f)$ be the corresponding cyclotomic field. We define $\mathscr{S}_{\mathbb{Q}(\mu_f)} := -\sum_{a=1}^{f} \left(\frac{a}{f} - \frac{1}{2}\right) \cdot \left(\frac{\mathbb{Q}(\mu_f)}{a}\right)^{-1}$ (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 an element of the annihilator of $\mu_{\mathbb{Q}(\mu_f)}$, which is generated by f (or $2\,f$) and the multipliers $1 - c \cdot \left(\frac{\mathbb{Q}(\mu_f)}{c}\right)^{-1}$, for any odd c prime to f. This shall give integral elements in the group algebra. If f is odd, one may take c even for annihilation in $\mathbb{Z}_p$-algebras for $p \neq 2$ or when the term $\frac{1}{2}\sum_{a=1}^{f} \left(\frac{\mathbb{Q}(\mu_f)}{a}\right)^{-1}$ can be neglected.

Put $q = p$ (resp. 4) if $p \neq 2$ (resp. $p = 2$). For $K = \mathbb{Q}(N)$, let $L = K(\mu_q)$; to simplify the notations, put $K_m := K\mathbb{Q}(p^m)$, $L_m := K_m L = K(\mu_{qp^m})$ for all $m \geq 0$; so $\cup_m K_m = K\mathbb{Q}(p^\infty) =: K_\infty$ and $\cup_m L_m = L\mathbb{Q}(p^\infty) =: L_\infty$.

Note, once for all, that the index m is relative to layers in cyclotomic $\mathbb{Z}_p$-extensions contrary to N used for fields in the composite of the cyclotomic $\mathbb{Z}_\ell$-extensions, $\ell \neq p$.

All this is summarized by the following diagram where $G_m := \mathrm{Gal}(L_m/\mathbb{Q}) \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/\phi(q)\mathbb{Z}$, ϕ being the Euler function:



3.2. **Multipliers of Stickelberger elements.** The conductor of L_m is $f_{L_m} = f_N \cdot qp^m$ for $2 \nmid N$ and $f_N \cdot p^{m+1}$ otherwise. Put $f_N^m := f_{L_m}$. Let c be an integer prime to f_N^m and, by restriction of $\mathscr{S}_{\mathbb{Q}(\mu_{f_N^m})}$ to L_m, let $\mathscr{S}_{L_m}^c := \left(1 - c\left(\frac{L_m}{c}\right)^{-1}\right) \cdot \mathscr{S}_{L_m}$; then $\mathscr{S}_{L_m}^c \in \mathbb{Z}[G_m]$. Indeed, we have:

$$\mathscr{S}_{L_m}^c = \frac{-1}{f_N^m} \sum_a \left[a\left(\frac{L_m}{a}\right)^{-1} - ac\left(\frac{L_m}{a}\right)^{-1}\left(\frac{L_m}{c}\right)^{-1}\right] + \frac{1-c}{2}\sum_a \left(\frac{L_m}{a}\right)^{-1};$$

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

$\big[\ \big]$ and $\Big(\frac{L_m}{a'_c}\Big)\Big(\frac{L_m}{c}\Big)=\Big(\frac{L_m}{a}\Big)$, this yields:

$$\begin{aligned}\mathscr{S}^c_{L_m} &= \frac{-1}{f^m_N}\Big[\sum_a a\Big(\frac{L_m}{a}\Big)^{-1}-\sum_a a'_c\cdot c\Big(\frac{L_m}{a'_c}\Big)^{-1}\Big(\frac{L_m}{c}\Big)^{-1}\Big]+\frac{1-c}{2}\sum_a\Big(\frac{L_m}{a}\Big)^{-1}\\ &= \frac{-1}{f^m_N}\sum_a\Big[a-a'_c\cdot c\Big]\Big(\frac{L_m}{a}\Big)^{-1}+\frac{1-c}{2}\sum_a\Big(\frac{L_m}{a}\Big)^{-1}\\ &= \sum_a\Big[\lambda^m_a(c)+\frac{1-c}{2}\Big]\Big(\frac{L_m}{a}\Big)^{-1}\in\mathbb{Z}[G_m].\end{aligned}$$

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

Proof. By definition, the integer $(f^m_N-a)'_c$ is in $[1,f^m_N]$ and congruent modulo f^m_N to $(f^m_N-a)\,c^{-1}\equiv -ac^{-1}\equiv -a'_c\pmod{f^m_N}$; thus $(f^m_N-a)'_c=f^m_N-a'_c$ and $\lambda^m_{f^m_N-a}(c)=\frac{(f^m_N-a)'_c\,c-(f^m_N-a)}{f^m_N}=\frac{(f^m_N-a'_c)\,c-(f^m_N-a)}{f^m_N}=c-1-\lambda^m_a(c)$, whence $\lambda^m_{f^m_N-a}(c)+\frac{1-c}{2}=-\big(\lambda^m_a(c)+\frac{1-c}{2}\big)$ 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 $\big(\frac{L_m}{a}\big)$, then $\big(\frac{L_m}{a}\big)^*\equiv a\cdot\big(\frac{L_m}{a}\big)^{-1}\bmod qp^m$.

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 $\omega:G_0=\mathrm{Gal}(L/\mathbb{Q})\to\mathbb{Z}_p^\times$. From Lemma 3.1, we have obtained $\mathscr{S}^{c*}_{L_m}=\mathscr{S}'^{c*}_{L_m}\cdot(1+s_\infty)$ in $(\mathbb{Z}/qp^m\mathbb{Z})[G_m]$.

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

Recall that, for $K=\mathbb{Q}(N)$, $K_m:=K\mathbb{Q}(p^m)$ and $L_m:=K_mL$. 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 element, of the kummer radical in $L^\times_m$ 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 [17, 22] for more history). The case $p=2$ is particularly tricky; to overcome this difficulty, we shall refer to [16, 30]. 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 [56, Theorem 5.18]. We have the following result with a detailed proof in [22, 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:

$$\mathscr{S}'^{c*}_{L_m}\equiv\sum_{a=1}^{f^m_N/2}\Big[\lambda^m_a(c)+\frac{1-c}{2}\Big]\,a^{-1}\Big(\frac{L_m}{a}\Big)\pmod{qp^m},\tag{1}$$

defining a coherent family in $\varprojlim_{m\geq e}(\mathbb{Z}/qp^m\mathbb{Z})[G_m]$ of annihilators of $\mathscr{T}_K$.

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 $\mathscr{A}^c_K:=\lim_{m\to\infty}\sum_{a=1}^{f^m_N/2}\Big[\lambda^m_a(c)+\frac{1-c}{2}\Big]\,a^{-1}\Big(\frac{K}{a}\Big)$ in $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$, is a canonical annihilator of $\mathscr{T}_K$.

Remark 4.2. *Let* $\alpha^*_{L_m} := \big[\sum_{a=1}^{f_N^m}\big(\frac{L_m}{a}\big)^{-1}\big]^* \equiv \sum_{a=1}^{f_N^m} a^{-1}\big(\frac{L_m}{a}\big) \pmod{qp^m}$*; then:* $\alpha^*_{L_m} := \sum_{a=1}^{f_N^m/2} a^{-1}\big(\frac{L_m}{a}\big) + (f_N^m - a)^{-1}\big(\frac{L_m}{f_N^m - a}\big) \equiv \sum_{a=1}^{f_N^m/2} a^{-1}\big(\frac{L_m}{a}\big)(1 - s_\infty) \bmod f_N^m$,
which annihilates $\mathscr{T}_K$ *by restriction for* m *large enough since* K *is real. We shall neglect in* $\mathscr{A}_K^c$ *the term* $\frac{1-c}{2}\cdot\alpha^*_{L_m}$ *and we still denote:*

$$\mathscr{A}_K^c = \lim_{m\to\infty}\Big[\sum_{a=1}^{f_N^m/2}\lambda_a^m(c)\,a^{-1}\Big(\frac{K}{a}\Big)\Big].$$

Lemma 4.3. *For* $K = \mathbb{Q}(N)$*,* ψ_N *of order* N *and conductor* f_N*,*

$$\psi_N(\mathscr{A}_K^c) = (1 - \psi_N(c))\cdot\tfrac{1}{2}L_p(1,\psi_N). \tag{2}$$

Proof. This comes from the classical construction of p-adic L-functions (e.g., [14, page 292], [17, Propositions II.2, II.3, Définition II.3, II.4, Remarques II.3, II.4], [56, Chapters 5, 7]). For more details, see [22, § 7.1]. □

Proposition 4.4. *Let* $K := \mathbb{Q}(N)$ *of Galois group* $G \simeq \mathbb{Z}/N\mathbb{Z}$ *and conductor* f_N*. Then, for the* p*-adic character* θ_N *above* 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 $p \neq 2$, 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; 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. [22, Corollary 7.3, (iii)]. *We have* $\mathscr{A}_K^c \equiv \sum_{a=1}^{f_N^0/2}\lambda_a^0(c)\,a^{-1}\Big(\frac{K}{a}\Big)$ *modulo* p*,* $p \nmid N$*, where* $f_N^0 = f_N\cdot q$ *for* $2 \nmid N$ *and* $f_N\cdot p$ *otherwise.*

Thus, we have obtained, putting $f_N^0 =: f_N$, a computable characterization of non-triviality of $\mathscr{T}_K$, for $K = \mathbb{Q}(N)$, $p \geq 2$, $p \nmid N$, N fixed:

Theorem 4.6. *Let* $L = K(\mu_q)$*,* $q = p$ *or* 4*. The conductor of* L *is* $f_N := f_N\,q$ *for* $2 \nmid N$ *and* $f_N\,p$ *otherwise. Let* c *be an integer prime to* f_N*. For all* $a \in [1, f_N]$*, prime to* f_N*, let* a'_c *be the unique integer in* $[1, f_N]$ *such that* $a'_c\cdot c \equiv a \pmod{f_N}$ *and put* $a'_c\cdot c - a = \lambda_a(c)\,f_N$*,* $\lambda_a(c) \in \mathbb{Z}$*.*

Let $\mathscr{A}_K^c := \sum_{a=1}^{f_N/2}\lambda_a(c)\,a^{-1}\Big(\frac{K}{a}\Big)$*,* ψ_N *a character of* K *of order* N *and* θ_N *the* p*-adic character above* ψ_N*. Then, if* $\psi_N(\mathscr{A}_K^c)$ *is not a* p*-adic unit, the* θ_N*-component of the* $\mathbb{Z}_p[G]$*-module* $\mathscr{T}_K$ *is non-trivial.*

4.1. **Numerical test** $\mathscr{T}^*_{\mathbb{Q}(\ell^n)} \neq 1$ **for** $\ell > 2$**,** $p > 2$**.** We have, from § 2.4, by induction, $\mathscr{T}_{\mathbb{Q}(\ell^n)} = \mathscr{T}^*_{\mathbb{Q}(\ell^n)} \bigoplus \mathscr{T}_{\mathbb{Q}(\ell^{n-1})}$. For a character ψ_n of order ℓ^n of K, the condition $\psi_n(\mathscr{A}^c_{\mathbb{Q}(\ell^n)}) \equiv 0 \pmod{\mathfrak{p}_n}$, for some $\mathfrak{p}_n \mid p$, is equivalent to the non-triviality of $\mathscr{T}^*_{\mathbb{Q}(\ell^n)}$, due to the p-adic character θ_n above ψ_n. We compute $\psi_n(\mathscr{A}^c_{\mathbb{Q}(\ell^n)}) \pmod p$ 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
{forprime(el=3,120,for(n=1,4,Q=polcyclo(el^n);
h=znprimroot(el^(n+1));H=lift(h);C=2;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 the cases ($\ell = 3$, $p = 7$), ($\ell = 3$, $p = 73$), ($\ell = 5$, $p = 11$) and ($\ell = 5$, $n = 2$, $p = 101$), of Table 2.3.

