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

GEORGES GRAS

ABSTRACT. Let $K := \mathbb{Q}(\ell^n)$, $n \geq 0$, be the nth layer in the cyclotomic $\mathbb{Z}_\ell$-extension of $\mathbb{Q}$. It is conjectured that, for all ℓ and n, K is principal (especially for $\ell = 2$, a conjecture due to Weber). Many studies (Ichimura–Morisawa–Nakajima–Okazaki...) go in this direction, as the Miller use of the Cohen–Lenstra–Martinet heuristics. Nevertheless, we examine in what circumstances 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. This questions the relevance of the conjecture since $\#\mathscr{T}_K = \#\mathscr{C}_K \cdot \#\mathscr{R}_K \cdot \#\mathscr{W}_K$, where $\mathscr{C}_K$ is the p-class group of K, $\mathscr{R}_K$ its normalized p-adic regulator, $\#\mathscr{W}_K = 1$ for $p > 2$, $\#\mathscr{W}_K = 2^{\#\{v,\, v|2\}-1}$ for $p = 2$; nevertheless, no counterexample has been found so far, even using the reflection theorem giving p-ranks equalities between $\mathscr{C}_K$ and a suitable component of $\mathscr{T}_{K(\mu_p)}$. When n increases, some relative components $\mathscr{T}_K^*$ may appear for large p. We give a method (Theorem 4.6), for testing $\#\mathscr{T}_K \neq 1$, allowing larger values of ℓ^n than those of the literature. Finally, we consider the subfields K of the composite $\widehat{\mathbb{Q}}$ of the $\mathbb{Z}_\ell$-extension and give programs finding again some rare cases of non-trivial class groups (Fukuda–Komatsu–Horie) due to genus theory in connection with a deep link involving $\mathscr{R}_K$ (Theorem 6.2) in relation with Greenberg's conjecture as initiated, via p-adic zeta-functions, by Taya. In all attempts, Jaulent's logarithmic class group $\widetilde{\mathscr{C}}_K$, $K \subset \widehat{\mathbb{Q}}$, governing Greenberg's conjecture for K and p, was trivial.

CONTENTS

Date: September 10, 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.

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 (or some deep analytic studies) of the class number has been done by many authors without complete success because of limitation of the order of magnitude of the degree ℓ^n; for instance, the results given in [43, 44, Tables 1, 2] only concerns $\ell^n = 2^7$, 3^4, 5^2, 11, 13, 17, 19, 23, 29, 31 (2^7, 3^4, 29, 31 under GRH). Using PARI/GP [53] programs, any "serious" computation needs the instruction $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P}, 1)$ (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 aspect needs other techniques and we are in a class field theory context. For these reasons, we will use the following trick.

Let K be a number field and let $\mathscr{T}_K$ be the torsion group of $\mathscr{G}_K^{\rm pr} := {\rm Gal}(H_K^{\rm pr}/K)$, 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, $\mathscr{R}_K$ the normalized p-adic regulator and $\mathscr{W}_K$ an obvious factor (see Lemma 2.1 about $\mathscr{W}_K$, in general trivial). Since Leopoldt's conjecture holds in K, 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.

Of course, the good new is that the test on $\mathscr{T}_K$ does not need $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P}, 1)$; it will be explained Section 3 and yields Theorem 4.6. Before we shall compute, in Subsection 2.3, some $\mathscr{T}_K$ by means of a classical program (using $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P}, 1)$) to show that this p-torsion group is non-trivial in some cases of small degrees ℓ^n.

Now we recall some classical properties of these invariants.

1.1. **p-class groups in $\mathbb{Q}(\ell^\infty)$.** We denote by p a prime number and by $\mathscr{A} \simeq A \otimes \mathbb{Z}_p$ the p-Sylow subgroup of any finite abelian group A (e.g., the class group $C_{\mathbb{Q}(\ell^n)}$ of $\mathbb{Q}(\ell^n)$ giving the p-class group $\mathscr{C}_{\mathbb{Q}(\ell^n)}$).