An interesting case is $\ell = 5$ and $n = 2, 3$ 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 a subgroup isomorphic to $\mathbb{Z}/2251\mathbb{Z} \times \mathbb{Z}/2251\mathbb{Z}$.

We have computed the structure of $\mathscr{T}_{\mathbb{Q}(\ell^n)}$ for $\ell = 3$, $n = 3$, $p = 109$, which is much longer and needs a 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 $\mathfrak{p}_n \mid p$ by means of a congruence $\mathsf{z} \equiv \mathsf{r}\ (\mathsf{mod}\,\mathfrak{p}_\mathsf{n})$, 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, taking $n = 1$ for $\ell > 11$.

```
PROGRAM IV. TEST #T*>1 MODULO (zeta-r) WHEN p=1 (mod el^n) FOR el>2, p>2
{forprime(el=3,250,for(n=1,6,Q=polcyclo(el^n);h=znprimroot(el^(n+1));
H=lift(h);C=2;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))))))}

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;for(n=1,10,Q=polcyclo(el^n);h=znprimroot(el^(n+1));H=lift(h);C=2;
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 and IV ($\ell > 2$):

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

4.2. **Numerical test $\mathscr{T}^*_{\mathbb{Q}(\ell^n)} \neq 1$ for $\ell > 2$, $p = 2$.** In the case $p = 2$, taking $c = 3$, we have the exceptional prime $\ell = 11$ for which 3 splits in $\mathbb{Q}(11)$, whence $1 - \psi_1(c) = 0$ giving

a wrong solution with the following program. Moreover, θ 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 $\mathbb{Q}(\mu_\ell)$.

```
PROGRAM V. TEST #T>1 WITH NORM COMPUTATIONS FOR p=2, el>2
{p=2;q=4;n=1;C=3;forprime(el=5,10^4,Q=polcyclo(el^n);
h=znprimroot(el^(n+1));H=lift(h);f=q*el^(n+1);cm=Mod(C,f)^-1;
g=Mod(-1,q);G=lift(g);gm=g^-1;
e=lift(Mod((1-H)*el^(-n-1),q));H=H+e*el^(n+1);h=Mod(H,f);
e=lift(Mod((1-G)*q^-1,el^(n+1)));G=G+e*q;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=1,2,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)))}
```

As expected, the program gives $\ell = 11$ $n = 1$ $p = 2$, $\ell = 1093$ $n = 1$ $p = 2$, $\ell = 3511$ $n = 1$ $p = 2$. For $\ell = 1093$, see complementary calculations in Remarks 5.2 (i).

4.3. **Numerical test $\mathscr{T}^*_{\mathbb{Q}(2^n)} \neq 1$ for $\ell = 2$, $p > 2$.** We have only to modify the conductor $f_n = p\,2^{n+2}$ of $L = K(\mu_p)$ where $K = \mathbb{Q}(\ell^n)$, then note that we must choose another multiplier for the Stickelberger element and the generator $\mathsf{h} = \mathsf{Mod}(5, \mathsf{el}^{(\mathsf{n}+2)})$ (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 for $a \in [1, f_n]$ we can neglect the subgroup generated by complex conjugation -1 in $\mathrm{Gal}(\mathbb{Q}(\mu_{2^{n+2}\,p})/\mathbb{Q})$:

```
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))))}
```

Since we use characters ψ_n of order 2^n, the program finds the relative p-group at each new layer. 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 2.3:

```
el=2 n=1 p=13  rk(T)=1 T=[13]        el=2 n=2 p=13  rk(T)=2 T=[169,13]
```

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

```
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

VARIANT FOR ANY NUMBER d OF p-PLACES USING THE FACTORIZATION OF Q (mod p)
d (a power of 2) may be optionally specified (e.g. d=1, d=2):
{el=2;for(n=1,12,Q=polcyclo(elˆn);h=Mod(5,elˆ(n+2));H=lift(h);C=3;
forprime(p=5,2*10ˆ4,f=p*elˆ(n+2);cm=Mod(C,f)ˆ-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=gˆ-1;
e=lift(Mod((1-H)*elˆ(-n-2),p));H=H+e*elˆ(n+2);h=Mod(H,f);
e=lift(Mod((1-G)*pˆ-1,elˆ(n+2)));G=G+e*p;g=Mod(G,f);
S=0;hh=1;gg=1;ggm=1;for(u=1,elˆn,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)*xˆu);s=lift(Mod(S,Qp));
for(k=1,d,t=Mod(s,R[k]);if(t==0,print("el=",el," n=",n," p=",p)))))}

Same results as above. No examples with d>1.
```

4.4. **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; if it is not the case, this only gives that very probably $\#\mathscr{C}_K = 1$.

Since with PARI/GP the computation of units implies that of the class number (because of $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P})$), there is no interest to test the p-divisibility of the regulator instead of looking at $\mathsf{K.no}$ (the class number), except to verify that the computation of $\mathscr{T}_K$ (with Programs I, II of § 2.3 computing suitable ray-class groups) is exact.

The following programs compute (for $\ell > 2$, $n = 1$, then $\ell = 2$, $n \geq 1$ and p given) 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 the $\mathbb{Q}$-base $\{1, x, \ldots, x^{\ell^n-1}\}$ of K, 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 $\mathrm{rank}(M) = \ell^n - 1$ (in each case, one verifies that $\mathsf{K.no} = 1$ (trivial class group C_K)):

```
PROGRAM VIII. TEST ON THE REGULATOR R FOR el>2, n=1
{el=17;p=239;dr=el;if(Mod(pˆ(el-1),elˆ2)==1,dr=1);P=polsubcyclo(elˆ2,el);
Pp=P*Mod(1,pˆ2);K=bnfinit(P,1);E=K.fu;L=List;for(k=1,el-1,e=E[k];
nu=norm(e);e0=Mod(lift(e),Pp);e=e0;for(u=1,dr-1,e=e0*eˆp);le=lift(e-nu);
LogE=0;for(i=0,el-1,c=lift(polcoeff(le,i))/p;LogE=LogE+c*xˆi);
listinsert(L,LogE,1));M=matrix(el-1,el,i,j,Mod(polcoeff(L[i],j),p));
R=matrank(M);print("el=",el," p=",p," rk(M)=",R);
if(R<el-1,print("R_K non-trivial"))}

el=3 p=7  rk(M)=1 R_K non-trivial   el=17 p=239 rk(M)=15 R_K non-trivial
el=3 p=73 rk(M)=1 R_K non-trivial   el=23 p=47  rk(M)=21 R_K non-trivial
el=5 p=11 rk(M)=2 R_K non-trivial   el=29 p=59  rk(M)=27 R_K non-trivial

PROGRAM IX. TEST ON THE REGULATOR R FOR el=2, n>=1
{el=2;n=3;p=521;dr=elˆn;P=x;for(j=1,n,P=Pˆ2-2);
Pp=P*Mod(1,pˆ2);K=bnfinit(P,1);E=K.fu;L=List;for(k=1,2ˆn-1,e0=E[k];
e=Mod(lift(e0),Pp);for(u=1,dr,e=eˆp);le=lift(e*e0ˆ-1-1);LogE=0;
for(i=0,elˆn-1,c=lift(polcoeff(le,i))/p;LogE=LogE+c*xˆi);
listinsert(L,LogE,1));M=matrix(elˆn-1,elˆn,i,j,Mod(polcoeff(L[i],j),p));
R=matrank(M);print("elˆn=",elˆn," p=",p," rk(M)=",R);
if(R<elˆn-1,print("R_K non-trivial"))}

elˆn=2 p=13 rk(M)=0 R_K non-trivial  elˆn=4 p=29 rk(M)=2 R_K non-trivial
elˆn=2 p=31 rk(M)=0 R_K non-trivial  elˆn=4 p=37 rk(M)=2 R_K non-trivial
elˆn=4 p=13 rk(M)=1 R_K non-trivial  elˆn=8 p=521rk(M)=6 R_K non-trivial
```

4.5. **Conjecture about the p-torsion groups $\mathscr{T}_{\mathbb{Q}(\ell^n)}$.** The annihilation Theorem 4.6 allows us to test the non-triviality of $\mathscr{T}_K$, for $K := \mathbb{Q}(\ell^n)$, when direct computation of the structure of this group is out of reach, giving possible non-trivial class groups, because of the identity:

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

(see Lemma 2.1, Remark 2.2 (i), 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 ℓ^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 $\#\mathscr{C}_K^* \neq 1$. Moreover, the Cohen–Lenstra–Martinet heuristics (see [4, 43, 44] for large developments of this aspect) give low probabilities for non-trivial p-class groups, even in the case of residue degree 1 of p in $\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}$.

As for the question of p-rationality of number fields, when K 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.

Conjecture 4.7. *There exist infinitely many triples (ℓ, n, p) with ℓ, p primes, $\ell \neq p$, $n \geq 1$, such that $\frac{1}{2}\,L_p(1,\psi_n) \equiv 0 \pmod{\mathfrak{p}_n}$, for some $\mathfrak{p}_n \mid p$ in $\mathbb{Q}(\mu_{\ell^n})$, where ψ_n is a character of K of order ℓ^n (whence $\mathscr{T}^*_{\mathbb{Q}(\ell^n)} \neq 1$).*

We have seen that the solutions p to $\mathscr{T}_K^* \neq 1$ 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 $\sqrt{D_K} = \ell^N$, where $N = O(n\,\ell^n)$, whence $\sqrt{D_K} = (\ell^n)^{O(\ell^n)}$, whereas the class number fulfills the following general property $\#C_K \leq c_{\ell^n,\epsilon} \cdot (\sqrt{D_K})^{1+\epsilon}$ [1] and (conjecturally) 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 ℓ_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 directly the p-class group $\mathscr{C}_K$ of $K = \mathbb{Q}(N)$ with a suitable component of the p-torsion group $\mathscr{T}_L$ of $L := K(\mu_p)$; these equalities of p-ranks show that, roughly speaking, all these invariants have analogous p-adic properties. But, as p increases, the computations take place in a too large field to get significant examples (if any).

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, with the trivial character; applied with the set S of prime ideals of K above 2, it is given by [15, 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):

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

$$\mathrm{rk}_2(\mathscr{T}_K^{\mathrm{ord}}) = \mathrm{rk}_2\big[\mathscr{C}_K^{\mathrm{res}}/c\ell_K^{\mathrm{res}}(S)\big] + \#S - 1, \tag{3}$$

$$\mathrm{rk}_2(\mathscr{T}_K^{\mathrm{ord}}) = \mathrm{rk}_2\big[\mathscr{C}_K^{\mathrm{ord}}/c\ell_K^{\mathrm{ord}}(S)\big] + \#S - 1, \tag{4}$$

$$\mathrm{rk}_2(\mathscr{C}_K^{(4)\,\mathrm{ord}}) = \mathrm{rk}_2(\mathscr{C}_K^{\mathrm{res}}), \tag{5}$$

$$\mathrm{rk}_2(\mathscr{C}_K^{(4)\,\mathrm{res}}) = \mathrm{rk}_2(\mathscr{C}_K^{\mathrm{ord}}) + \ell^n. \tag{6}$$

Thus, $\mathscr{T}_K^{\rm ord}=1$ (i.e., $\mathscr{C}_K^{\rm ord}=\mathscr{R}_K^{\rm ord}=\mathscr{W}_K^{\rm ord}=1$) if and only if 2 is inert in $K/\mathbb{Q}$ and $\mathscr{C}_K^{\rm ord}=1$ (or 2 is inert and $\mathscr{C}_K^{\rm res}=1$, or 2 is inert and $\mathscr{C}_K^{(4)\rm ord}=1$).

Proof. If $\mathscr{T}_K^{\rm ord}=1$, then $\#S=1$ and 2 is inert in $K/\mathbb{Q}$; since in that case $\mathscr{W}_K=1$ and since $H_K^{\rm ord}\cap K(2^\infty)=K$, we get $\mathscr{C}_K^{\rm ord}=\mathscr{R}_K^{\rm ord}=1$ (in other words, the ordinary 2-class group of K is odd and the normalized regulator is trivial, which can be written $\overline{E_K^1}=U_K^{1*}:=\{u\in U_K^1,\ {\rm N}_{K/\mathbb{Q}}(u)=\pm1\}$). The reciprocal is obvious. Whence the other claims. □

Remarks 5.2. *Let $K=\mathbb{Q}(N)$, for any odd $N>1$.*

(*i*) *If $p=2$ is inert in K, ${\rm rk}_2(\mathscr{T}_K^{\rm ord})={\rm rk}_2(\mathscr{C}_K^{\rm res})={\rm rk}_2(\mathscr{C}_K^{\rm ord})$ ((3), (4)).*
This does not apply for $N=\ell=1093$, 3511 and (unknown) primes ℓ such that the Fermat quotient of 2 modulo ℓ is non-trivial. For $\ell=1093$ and from ${\rm rk}_2(\mathscr{T}_K^{\rm ord})={\rm rk}_2(\mathscr{C}_K^{\rm res}/\mathscr{cl}_K^{\rm res}(S))+1092={\rm rk}_2(\mathscr{C}_K^{\rm ord}/\mathscr{cl}_K^{\rm ord}(S))+1092$, we have verified that the norm of $(1-\psi_1(3))\cdot\frac{1}{2}L_p(1,\psi_1)$ is exactly 2^{1092}; this means that 2 annihilates $\mathscr{T}_K^{\rm ord}$, whence that $\mathscr{C}_K^{S\ {\rm res}}=\mathscr{C}_K^{S\,{\rm ord}}=1$ and that $\mathscr{T}_K^{\rm ord}\simeq(\mathbb{Z}/2\mathbb{Z})^{1092}$. This only proves that $\mathscr{C}_K$ is generated by the classes of the 1093 prime ideals above 2 in K.

(*ii*) *We have used, in reflection theorems, the relation $\mathscr{T}_K^{\rm res}\simeq\mathscr{T}_K^{\rm ord}\bigoplus\mathbb{F}_2^{\ell^n}$* [15, Theorem III.4.1.5], *valid under Leopoldt's conjecture for $p=2$.*

5.2. **Case $p\neq2$.** 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 ${\rm Gal}(L/K)$.

Let $\omega_p=:\omega$ be the Teichmüller character defined by $\zeta^s=\zeta^{\omega(s)}$ for all $\zeta\in\mu_p$ and all $s\in{\rm Gal}(L/K)$; then any $\mathbb{Q}_p$-irreducible character χ of ${\rm Gal}(L/K)$ is of degree 1 of the form ω^k, $1\leq k\leq p-1$. We denote by ${\rm rk}_\chi(A)$ the $\mathbb{F}_p$-dimension of the χ-component of A/A^p; whence ${\rm rk}_1(A)={\rm rk}_p(A)$.

Let S_K and S_L be the sets of p-places in K and L, respectively. Since p is totally ramified in L/K one has $\#S_L=\#S_K$. In $\mathbb{Q}(\ell^\infty)$, for each $\ell\mid N$, this number is given by ℓ^{g_p}, where $p^{\ell-1}=1+\lambda\,\ell^{g_p+1}$, $\ell\nmid\lambda$, in the case $\ell\neq2$, then $\pm p=1+\lambda\,2^{g_p+2}$, λ odd for $\ell=2$ (see § 2.4), whence $\#S_K$ if $n<g_p$.

Let $\mathscr{cl}_K(S_K)\subseteq\mathscr{C}_K$ and $\mathscr{cl}_L(S_L)\subseteq\mathscr{C}_L$ generated by the classes of the prime ideals dividing p in K and L, respectively; we have $\mathscr{cl}_L(S_L)\simeq\mathscr{cl}_K(S_K)$.

Theorem 5.3. *Let $p>2$ be a prime not dividing N. Consider the layer $K:=\mathbb{Q}(N)$ and put $L:=K(\mu_p)$. We have the following equalities:*

$$\begin{aligned}
{\rm rk}_p(\mathscr{T}_K) &= {\rm rk}_\omega(\mathscr{C}_L) &(7)\\
{\rm rk}_p\big[\mathscr{C}_K/\mathscr{cl}_K(S_K)\big] &= {\rm rk}_\omega(\mathscr{T}_L)+1-\#S_K &(8)\\
{\rm rk}_p(\mathscr{C}_K) &= {\rm rk}_\omega(\mathscr{C}_L^{\mathfrak{P}^*})+1-N &(9)\\
{\rm rk}_p\big[{\rm N}_{L/K}(\mathscr{C}_L^{\mathfrak{P}^*})\big] &= {\rm rk}_\omega(\mathscr{C}_L)+1 &(10)
\end{aligned}$$

where $\mathfrak{P}^*=(p)\cdot(1-\zeta_p)$ in L, and $\mathscr{C}_L^{\mathfrak{P}^*}$ is the ray class group of modulus $\mathfrak{P}^*$.

Proof. It suffices to consider the general formula of [15, § II.5.4.2 and Theorem II.5.4.5] in L/K, with the character $\chi=\omega$, hence $\chi^*=1$ giving p-ranks. The formulas are obtained, varying the parameters of ramification or splitting and exchanging the characters χ and χ^*. □

The computation of the ω-component $\mathscr{T}_L^\omega$ of $\mathscr{T}_L$ is not easy from the direct computation of $\mathscr{T}_L$, except for $p=3$ since, in this case $\mathscr{T}_L\simeq\mathscr{T}_K\oplus\mathscr{T}_L^\omega$; thus this reduces to the computation of the 3-ranks of $\mathscr{T}_L$ and $\mathscr{T}_K$. The following program illustrates the formula (8) of the theorem for $N=\ell$ and computes:

$$1+{\rm rk}_\omega(\mathscr{T}_L)-\#S_{K,3}={\rm rk}_3(\mathscr{T}_L)-{\rm rk}_3(\mathscr{T}_K)-\#S_{K,3};$$

note that 3 splits in $\mathbb{Q}(\ell)$ if and only if $3^{\ell-1} \equiv 1 \pmod{\ell^2}$ (the only known primes are $\ell = 11$ and $\ell = 1006003$); whence a particular line for $\ell = 11$ and in general 3 is inert and $c\ell_K(S_{K,3}) = 1$ which yields $\mathrm{rk}_3(\mathscr{C}_K) = \mathrm{rk}_\omega(\mathscr{T}_L)$. We have no counterexamples ($\mathsf{Delta} = 0$ for $\ell = 11$ means $\mathrm{rk}_\omega(\mathscr{T}_L) = 0$):

```
PROGRAM X. OMEGA COMPONENT OF T_L FOR p=3
{p=3;forprime(el=2,100,P=polsubcyclo(el^2,el);N=2;if(el==2,P=x^2-2;N=3);
Q=polcompositum(P,x^2+x+1)[1];L=bnfinit(Q,1);LN=bnrinit(L,p^N);
HpNL=LN.cyc;LL=List;e=matsize(HpNL)[2];R=0;for(k=1,e-(el+1),c=HpNL[e-k+1];
w=valuation(c,p);if(w>0,R=R+1;listinsert(LL,p^w,1)));RL=R+el+1;
print("el=",el," LL=",LL);if(R>0,K=bnfinit(P,1);KpN=bnrinit(K,p^N);
HpN=KpN.cyc;LK=List;e=matsize(HpN)[2];R=0;for(k=1,e-1,c=HpN[e-k+1];
w=valuation(c,p);if(w>0,R=R+1;listinsert(LK,p^w,1)));RK=R+1;
S=1;if(Mod(p^(el-1)-1,el^2)==0,S=el);Delta=1-S+RL-RK-el;
print("el=",el," Delta=",Delta," LK=",LK," LL=",LL)))}

el=2  LL=[]        el=3  LL=[]        el=5 LL=[]        el=7 LL=[]
el=11 LL=[3,3,3,3,3,3,3,3,3,3]   Delta=0   LK=[]
el=13 LL=[]        el=17 LL=[]
```

Unfortunately, for $p > 3$, the computations in $L = K(\mu_p)$ of any $\mathscr{T}_L$, *for an imaginary field* needs the determination (with PARI/GP) of $\mathsf{bnfinit}(\mathsf{Q})$ for a field of degree $\ell^n\,(p-1)$ (conductor $\ell^{n+1}\,p$ for $\ell \neq 2$, $2^{n+2}\,p$ for $\ell = 2$). Which gives a serious limitation of the parameters ℓ, n, p.

5.3. **Illustration of formula (10) of Theorem 5.3.** We can compute, for $N = \ell^n$ and $p \neq 2$, the structure of the group $\mathscr{C}_L^{\mathfrak{P}^*} = \bigoplus_{i=1}^{p-1} \mathscr{C}_L^{\mathfrak{P}^*,\omega^i}$. The parameter $\#\mathsf{zp}$ 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 its conductor is p^2 larger that $\mathfrak{P}^*$; thus, $\#\mathsf{zp} - 1 - \mathsf{rk}(\mathsf{Hp})$, where Hp is the ray class group, measures the p-rank of the torsion part (e.g., $\ell = 2$, $p = 11, 13, 19$).

But the character of this torsion part is unknown; for each odd ω^{2i+1}, $i = 0, \ldots, \frac{p-1}{2} - 1$, the p-rank of the ω^{2i+1}-part of the composite of the $\mathbb{Z}_p$-extensions is ℓ^n, whence the formula (9) for ω. This suggests that these ω^{2i+1}-ranks may be nontrivial since these odd characters play, a priori, the same role (except that ω is "not any character" in many circumstances).