Chevalley's formula [6, p. 406] (1933) for class groups $C_K^{\rm res}$ and $C_k^{\rm res}$ (restricted sense), in any cyclic extension K/k of Galois group G, is in whole generality:

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

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 $(C_{\mathbb{Q}(\ell^n)}^{\rm res})^G = 1$ since ℓ is the unique (totally) ramified prime and since $E_{\mathbb{Q}}^{\rm pos} = 1$. So $\mathscr{C}_{\mathbb{Q}(\ell^n)}^{\rm res} = 1$, 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 $p \neq \ell$.

1.2. **p-torsion group of abelian p-ramification in $\mathbb{Q}(\ell^\infty)$.** The analogous "fixed points formula" for the *ℓ-torsion group* $\mathscr{T}_{\mathbb{Q}(\ell^n)}$, in $\mathbb{Q}(\ell^n)/\mathbb{Q}$ (i.e., $p = \ell$), gives also $\mathscr{T}_{\mathbb{Q}(\ell^n)} = 1$ for all n [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.

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 $C_{\mathbb{Q}(\ell^n)}$) 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 the $\mathscr{C}_{\mathbb{Q}(\ell^n)}$ has no counterexamples as ℓ, n, p vary, but that of the $\mathscr{T}_{\mathbb{Q}(\ell^n)}$ is, on the contrary, not true as we shall see with various numerical experiments.

These invariants of p-torsion were less (numerically) computed than class groups, which is unfortunate because they are of basic use in Galois cohomology since, for all number field K, $\mathscr{T}_K$ is the dual of $\mathrm{H}^2(\mathscr{G}_{K,p}, \mathbb{Z}_p)$ [52], where $\mathscr{G}_{K,p}$ is the Galois group of the maximal p-ramified pro-p-extension of K (ordinary sense); then we have the local-global approach defining the first and second Shafarevich–Tate groups in the simplest framework of p-ramification (see [42, Theorem 3.74]):

$$Ш^i_{K,p} := {\rm Ker}\Big[\mathrm{H}^i(\mathscr{G}_{K,p}, \mathbb{F}_p) \longrightarrow \bigoplus_{v|p} \mathrm{H}^1(\mathscr{G}_{K_v}, \mathbb{F}_p)\Big],\ i = 1, 2,$$

which essentially depend on $V_{K,p}/K^{\times p}$ where:

$$V_{K,p} := \{\alpha \in K^\times,\ (\alpha) = \mathfrak{a}^p,\ \alpha \in K_v^\times,\ \forall v \in S\},$$

giving the Shafarevich formula (see some generalizations with ramification and decomposition in [15, II.5.4.1] as well as in [38], after pioneering works of Haberland–Koch–Neumann–Schmidt); this depends on the p-rank of the S-class group $C_K^S := C_K/\mathscr{C}\ell_K(S)$, where S is the set of p-places of K. Then the reflection theorem obtained by "Kummer duality" gives a precise relation with the p-rank of $\mathscr{T}_K$ ([19] and [15, II.5.4.5 and Theorem III.4.2]).

More generally, 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 relation 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, one speaks of p-rational field; in this case, the Shafarevich–Tate groups are trivial, which has deep consequences as shown for instance in [2] in relation with our conjectures in [20]. 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].

Finally, 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 using a suitable algorithm).

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

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 $H_K^{\rm nr}$ be the p-Hilbert class field of K; then we have $\mathrm{Gal}(H_K^{\rm pr}/H_K^{\rm nr}) \simeq U_K^1/\overline{E_K^1}$. The Leopoldt conjecture leads to the (not so trivial) exact sequence:

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

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

(*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 with the residue of the p-adic zeta function of K).

(*e*) Let $K(p^\infty)$ 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.