```
PROGRAM XI. ILLUSTRATION OF FORMULA (8) FOR el=2
{el=2;for(n=1,3,print("el=",el," n=",n);P=x;for(j=1,n,P=P^2-2);
forprime(p=3,23,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,
                                      13,13,13,13,13,13,13,13,13,13,13,13]

PROGRAM XII. ILLUSTRATION OF FORMULA (8) FOR el>2
{el=3;for(n=1,2,print("el=",el," n=",n);P=polsubcyclo(elˆ(n+1),elˆn);
forprime(p=5,19,Q=polcompositum(P,polcyclo(p))[1];L=bnfinit(Q,1);
r=elˆn*(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,pˆw,1)));print("p=",p," rk(Hp)=",R," #zp=",r," Hp=",LT)))}

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]
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]
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]
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=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]
```

5.4. **Probabilistic analysis from the reflection theorem.** Consider the following reflection theorem [15, II.5.4.9.2, formula (4)]:

Proposition 5.4. *For $K=\mathbb{Q}(N)$, $N\geq 2$, $L=K(\mu_p)$, $p>2$, $p\nmid N$, then* $\mathrm{rk}_p(\mathscr{C}_K)=\mathrm{rk}_p(Y^\omega_{L,\mathrm{prim}})$, *where:*

$$Y^\omega_{L,\mathrm{prim}}\subseteq Y^\omega_L:=\left(\{\alpha\in L^\times,\ (\alpha)=\mathfrak{A}^p\}\cdot L^{\times p}/L^{\times p}\right)^\omega$$

is the ω-component of the subset of p-primary elements α (i.e., such that $L(\sqrt[p]{\alpha})/L$ is unramified and decomposed over K into a cyclic subfield of H_K^{nr}). 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 $Y^\omega_L=\{\alpha_1,\dots,\alpha_r\}\cup\{\zeta_p\}$ 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 $\mathrm{rk}_p(\mathscr{C}_K)=\mathrm{rk}_p(Y^\omega_{L,\mathrm{prim}})=\mathrm{rk}_p(\langle\alpha_1,\dots,\alpha_r\rangle_{\mathrm{prim}})$. 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 IV 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 is (in a standard point of view) $\frac{1}{p}$.

The computation of the class group of L is 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 § 4.4, that the regulator of K is not a 7-adic unit).

6. The p-torsion groups in $\widehat{\mathbb{Q}}$

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 composite field $K = \mathbb{Q}(N)$, $N = \ell_1^{n_1} \cdots \ell_t^{n_t} \geq 2$, and give larger groups. This field has by nature a cyclic Galois group and lives in the cyclotomic $\widehat{\mathbb{Z}}$-extension $\widehat{\mathbb{Q}}$ of $\mathbb{Q}$, composite of all the $\mathbb{Z}_\ell$-extension $\mathbb{Q}(\ell^\infty)$. So we have essentially to compute $\mathscr{T}_K^*$ (the relative submodule).

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 a composite conductor; we limit to 4 the number of prime divisors of N, which is largely sufficient in practice. All primes p are tested, which will give some cases of annihilators of degree > 1 (hence primes p of residue degree > 1 in $\mathbb{Q}(\mu_N)$). If necessary, the user may specifies that, for example, $p \equiv 1 \pmod N$.

The calculation of c, defining the multiplier $1 - c \cdot \left(\frac{\mathbb{Q}(\mu_f)}{c}\right)^{-1}$, gives some difficulty for even N since for odd N, $c = 2$ 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 $\psi(c) \neq 1$, where ψ is the character of order N of K, 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 the conductor f. Doing this, the case $\psi(c) = 1$ may occur, giving in relation (2), $\psi(\mathscr{A}_K^c) = (1 - \psi(c)) \cdot \frac{1}{2} L_p(1, \psi) = 0$ 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 $\psi(c) = 1$ equivalent to a trivial Artin symbol. Thus, in that case, the program gives necessarily the annihilator $\mathsf{Q} = \mathsf{polcyclo(N)}$ and possibly a false result; a unique case occurs for $N = 10$ and the line ** of the table must be dropped since a direct verification does not give any solution p in the selected interval.

It is easy to prove that, in the even case, since $p \neq 2$, one can neglect the complex conjugation (more precisely the component $\mathrm{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q}(\mu_f)^+)$) in the summation over $a \in [1, f]$ giving the Stickelberger element and its image by the Spiegel involution (this comes essentially from the fact that ψ is even).

Then we shall perform some verifications by using the basic PROGRAMS I, II, § 2.3, when computation via $\mathsf{K} = \mathsf{bnfinit(P)}$ is possible, which holds only for small conductors contrary to the present method with p-adic measures allowing computations up to $N = 200$ 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.

```
PROGRAM XIII.
{BN=200;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;

\\ EVEN CASE
if(Mod(N,2)==0,Nf=factor(N);D=component(Nf,1);Exp=component(Nf,2);
q1=D[1]^Exp[1];listput(Lq,q1,1);Q1=4*q1;listput(LQ,Q1,1);
N1=N/q1;listput(LN,N1,1);NN=Q1;
for(i=2,dim,qi=D[i]^Exp[i];listput(Lq,qi,i);Qi=qi*D[i];listput(LQ,Qi,i);
Ni=N/qi;listput(LN,Ni,i);NN=NN*Qi);
```

```
h1=Mod(5,LQ[1]);listput(Lh,h1,1);H1=lift(h1);listput(LH,H1,1);
for(i=2,dim,hi=znprimroot(LQ[i]);listput(Lh,hi,i));
for(i=2,dim,H=lift(Lh[i]);listput(LH,H,i));
forprime(p=3,Bp,if(Mod(N,p)==0,next);f=p*NN;
Cc=2;while(gcd(Cc,f)!=1,Cc=Cc+1);C=Cc;cm=Mod(C,f)^-1;
Qp=Q*Mod(1,p);F=factor(Q+O(p));R=lift(component(F,1));d=matsize(F)[1];
Rp=List;for(j=1,d,r=R[j]*Mod(1,p);listput(Rp,r,j));
g=znprimroot(p);G=lift(g);gm=g^-1;
M=f/p;E=lift(Mod((1-G)*p^-1,M));G=G+E*p;g=Mod(G,f);
M=f/LQ[1];E=lift(Mod((1-LH[1])*LQ[1]^-1,M));
H=LH[1]+E*LQ[1];h=Mod(H,f);listput(Lh,h,1);
for(j=2,dim,
M=f/LQ[j];E=lift(Mod((1-LH[j])*LQ[j]^-1,M));
H=LH[j]+E*LQ[j];h=Mod(H,f);listput(Lh,h,j));
if(dim>=1,E1=eulerphi(LQ[1]));if(dim>=2,E2=eulerphi(LQ[2]));
if(dim>=3,E3=eulerphi(LQ[3]));if(dim>=4,E4=eulerphi(LQ[4]));
hh1=1;hh2=1;hh3=1;hh4=1;gg=1;ggm=1;
if(dim==1,S=0;
for(u1=1,E1,hh1=hh1*Lh[1];t=0;
for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh1*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,S=0;
for(u1=1,E1,hh1=hh1*Lh[1];for(u2=1,E2,hh2=hh2*Lh[2];
t=0;for(v=1,p-1,gg=gg*g;ggm=ggm*gm;
a=lift(hh1*hh2*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,S=0;
for(u1=1,E1,hh1=hh1*Lh[1];for(u2=1,E2,hh2=hh2*Lh[2];
for(u3=1,E3,hh3=hh3*Lh[3];t=0;
for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh1*hh2*hh3*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,S=0;
for(u1=1,E1,hh1=hh1*Lh[1];for(u2=1,E2,hh2=hh2*Lh[2];
for(u3=1,E3,hh3=hh3*Lh[3];for(u4=1,E4,hh4=hh4*Lh[4];t=0;
for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh1*hh2*hh3*hh4*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))))));

\\ ODD CASE
if(Mod(N,2)!=0,Nf=factor(N);D=component(Nf,1);Exp=component(Nf,2);
NN=1;C=2;
for(i=1,dim,qi=D[i]^Exp[i];listput(Lq,qi,i);Qi=qi*D[i];listput(LQ,Qi,i);
NN=NN*Qi;Ni=N/qi;listput(LN,Ni,i));
for(i=1,dim,hi=znprimroot(LQ[i]);listput(Lh,hi,i));
for(i=1,dim,H=lift(Lh[i]);listput(LH,H,i));
forprime(p=3,Bp,if(Mod(N,p)==0,next);f=p*NN;cm=Mod(C,f)^-1;
Qp=Q*Mod(1,p);F=factor(Q+O(p));R=lift(component(F,1));d=matsize(F)[1];
Rp=List;for(j=1,d,r=R[j]*Mod(1,p);listput(Rp,r,j));
```

```
g=znprimroot(p);G=lift(g);gm=g^-1;
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];h=Mod(H,f);listput(Lh,h,j));
if(dim>=1,E1=eulerphi(LQ[1]));if(dim>=2,E2=eulerphi(LQ[2]));
if(dim>=3,E3=eulerphi(LQ[3]));if(dim>=4,E4=eulerphi(LQ[4]));
hh1=1;hh2=1;hh3=1;hh4=1;gg=1;ggm=1;
if(dim==1,S=0;
for(u1=1,E1,hh1=hh1*Lh[1];t=0;
for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh1*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,S=0;
for(u1=1,E1,hh1=hh1*Lh[1];for(u2=1,E2,hh2=hh2*Lh[2];t=0;
for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh1*hh2*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,S=0;
for(u1=1,E1,hh1=hh1*Lh[1];for(u2=1,E2,hh2=hh2*Lh[2];
for(u3=1,E3,hh3=hh3*Lh[3];t=0;
for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh1*hh2*hh3*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,S=0;
for(u1=1,E1,hh1=hh1*Lh[1];for(u2=1,E2,hh2=hh2*Lh[2];
for(u3=1,E3,hh3=hh3*Lh[3];for(u4=1,E4,hh4=hh4*Lh[4];t=0;
for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh1*hh2*hh3*hh4*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)))))))}
```

```
   N=2   p=13    annihilator = Mod(1,13)*x+Mod(1,13)
   N=2   p=31    annihilator = Mod(1,31)*x+Mod(1,31)
   N=3   p=7     annihilator = Mod(1,7)*x+Mod(5,7)
   N=3   p=73    annihilator = Mod(1,73)*x+Mod(9,73)
   N=4   p=13    annihilator = Mod(1,13)*x+Mod(5,13)
   N=4   p=29    annihilator = Mod(1,29)*x+Mod(12,29)
   N=4   p=37    annihilator = Mod(1,37)*x+Mod(31,37)
   N=5   p=11    annihilator = Mod(1,11)*x+Mod(7,11)
   N=5   p=11    annihilator = Mod(1,11)*x+Mod(8,11)
   N=6   p=7     annihilator = Mod(1,7)*x+Mod(2,7)
   N=6   p=13    annihilator = Mod(1,13)*x+Mod(9,13)
   N=6   p=43    annihilator = Mod(1,43)*x+Mod(36,43)
   N=8   p=3     annihilator = Mod(1,3)*x^2+Mod(1,3)*x+Mod(2,3)
   N=8   p=521   annihilator = Mod(1,521)*x+Mod(206,521)
** N=10  p=3     annihilator = Mod(1,3)*x^4+Mod(2,3)*x^3
                              +Mod(1,3)*x^2+Mod(2,3)*x+Mod(1,3)
   N=12  p=13    annihilator = Mod(1,13)*x+Mod(7,13)
   N=14  p=113   annihilator = Mod(1,113)*x+Mod(106,113)
   N=15  p=31    annihilator = Mod(1,31)*x+Mod(11,31)
   N=15  p=31    annihilator = Mod(1,31)*x+Mod(22,31)
```

```
N=15  p=241   annihilator = Mod(1,241)*x+Mod(81,241)
N=15  p=1291  annihilator = Mod(1,1291)*x+Mod(958,1291)
N=17  p=239   annihilator = Mod(1,239)*x+Mod(172,239)
N=18  p=37    annihilator = Mod(1,37)*x+Mod(33,37)
N=22  p=397   annihilator = Mod(1,397)*x+Mod(16,397)
N=22  p=2729  annihilator = Mod(1,2729)*x+Mod(1268,2729)
N=23  p=47    annihilator = Mod(1,47)*x+Mod(19,47)
N=25  p=101   annihilator = Mod(1,101)*x+Mod(21,101)
N=25  p=1151  annihilator = Mod(1,1151)*x+Mod(744,1151)
N=25  p=2251  annihilator = Mod(1,2251)*x+Mod(1033,2251)
N=27  p=109   annihilator = Mod(1,109)*x+Mod(20,109)
N=28  p=701   annihilator = Mod(1,701)*x+Mod(338,701)
N=29  p=59    annihilator = Mod(1,59)*x+Mod(56,59)
N=30  p=1831  annihilator = Mod(1,1831)*x+Mod(261,1831)
N=33  p=397   annihilator = Mod(1,397)*x+Mod(136,397)
N=38  p=2357  annihilator = Mod(1,2357)*x+Mod(659,2357)
N=39  p=157   annihilator = Mod(1,157)*x+Mod(44,157)
N=40  p=41    annihilator = Mod(1,41)*x+Mod(22,41)
N=40  p=41    annihilator = Mod(1,41)*x+Mod(30,41)
N=40  p=41    annihilator = Mod(1,41)*x+Mod(35,41)
N=43  p=173   annihilator = Mod(1,173)*x+Mod(41,173)
N=45  p=541   annihilator = Mod(1,541)*x+Mod(336,541)
N=47  p=283   annihilator = Mod(1,283)*x+Mod(27,283)
N=48  p=193   annihilator = Mod(1,193)*x+Mod(28,193)
N=50  p=101   annihilator = Mod(1,101)*x+Mod(88,101)
N=50  p=251   annihilator = Mod(1,251)*x+Mod(123,251)
N=50  p=1201  annihilator = Mod(1,1201)*x+Mod(493,1201)
N=52  p=53    annihilator = Mod(1,53)*x+Mod(12,53)
N=52  p=53    annihilator = Mod(1,53)*x+Mod(21,53)
N=52  p=53    annihilator = Mod(1,53)*x+Mod(27,53)
N=52  p=157   annihilator = Mod(1,157)*x+Mod(128,157)
N=54  p=163   annihilator = Mod(1,163)*x+Mod(21,163)
N=56  p=13    annihilator = Mod(1,13)*x^2+Mod(5,13)*x+Mod(5,13)
N=60  p=61    annihilator = Mod(1,61)*x+Mod(43,61)
N=63  p=379   annihilator = Mod(1,379)*x+Mod(302,379)
N=64  p=193   annihilator = Mod(1,193)*x+Mod(160,193)
N=66  p=1321  annihilator = Mod(1,1321)*x+Mod(617,1321)
N=67  p=269   annihilator = Mod(1,269)*x+Mod(176,269)
N=67  p=269   annihilator = Mod(1,269)*x+Mod(208,269)
N=69  p=829   annihilator = Mod(1,829)*x+Mod(532,829)
N=70  p=71    annihilator = Mod(1,71)*x+Mod(40,71)
N=70  p=211   annihilator = Mod(1,211)*x+Mod(76,211)
N=72  p=73    annihilator = Mod(1,73)*x+Mod(28,73)
N=80  p=241   annihilator = Mod(1,241)*x+Mod(124,241)
N=81  p=487   annihilator = Mod(1,487)*x+Mod(287,487)
N=83  p=499   annihilator = Mod(1,499)*x+Mod(312,499)
N=84  p=757   annihilator = Mod(1,757)*x+Mod(685,757)
N=86  p=431   annihilator = Mod(1,431)*x+Mod(145,431)
N=87  p=349   annihilator = Mod(1,349)*x+Mod(157,349)
N=87  p=523   annihilator = Mod(1,523)*x+Mod(62,523)
N=88  p=353   annihilator = Mod(1,353)*x+Mod(17,353)
N=93  p=373   annihilator = Mod(1,373)*x+Mod(307,373)
N=95  p=191   annihilator = Mod(1,191)*x+Mod(132,191)
N=95  p=191   annihilator = Mod(1,191)*x+Mod(137,191)
N=99  p=991   annihilator = Mod(1,991)*x+Mod(91,991)
N=99  p=991   annihilator = Mod(1,991)*x+Mod(818,991)
N=100 p=199   annihilator = Mod(1,199)*x^2+Mod(173,199)*x+Mod(1,199)
N=101 p=607   annihilator = Mod(1,607)*x+Mod(277,607)
N=101 p=607   annihilator = Mod(1,607)*x+Mod(514,607)
```

```
   N=102 p=103   annihilator = Mod(1,103)*x+Mod(83,103)
   N=102 p=103   annihilator = Mod(1,103)*x+Mod(97,103)
   N=104 p=937   annihilator = Mod(1,937)*x+Mod(609,937)
   N=106 p=107   annihilator = Mod(1,107)*x+Mod(39,107)
   N=106 p=107   annihilator = Mod(1,107)*x+Mod(61,107)
   N=107 p=857   annihilator = Mod(1,857)*x+Mod(263,857)
   N=108 p=109   annihilator = Mod(1,109)*x+Mod(24,109)
   N=111 p=223   annihilator = Mod(1,223)*x+Mod(176,223)
   N=115 p=461   annihilator = Mod(1,461)*x+Mod(87,461)
   N=115 p=461   annihilator = Mod(1,461)*x+Mod(103,461)
   N=118 p=709   annihilator = Mod(1,709)*x+Mod(27,709)
   N=124 p=5     annihilator = Mod(1,5)*x^3+Mod(2,5)*x^2+
                                                Mod(2,5)*x+Mod(3,5)
   N=124 p=373   annihilator = Mod(1,373)*x+Mod(139,373)
   N=124 p=373   annihilator = Mod(1,373)*x+Mod(340,373)
   N=126 p=379   annihilator = Mod(1,379)*x+Mod(165,379)
   N=128 p=257   annihilator = Mod(1,257)*x+Mod(113,257)
   N=128 p=641   annihilator = Mod(1,641)*x+Mod(287,641)
   N=129 p=257   annihilator = Mod(1,257)*x^2+Mod(81,257)*x+Mod(1,257)
   N=136 p=137   annihilator = Mod(1,137)*x+Mod(35,137)
   N=138 p=139   annihilator = Mod(1,139)*x+Mod(31,139)
   N=140 p=29    annihilator = Mod(1,29)*x^2+Mod(3,29)*x+Mod(5,29)
   N=144 p=433   annihilator = Mod(1,433)*x+Mod(292,433)
   N=153 p=307   annihilator = Mod(1,307)*x+Mod(178,307)
   N=155 p=311   annihilator = Mod(1,311)*x+Mod(203,311)
   N=156 p=157   annihilator = Mod(1,157)*x+Mod(80,157)
   N=172 p=173   annihilator = Mod(1,173)*x+Mod(143,173)
   N=174 p=349   annihilator = Mod(1,349)*x+Mod(16,349)
   N=178 p=179   annihilator = Mod(1,179)*x+Mod(129,179)
   N=190 p=761   annihilator = Mod(1,761)*x+Mod(94,761)
   N=191 p=383   annihilator = Mod(1,383)*x+Mod(315,383)
   N=191 p=383   annihilator = Mod(1,383)*x+Mod(360,383)
   N=192 p=193   annihilator = Mod(1,193)*x+Mod(115,193)
   N=210 p=211   annihilator = Mod(1,211)*x+Mod(59,211)
   N=210 p=211   annihilator = Mod(1,211)*x+Mod(154,211)
```

The case of

```
N=8  p=3  annihilator = Mod(1,3)*x^2+Mod(1,3)*x+Mod(2,3)
```

is the first annihilator of degree > 1; since (from the table) $\mathscr{T}_K$ is annihilated by the relative norm $x^4+1 \equiv (x^2+x+2)(x^2+2x+2) \pmod 3$ and since 3 is totally inert, the result gives at least a 3-rank 2. This is validated by the (highly reliable) standard program as:

```
N=8  p=3  rk(T)=2  T=List([3,3])
```

We give below some verifications still using the standard program giving the structure of $\mathscr{T}_K$; only small N can be tested because of the instructions $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P}); \mathsf{KpN} = \mathsf{bnrinit}(\mathsf{K}, \mathsf{p}^{\mathsf{N}})$.

```
PROGRAM XIV. COMPUTATION OF T IN COMPOSITE FIELDS K - SOME VERIFICATIONS
{P1=polsubcyclo(3^2,3);P2=polsubcyclo(5^2,5);P=polcompositum(P1,P2)[1];
K=bnfinit(P,1);print("h=",K.no);N=8;forprime(p=2,1000,KpN=bnrinit(K,p^N);
HpN=KpN.cyc;L=List;e=matsize(HpN)[2];R=0;for(k=1,e-1,c=HpN[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)=",R," T=",L)))}

{P1=x^2-2;P2=polsubcyclo(7^2,7);P=polcompositum(P1,P2)[1];K=bnfinit(P,1);
print("h=",K.no);N=8;forprime(p=2,1000,KpN=bnrinit(K,p^N);HpN=KpN.cyc;
L=List;e=matsize(HpN)[2];R=0;for(k=1,e-1,c=HpN[e-k+1];
w=valuation(c,p);if(w>0,R=R+1;listinsert(L,p^w,1)));
if(R>0,print("p=",p," T=",L)))}
(a) Field K=Q(14)   Cl=1
    p=13  T=[13]              p=31 T=[31]         p=113  T=[113]
```

```
(b) Field K=Q(6)    Cl=1
    p=7   T=[7,7]             p=43  T=[43]          p=31  T=[31]
    p=13  T=[13,13]           p=73  T=[73]
(c) Field K=Q(30)   Cl=1
    p=7   T=[7,7]             p=13  T=[13,13]       p=43  T=[43]
    p=11  T=[11,11]           p=31  T=[31,31,31]    p=73  T=[73]
(d) Field K=Q(42)   Cl=1
    p=7   T=[49,49,7,7]       p=13  T=[13,13]
(e) Field K=Q(21)   Cl=1
    p=7   T=[49,7]
(f) Field K=Q(12)   Cl=1
    p=3   T=[9,9]             p=29  T=[29]          p=43  T=[43]
    p=7   T=[7,7]             p=31  T=[31]          p=73  T=[73]
    p=13  T=[169,169,13,13]   p=37  T=[37]
(g) Field K=Q(15)   Cl=1
    p=7   T=[7]               p=31  T=[31,31]
    p=11  T=[11,11]           p=73  T=[73]
```

Remark 6.1. *The composite K of $k=\mathbb{Q}(6)$ with $\mathbb{Q}(7)$ for $p=7$ has some interest since $\mathscr{T}_K \simeq (\mathbb{Z}/7\mathbb{Z})^2$ (from example (d) above); so we know that $\mathscr{T}_K^{\mathrm{Gal}(K/k)} \simeq \mathscr{T}_k$, 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 $\mathscr{T}_K^* \simeq (\mathbb{Z}/7^2\mathbb{Z})^2$. The groups $\mathscr{T}_k$ and $\mathscr{T}_K$, annihilated by $\mathrm{N}_{K/\mathbb{Q}(14)}$, are modules over $\mathbb{Z}[\mu_3]$ in which $p=7$ is inert; whence the residue degree 2 and the structures obtained (note that the case $N=42$ does not appear in the table of Program XIII because of the condition $p \nmid N$).*

6.2. **Use of Genus theory.** We consider, in the cyclotomic $\widehat{\mathbb{Z}}$-extension $\widehat{\mathbb{Q}}$ of $\mathbb{Q}$, composite of all the $\mathbb{Z}_\ell$-extension $\mathbb{Q}(\ell^\infty)$, any subfield of degree finite or infinite, and fix a prime p (see [47] for analytic results of non-divisibility in this context). Such a field (finite or infinite) can be written $K =: \mathbb{Q}(\mathscr{L}^{\mathscr{N}})$, $\mathscr{L}=\{\ell_1,\dots,\ell_t,\dots\}$, $\mathscr{N}=\{n_1,\dots,n_t,\dots\}$, with an obvious meaning; when $\mathscr{L}$, $\mathscr{N}$ are finite, $K =: \mathbb{Q}(N)$, $N=\prod_{i=1}^m \ell_i^{n_i}$.
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 written as composite $F = K\,\mathbb{Q}(p^m)$, $K \subset \widehat{\mathbb{Q}}^*$, $m \geq 1$.

In the first case, we are in a generalization of Weber's problem. In the second one the problem is in some sense related to genus theory, whence to Greenberg's conjecture [29], for which one very strongly admits that $\#\mathscr{C}_{K\mathbb{Q}(p^m)}$ is constant for all $m \gg 0$ (i.e., the invariants λ, μ of K for the prime p are zero); see for instance [9, 28, 40] for some developments. But we have:

Theorem 6.2. *Let $K=\mathbb{Q}(N) \subset \widehat{\mathbb{Q}}^*$ for some prime p and let $m \geq 0$. Then, under Leopoldt's conjecture, $\mathscr{T}_{K\mathbb{Q}(p^m)}=1$, if and only if $\mathscr{T}_K=1$.*

Proof. Since $K\mathbb{Q}(p^m)/K$ is p-ramified, the claim comes from the fixed points formula giving here $\mathscr{T}_{K\mathbb{Q}(p^m)}^{\mathrm{Gal}(K\mathbb{Q}(p^m)/K)} \simeq \mathscr{T}_K$ ([15, Theorem IV.3.3], [18, Proposition 6], [27, Appendix A.4.2]). □

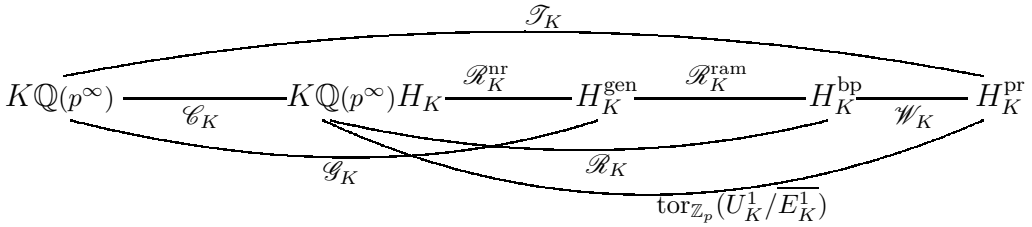
6.3. **The p-class group of $\mathbb{Q}(N)\,\mathbb{Q}(p^m)$ – Use of genus theory.** The analog of Weber's problem in $\widehat{\mathbb{Q}}$ may be doubtful because of Chevalley's formula in an extension F/K with $K := \mathbb{Q}(N)$ fixed (with $N \neq 1$) and $F := K\mathbb{Q}(p^m)$ ($m \geq m_0+1$ if $K \cap \mathbb{Q}(p^\infty) = \mathbb{Q}(p^{m_0})$),

in which p is totally ramified:

$$\#(C_F^{\rm res})^{{\rm Gal}(F/K)} = \#C_K^{\rm res} \cdot \frac{p^{(m-m_0)\,(s_p-1)}}{(E_K^{\rm pos} : E_K^{\rm pos} \cap {\rm N}_{F/K}(F^\times))},$$

where s_p is the number of prime ideals $\mathfrak{p} \mid p$ in K. So $\mathscr{C}_F^{\rm res} = 1$ as soon as $\mathscr{C}_K^{\rm res} = 1$ and p does not split in $K/\mathbb{Q}$. If $s_p > 1$, the right factor of the formula may be a power of p depending of local properties of the units of K.

6.3.1. *Fundamental relation with $\mathscr{R}_K$.* Consider the general diagram [28, Diagram 3] in which $H_K^{\rm gen}$ (with $\mathscr{G}_K := {\rm Gal}(H_K^{\rm gen}/K\mathbb{Q}(p^\infty))$) is the union of the genus fields $H_{K\mathbb{Q}(p^\mu)/K}$ (maximal abelian p-extensions of K, unramified over $K\mathbb{Q}(p^\mu)$; it follows that $H_K^{\rm gen}$ is the maximal unramified extension of $K\mathbb{Q}(p^\infty)$ in $H_K^{\rm pr}$ [28, Proposition 3.6]):



We have the following result about $\frac{p^{(m-m_0)\,(s_p-1)}}{(E_K^{\rm pos} : E_K^{\rm pos} \cap {\rm N}_{F/K}(F^\times))}$, in relation with Greenberg's conjecture ([21, Theorem 4.7], [26, Section 3], [28, Proposition 3.3] for more information after the pioneering Taya's work [55, Theorem 1.1]).

Theorem 6.3. *Let $K = \mathbb{Q}(N) \subset \widehat{\mathbb{Q}}^*$ (i.e., $p \nmid N$) and let $F := K\mathbb{Q}(p^m)$. Then the factor $\frac{p^{m\,(s_p-1)}}{(E_K^{\rm pos} : E_K^{\rm pos} \cap {\rm N}_{F/K}(F^\times))}$ divides $\#\mathscr{R}_K^{\rm nr}$. If p totally splits in K, then for all m large enough there is equality (*[28, Theorem 1]*).*

Corollary 6.4. *If $p \nmid N$ totally splits in $K = \mathbb{Q}(N)$, there exists $m \geq 0$ such that the p-class group of the composite $K\mathbb{Q}(p^m)$ is non-trivial, if and only if $\mathscr{R}_K^{\rm nr} \neq 1$.*

Remarks 6.5. (*i*) *When p totally splits in K, the subgroup $\mathscr{R}_K^{\rm ram}$ is generated by the inertia groups $U_{K_\mathfrak{p}}^1/\overline{E_K^1} \cap U_{K_\mathfrak{p}}^1$, $\mathfrak{p} \mid p$.*

The test $\mathscr{R}_K^{\rm nr} \neq 1$ is equivalent to the computation of the rank of a $\mathbb{F}_p$-matrix with PROGRAMS XV-XVIII.

(*ii*) *Under the assumption $\mathscr{C}_K^{\rm res} = 1$, $\mathscr{C}_F^{\rm res} \neq 1$ is equivalent to $\frac{p^{m\,(s_p-1)}}{(E_K^{\rm pos} : E_K^{\rm pos} \cap {\rm N}_{F/K}(F^\times))} \neq 1$; in the simplest case where p totally splits in K and $m = 1$, then $E_K^{\rm pos} \cap {\rm N}_{F/K}(F^\times) \subseteq U_K^p$.*

(*iii*) *We observe that most of the case $\mathscr{T}_K \neq 1$ are such that $p \equiv 1 (\mathrm{mod}\ \ell^n)$, which may give smallest p-ranks, but such that $p \not\equiv 1 \pmod{\ell^{n+1}}$ (or $\bmod 2^{n+2}$), which implies the non-total splitting of p in K, whence a less probability of non-trivial $\mathscr{C}_F$, $F \subset K\mathbb{Q}(p^m)$. The exceptional case were $(\ell^n, p) = (2^8, 18433)$, $(2^{10}, 114689)$, $(3, 73)$, $(3^4, 487)$, $(5^2, 2251)$.*

6.3.2. *Search for counterexamples of principality in $\widehat{\mathbb{Q}}$.* Any composite F of $K = \mathbb{Q}(\ell)$ with $\mathbb{Q}(p)$ gives huge conductors limiting computations of whole class groups C_F. We have done the following ones (in the restricted sense):

```
PROGRAM XV. COMPUTATION OF CF IN COMPOSITE FIELDS F
{PK=x^2-2;P=polsubcyclo(7^2,7);Q=polcompositum(PK,P)[1];
F=bnfinit(Q,1);print("CF=",F.no," CF'=",bnfnarrow(F))}

F=Q(2)Q(7)     CF=1  CF'=[1,[],[]]     F=Q(2)Q(3)Q(7)  CF=1  CF'=[1,[],[]]
```

```
F=Q(2)Q(3)Q(5) CF=1  CF'=[1,[],[]]

{PK=polsubcyclo(11^2,11);P=polsubcyclo(3^2,3);Q=polcompositum(PK,P)[1];
F=bnfinit(Q,1);print(F.no)}
F=Q(11)Q(3)    CF=1                    F=Q(5)Q(7)  CF=1
```

In all cases, $\#C_F = 1$, giving the following observations:

(*i*) $K = \mathbb{Q}(2)$, $F = K\mathbb{Q}(7)$, $p = 7$, is the minimal case with splitting since 7 splits in $K/\mathbb{Q}$, but $\frac{7}{(E_K : E_K \cap \mathrm{N}_{F/K}(F^\times))} = 1$. Same results replacing $p = 7$ by $p = 17$ (with more computing time). In that cases, $\mathscr{T}_K = \mathscr{T}_F = 1$.

(*ii*) $K = \mathbb{Q}(2)$, $F = K\mathbb{Q}(3)\mathbb{Q}(5)$, all the decomposition groups are equal to $\mathrm{Gal}(F/\mathbb{Q})$ and the p-torsion groups of F are trivial for $p = 2, 3, 5$.

(*iii*) $K = \mathbb{Q}(2)$, $F = K\mathbb{Q}(3)\mathbb{Q}(7)$, 7 totally splits in $\mathbb{Q}(2)\mathbb{Q}(3)$, $\#\mathscr{T}_{\mathbb{Q}(3)} = 7$.

(*iv*) $K = \mathbb{Q}(11)$, $F = \mathbb{Q}(11)\mathbb{Q}(3)$, $p = 3$ splits, $\frac{3^{10}}{(E_K : E_K \cap \mathrm{N}_{F/K}(F^\times))} = 1$. Note that as $\mathbb{Z}[\mu_{11}]$-module, $E_K/E_K \cap \mathrm{N}_{F/K}(F^\times)$ is, a priori, isomorphic to $(\mathbb{F}_{3^5})^h$, $0 \leq h \leq 2$ since the residue degree of 3 in $\mathbb{Q}[\mu_{11}]$ is 5.

(*v*) $K = \mathbb{Q}(5)$, $F = \mathbb{Q}(5)\mathbb{Q}(7)$, $p = 7$ splits, $\frac{7^4}{(E_K : E_K \cap \mathrm{N}_{F/K}(F^\times))} = 1$; a priori, $E_K/E_K \cap \mathrm{N}_{F/K}(F^\times) \simeq (\mathbb{F}_{7^4})^h$, $0 \leq h \leq 1$.

A this step we did not find counterexamples because of $\mathsf{F} = \mathsf{bnfinit}(\mathsf{Q})$ limiting degrees and conductors. So we must restrict ourselves to computation of p-class groups in p-extensions F/K via Chevalley's formula. In fact the literature does contain few counterexamples (see Coates [8, Section 3], relating results from Fukuda–Komatsu, Horie [32, 33]). We shall examine these cases and try to find others or to become aware of the rarity of them, by computing Hasse's normic symbols, in F/K, of the units of K, using a trick due to the "product formula" of class field theory.

6.3.3. *Search for counterexamples of p-principality in p-extensions.* Let $K = \mathbb{Q}(\ell)$, $\ell \geq 2$, and let $p \neq \ell$ totally split in $K/\mathbb{Q}$; let $F := K\mathbb{Q}(p)$. The computation of the index $(E_K : E_K \cap \mathrm{N}_{F/K})$ is easy and only needs to compute $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P})$, instead of $\mathsf{F} = \mathsf{bnfinit}(\mathsf{Q})$, to get the units of K. The Remark 6.5 gives a mean to compute this index, but the test of local pth power may be replaced by that of local normic Hasse's symbols. Then, following the practical method described in [15, II.4.4.3], the normic symbol $(\varepsilon, F/K)_{\mathfrak{p}}$ 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):

$$\begin{aligned} \alpha &\equiv \varepsilon \pmod{\mathfrak{p}^2}, \\ \alpha &\equiv 1 \pmod{(p^2\mathfrak{p}^{-2}}. \end{aligned}$$

Then (α) is an ideal, prime to p, whose Artin symbol in $\mathrm{Gal}(F/K)$ characterizes the normic symbol; the image of this symbol in $\mathrm{Gal}(\mathbb{Q}(p)/\mathbb{Q})$ is given by the Artin symbol of $\mathrm{N}_{F/\mathbb{Q}(p)}(\alpha)$, seen in $(\mathbb{Z}/p^2\mathbb{Z})^\times$. Finally, taking into account the "product formula", the $\mathbb{F}_p$-rank of the matrix of this symbols gives ($(E_K : E_K \cap \mathrm{N}_{F/K}(F^\times)) = p^{\ell-1}$ if and only if this rank is $\ell - 1$).

Various programs are given; the variables $\mathsf{M1}, \mathsf{M2}$ denote the modulus $\mathfrak{p}^2$ and $(p^2)\mathfrak{p}^{-2}$, the variable $\mathsf{m} = \mathsf{M1} + \mathsf{M2}$ allows the above congruence satisfied by α (in Z). The last programs assume that $C_{\mathbb{Q}(\ell)} = 1$, which allows computing with cyclotomic units (as given in [56, Lemma 8.1 (a)]) without the function $\mathsf{bnfinit}(\mathsf{P})$, unfeasible for $\ell > 17$; thus we can compute the $\mathbb{F}_p$-rank (in rkM) of the matrix M for larger primes p.

```
PROGRAM XVI. RANK OF THE MATRIX OF NORMIC SYMBOLS FOR el=2, n=1
{el=2;P=x^2-2;K=bnfinit(P,1);E=K.fu[1];forprime(p=1,2*10^9,
if(kronecker(p,2)!=1,next);g=znprimroot(p^2);F=bnfisintnorm(K,p);
m1=Mod(F[1],P);m2=Mod(F[2],P);M1=m1^2;M2=m2^2;m=M1+M2;Z=E+(1-E)*M1/m;
N=Mod(norm(Z),p^2);Ln=znlog(N,g);if(Mod(Ln,p)==0,print("p=",p,"rkM=0")))}
or
```

```
{el=2;P=x^2-2;K=bnfinit(P,1);E=K.fu[1];forprime(p=3,10^9,
if(kronecker(p,2)!=1,next);F=bnfisintnorm(K,p);
m1=Mod(F[1],P);m2=Mod(F[2],P);M1=m1^2;M2=m2^2;m=M1+M2;Z=E+(1-E)*M1/m;
N=Mod(norm(Z),p^2);Ln=Mod(N,p^2)^(p-1);if(Ln==1,print("p=",p,"rkM=0")))}

el=2    p=31   rkM=0              el=2    p=1546463    rkM=0

PROGRAM XVII. RANK OF THE MATRIX OF NORMIC SYMBOLS FOR el>2, n=1
{el=3;P=polsubcyclo(el^2,el);K=bnfinit(P,1);e=K.fu;
forprime(p=1,2*10^5,if(Mod(p^(el-1),el^2)!=1,next);g=znprimroot(p^2);
A=bnfisintnorm(K,p);W=List;for(k=1,el-1,E=Mod(e[k],P);V=List;
for(j=1,el-1,m1=Mod(A[j],P);m2=p/m1;M1=m1^2;M2=m2^2;m=M1+M2;
Z=E+(1-E)*M1/m;N=Mod(norm(Z),p^2);F=Mod(znlog(N,g),p);listput(V,F));
listput(W,V));M=matrix(el-1,el-1,u,v,W[u][v]);r=matrank(M);
if(r<el-1,print("el=",el," p=",p," rkM=",r)))}

el=3     p=73      rkM=1
```

For these known counterexamples, $\#\mathscr{T}_K = p$, which indicates that $\#\mathscr{R}_K = p$ since $\mathscr{C}_K = 1$ (see Section 4.4). The case $\ell = 3$, $n = 1$, $p = 73$ may be elucidate in more details; indeed, with the defining polynomial $P = x^3 - 3\,x + 1$, 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 $\mathscr{R}_K^{\mathrm{ram}} = 1$, $\mathscr{R}_K^{\mathrm{nr}} = \mathscr{T}_K$, as expected.

In the case $\ell = 5$, $n = 2$, $p = 2251$ totally splits in $K/\mathbb{Q}$; some partial computations in E_K/E_K^{2251} (of order 2251^{24}) indicate, as expected from the previous matrix rank computation, that the $(\varepsilon_i)^{2250} = 1 + 2251 \cdot \alpha_i$, with non-independent α_i modulo 2251, which implies that the inertia groups $\mathrm{tor}_{\mathbb{Z}_{2251}}(U_{\mathfrak{p}_i}/\overline{E_K} \cap U_{\mathfrak{p}_i})$, for $1 \leq i \leq 24$, generate $\mathscr{T}_K = \mathscr{R}_K$ of order p.

This shows that a direct p-adic computation on the units is hopeless contrary to the use of local norm symbols.

```
PROGRAM XVIII. RANK OF THE MATRIX OF NORMIC SYMBOLS FOR LARGE el>2
(computations with cyclotomic units)
{el=17;hh=znprimroot(el^2);h=hh^el;H=hh^(el-1);z=exp(2*I*Pi/el^2);P=1;
for(k=1,el,c=H^k;u=1;
for(j=1,(el-1)/2,u=u*(z^(lift(c*h^j))+z^-(lift(c*h^j))));
P=P*(x-u));P=round(P);e=nfgaloisconj(P);
forprime(p=1,2*10^5,if(Mod(p^(el-1),el^2)!=1,next);g=znprimroot(p^2);
for(aa=1,p-1,T=norm(Mod(x-aa,P));v=valuation(T,p);if(v==1,a=aa;break));
A=List;for(k=1,el,listput(A,e[k]-a,k));W=List;for(j=1,el,E=Mod(e[j],P);
V=List;for(k=1,el,m1=Mod(A[k],P);m2=Mod(1,P);
for(i=1,k-1,m2=m2*Mod(A[i],P));for(i=k+1,el,m2=m2*Mod(A[i],P));
M1=m1^2;M2=m2^2;m=M1+M2;Z=E+(1-E)*M1/m;
N=Mod(norm(Z),p^2);Ln=Mod(znlog(N,g),p);listput(V,Ln));
listput(W,V));M=matrix(el,el,u,v,W[u][v]);r=matrank(M);
if(r<el-1,print("el=",el," p=",p," rank(M)=",r));
print("control: ","p=",p," valuation=",v," root=",a," rank(M)=",r))}

PROGRAM XIX. RANK OF THE MATRIX OF NORMIC SYMBOLS FOR POWERS OF el=2
(computations with cyclotomic units)
\p {128}
{el=2;n=4;H=Mod(5,el^(n+2));z=exp(2*I*Pi/(el^(n+2)));P=1;
for(j=1,el^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);forprime(p=3,2*10^5,
w=n+3-valuation(p+1,2)-valuation(p-1,2);if(w>0,next);g=znprimroot(p^2);
for(aa=1,p-1,T=norm(Mod(x-aa,P));v=valuation(T,p);if(v==1,a=aa;break));
```

```
A=List;for(k=1,el^n,listput(A,e[k]-a,k));W=List;
for(j=1,el^n,E=Mod(e[j],P);V=List;for(k=1,el^n,m1=Mod(A[k],P);m2=Mod(1,P);
for(i=1,k-1,m2=m2*Mod(A[i],P));for(i=k+1,el^n,m2=m2*Mod(A[i],P));
M1=m1^2;M2=m2^2;m=M1+M2;Z=E+(1-E)*M1/m;
N=Mod(norm(Z),p^2);Ln=Mod(znlog(N,g),p);listput(V,Ln));
listput(W,V) );M=matrix(el^n,el^n,u,v,W[u][v] );r=matrank(M);
if(r<el^n-1,print("el^n=",el^n," p=",p,"  rank(M)=",r));
print("control: ","p=",p," valuation=",v," root=",a," rank(M)=",r))}
el^n=8   p=31    rank(M)=6
```

Remark 6.6. *We have performed such computations as follows with Programs XV–XVIII (several days of calculations):*

(i) $\ell^n = 2, 3, 4, 5, 7, 8, 11$ *in very large intervals of primes* p,

(ii) $\ell^n = 13, 17, 19, 23, 29$, *up to* $p \leq 2 \cdot 10^5$ *or* $3 \cdot 10^4$,

(iii) $\ell^n = 2^4$, *up to* $1.2 \cdot 10^6$, $\ell^n = 2^5$, *up to* $p = 35969$,

(iv) $\ell^n = 41$ *up to* $p = 7211$, *and some others in smaller intervals,*

without finding new solutions. This enforces [8, 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 [20, 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, including sometimes a huge one !

6.3.4. *On the conjectural triviality of the logarithmic class groups in* $\widehat{\mathbb{Q}}$. The following result (from Jaulent [39, Theorem 4.5, Remarques]) is perhaps a key to understand some phenomena in the composite $\widehat{\mathbb{Q}}$ of all the cyclotomic $\mathbb{Z}_\ell$-extensions, regarding Greenberg's conjecture:

Theorem 6.7. *Let* $K = \mathbb{Q}(N) \subset \widehat{\mathbb{Q}}^*$, *for some prime* $p \nmid N$ *and* $m \geq 0$. *Under the Leopoldt and Gross–Kuz'min conjectures for* p, $\widetilde{\mathscr{C}}_{K\mathbb{Q}(p^m)} = 1$ *if and only if* $\widetilde{\mathscr{C}}_K = 1$.

Proof. Since the extension is unramified, in the logarithmic sense, the fixed points formula becomes in our context $(\widetilde{\mathscr{C}}_{K\mathbb{Q}(p^m)})^{\mathrm{Gal}(K\mathbb{Q}(p^m)/K)} \simeq \widetilde{\mathscr{C}}_K$. □

This gives many cases of triviality; moreover, we know that $\widetilde{\mathscr{C}}_K = 1$ implies that Greenberg's conjecture holds true in $K\mathbb{Q}(p^\infty)$ for the p-class groups ($\lambda = \mu = 0$). For the base fields $K = \mathbb{Q}(2)$ and $K = \mathbb{Q}(3)$, the logarithmic class groups $\widetilde{\mathscr{C}}_K$ are trivial for $p = 31$ and 73, respectively:

```
PROGRAMS XX. COMPUTATION OF LOGARITHMIC CLASS GROUPS
{el=2;p=31;P=x^2-2;K=bnfinit(P,1);cl=K.no;clog=bnflog(K,p);
print("el=",el," p=",p," cl=",cl," clog=",clog)}
el=2    p=31    cl=1    clog=[[],[],[]]

{el=3;p=73;P=polsubcyclo(3^2,3);K=bnfinit(P,1);cl=K.no;clog=bnflog(K,p);
print("el=",el," p=",p," cl=",cl," clog=",clog)}
el=3    p=73    cl=1    clog=[[],[],[]]
```

So, even if in our computations, for $F = K\,\mathbb{Q}(31) = \mathbb{Q}(2)\,\mathbb{Q}(31)$ ($p = 31$) and for $F = K\,\mathbb{Q}(73) = \mathbb{Q}(3)\,\mathbb{Q}(73)$ ($p = 73$), the ordinary class groups $\mathscr{C}_F$ are non-trivial, it follows that the logarithmic class groups $\widetilde{\mathscr{C}}_F$ are trivial for all the tested primes p, including $31, 73$.

6.3.5. *Decomposition groups in* $\widehat{\mathbb{Q}}/\mathbb{Q}$. 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 this extension D_p which is necessarily of the form $\mathbb{Q}(N)$. Since the number ℓ^{g_p} of prime ideals above p in a single $\mathbb{Z}_\ell$-extension $\mathbb{Q}(\ell^\infty)$ is finite and given by $p^{\ell-1} =: 1+\lambda\,\ell^{1+g_p}$ for $\ell \neq 2$, $p =: \pm 1+\lambda\,2^{2+g_p}$ for $\ell = 2$, $\lambda \not\equiv 0 \pmod{\ell}$, the integers $n \in \mathscr{N}$ are finite numbers but not necessarily the set $\mathscr{L}$. 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 $D_2 = \mathbb{Q}(1093)\,\mathbb{Q}(3511)$.

6.4. **Conclusion and questions.** Genus theory has succeeded to give few non-trivial class groups of *composite subfields* of $\widehat{\mathbb{Q}}$, but there are not enough computations to give more precise heuristics since it is not possible to use PARI/GP with higher degrees. This invites to ask for some questions about the arithmetic properties of $\widehat{\mathbb{Q}}$:

(*i*) Is the decomposition group of p in $\widehat{\mathbb{Q}}/\mathbb{Q}$ of finite index in $\mathrm{Gal}(\widehat{\mathbb{Q}}/\mathbb{Q})$? As recalled above, this is the conjecture given in [20, Conjecture 8.4]. Of course, this seems linked to the order of magnitude of p since, taking a prime of the form $p = 1+\lambda\,q_1^{a_1}\cdots q_s^{a_s}$, with primes q_i, $a_i \geq 2$, this gives unbounded indices since p splits in $\mathbb{Q}(q_1^{a_1-1}\cdots q_s^{a_s-1})$.

(*ii*) Let $K = \mathbb{Q}(N)$, $N \geq 2$, and for any p unramified in K, let s_p be the number of p-places of K. Let $F = K\,\mathbb{Q}(p^m)$ for m large enough such that $\dfrac{p^{m\,(s_p-1)}}{(E_K^{\rm pos} : E_K^{\rm pos} \cap \mathrm{N}_{F/K}(F^\times))} = {}_{\#}\mathscr{R}_K^{\rm nr}$ (Theorem 6.3); is the set of primes p, such that $\mathscr{R}_K^{\rm nr} \neq 1$, finite in number ? If so, this gives new feature about the units in $\widehat{\mathbb{Q}}$ and is also related to Greenberg's conjecture for the subfields of $\widehat{\mathbb{Q}}$.

(*iii*) In the context of (ii), we have obtained that in the three following cases, where $\mathscr{T}_K \neq 1$ and $\mathscr{C}_K = 1$ (see Programs III and VII, §§ 4.1 and 4.3):

$$\ell = 3,\quad n = 4,\quad p = 487 \equiv 1 \pmod{3^5}, \tag{11}$$

$$\ell = 2,\quad n = 8,\quad p = 18433 \equiv 1 \pmod{2^{11}}, \tag{12}$$

$$\ell = 2,\quad n = 10,\quad p = 114689 \equiv 1 \pmod{2^{14}}, \tag{13}$$

the prime p totally splits in $K = \mathbb{Q}(\ell^n)$ and the p-class group of $F = K\mathbb{Q}(p)$ is divisible by $\dfrac{p^{\ell^n-1}}{(E_K : E_K \cap \mathrm{N}_{F/K}(F^\times))}$, only depending of the p-adic properties of E_K, whence of the group of cyclotomic units, but our PARI/GP programs do not succeed in proving if p divides or not ${}_{\#}C_F$.

In case (11) we have obtained $\widetilde{\mathscr{C}}_K = 1$. What is the order of the logarithmic class group $\widetilde{\mathscr{C}}_K$ for cases (12), (13), of too large degrees ?

(*iv*) Let $K = \mathbb{Q}(N)$ and consider $K\mathbb{Q}(p^m)$, $m \geq 0$; what are the Iwasawa invariants of $\varprojlim\limits_m \mathscr{T}_{K\mathbb{Q}(p^m)}$?

(*v*) In [54] 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 (stated, to simplify, for $K = \mathbb{Q}(\ell^n)$):

$$R_K > c_K(\log(\gamma_K|D_K|))^{\ell^{n-1}(\ell-1)}.$$

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 [24, Conjecture 8.2] a "folk conjecture" about the p-adic object ${}_{\#}\mathscr{T}_K$, which applies to $\mathscr{R}_K$, equal to $\mathscr{T}_K$ for all p large enough, and justified by extensive computations:

Conjecture 6.8. *Let $\mathscr{K}$ be the set of totally real number fields K; for $K \in \mathscr{K}$, let D_K be its discriminant and let $\mathscr{R}_K := \mathrm{tor}_{\mathbb{Z}_p}(\log(U_K^1)/\log(\overline{E_K^1}))$ be its normalized p-adic regulator (see § 2.1). There exists a constant $C_p > 0$ such that:*

$$\log_\infty(\#\mathscr{R}_K) \leq \log_\infty(\#\mathscr{T}_K) \leq C_p \cdot \log_\infty(\sqrt{|D_K|}), \ \textit{for all } K \in \mathscr{K},$$

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

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

[3] 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

[4] 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., vol. 41, Amer. Math. Soc., Providence, RI (2004), pp. 149–157. http://dx.doi.org/10.1090/fic/041

[5] 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. http://www.numdam.org/item/JTNB_2000__12_1_103_0/

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

[7] 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.

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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. https://doi.org/10.1007/978-3-642-55245-8_6

[14] J. Fresnel, Nombres de Bernoulli et fonctions L p-adiques, Séminaire Delange–Pisot–Poitou (Théorie des nombres), Tome **7**(2), (1965-1966), Exposé no. 14, 1–15. http://www.numdam.org/item?id=SDPP_1965-1966__7_2_A3_0

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

[16] 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

[17] G. Gras, Sur la construction des fonctions L p-adiques abéliennes, Séminaire Delange–Pisot–Poitou (Théorie des nombres) **20**(2) (1978–1979), Exposé no. 22, 1–20. http://www.numdam.org/item?id=SDPP_1978-1979__20_2_A1_0

[18] G. Gras, Remarks on K_2 of number fields, J. Number Theory **23**(3) (1986), 322–335. https://doi.org/10.1016/0022-314X(86)90077-6

[19] G. Gras, Théorèmes de réflexion, Journal de Théorie des Nombres de Bordeaux **10**(2) (1998), 399–499. http://www.numdam.org/item/JTNB_1998__10_2_399_0/

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

https://arxiv.org/pdf/1701.02618
[21] 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] 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. https://dergipark.org.tr/en/download/article-file/543993
[23] 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
[24] 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
[25] 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 https://arxiv.org/abs/1709.06388
[26] 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. https://doi.org/10.1007/s40316-018-0108-3
[27] 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
[28] G. Gras, Greenberg's conjecture for totally real number fields in terms of algorithmic complexity. https://arxiv.org/abs/2004.06959
[29] 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
[30] 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
[31] F. Hajir, C. Maire, R. Ramakrishna, On the Shafarevich Group of Restricted Ramification Extensions of Number Fields in the Tame Case. https://arxiv.org/abs/1909.03689
[32] 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
[33] 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
[34] 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
[35] 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
[36] 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
[37] 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. https://doi.org/10.1007/s12188-010-0036-x
[38] 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
[39] 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
[40] 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
[41] J.-F. Jaulent, Annulateurs de Stickelberger des groupes de classes logarithmiques (2020). https://arxiv.org/abs/2003.05768
[42] H. Koch, Galois theory of p-extensions (English translation of *"Galoissche Theorie der p-Erweiterungen"*, 1970), Springer Monographs in Math., Springer, 2002.
[43] 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.pdf https://doi.org/10.4064/aa164-4-4
[44] J.C. Miller, Class numbers in cyclotomic $\mathbb{Z}_p$-extensions, J. of Number Theory **150** (2015), 47–73. https://doi.org/10.1016/j.jnt.2014.11.008
[45] 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). https://doi.org/10.1063/1.3478179
[46] T. Morisawa, On Weber's class number problem, PhD thesis, Waseda University, 2012. http://hdl.handle.net/2065/37750

[47] 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

[48] 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

[49] 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. https://doi.org/10.2748/tmj/1372182725

[50] 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

[51] A. Movahhedi, T. Nguyen Quang Do, Sur l'arithmétique des corps de nombres p-rationnels, Séminaire de Théorie des Nombres, Paris 1987–88, Progress in Math. **81** (1990), 155–200. https://doi.org/10.1007/978-1-4612-3460-9_9

[52] 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

[53] The PARI Group, PARI/GP, version 2.9.0, Université de Bordeaux (2016). http://pari.math.u-bordeaux.fr/

[54] 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

[55] 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

[56] 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

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