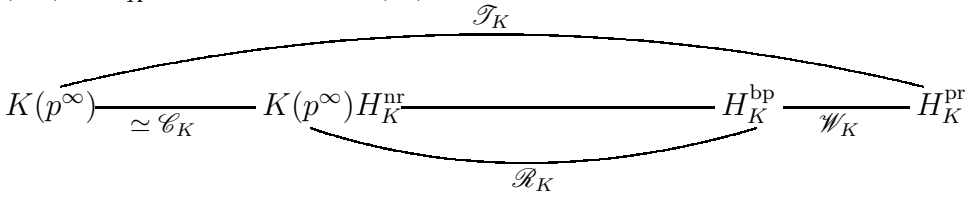
[1] We warmly thank John Coates for sending me his conference paper (loc.cit.), not so easy to find for me, but which contains useful numerical and bibliographical information.

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, $\mathscr{W}_K\simeq\mathbb{F}_2^{\delta_K-1}$ where δ_K is the number of primes $\mathfrak{p}\mid 2$ in K.*

Proof. For $p\neq 2$, the p-completions $K_\mathfrak{p}$ of K (unramified of ℓth power degree) 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 $W_K\simeq\mathbb{F}_2^{\delta_K}$, thus $\mathscr{W}_K\simeq\mathbb{F}_2^{\delta_K-1}$. □

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



Remarks 2.2.
(*i*) *If $\mathscr{W}_K=\mathscr{C}_K=1$, we have $\mathscr{T}_K=\mathscr{R}_K$, 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 only for larger values of ℓ^n and probably more easily when p totally splits in $\mathbb{Q}(\mu_{\ell^n})$ (i.e., $p\equiv 1 \pmod{\ell^n}$); see § 2.4.*
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 $\rho_n>\frac{n\log(\ell)}{\log(p)}$, 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 $C^*_{\mathbb{Q}(\ell^n)}$, 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 by* [4, 9, 10, 13, 34, 35, 36, 37, 45, 46, 48, 49] *(e.g.,* [13, Corollary 1]*).*

2.3. **General computation of $\#\mathscr{T}_{\mathbb{Q}(\ell^n)}$.** We shall 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 $\mathsf{P}=\mathsf{polsubcyclo}(\mathsf{el}^{\mathsf{n}+1},\mathsf{el}^{\mathsf{n}})$ (or $\mathsf{P}=\mathsf{polsubcyclo}(2^{\mathsf{n}+2},2^{\mathsf{n}})$) defining the real field $\mathbb{Q}(\ell^n)$ (they are simplified forms of the general program 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 is specific of the case $\ell=2$ (the Weber context), Program II works for any odd prime ℓ:

```
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))))}
```

```
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, 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)))}
el=2  n=3   p=3     #T=9          el=2  n=3   p=31   #T=31
el=2  n=3   p=13    #T=169        el=2  n=3   p=37   #T=37
el=2  n=3   p=29    #T=29         el=2  n=3   p=521  #T=521
```

```
PROGRAM II. STRUCTURE OF T FOR el>2
{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 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)))}
el=3 n=1 p=7  #T=7       el=5 n=1 p=11  #T=121       el=3 n=1 p=73  #T=73
```

These partial results show that the p-ramification aspects are more complex 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 Subsection 2.4 for more explanations).

Unfortunately, it is not possible in practice to compute easily beyond $\ell = 17$ for various p. 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.** When ℓ and $p \neq \ell$ are fixed, the transfer maps $\mathscr{T}_{\mathbb{Q}(\ell^{n-1})} \to \mathscr{T}_{\mathbb{Q}(\ell^n)}$, $\mathscr{R}_{\mathbb{Q}(\ell^{n-1})} \to \mathscr{R}_{\mathbb{Q}(\ell^n)}$, $\mathscr{C}_{\mathbb{Q}(\ell^{n-1})} \to \mathscr{C}_{\mathbb{Q}(\ell^n)}$, are injective and the arithmetic norms $\mathscr{T}_{\mathbb{Q}(\ell^n)} \to \mathscr{T}_{\mathbb{Q}(\ell^{n-1})}$, $\mathscr{R}_{\mathbb{Q}(\ell^n)} \to \mathscr{R}_{\mathbb{Q}(\ell^{n-1})}$, $\mathscr{C}_{\mathbb{Q}(\ell^n)} \to \mathscr{C}_{\mathbb{Q}(\ell^{n-1})}$, are surjective since $p \neq \ell$; so $\#\mathscr{T}_{\mathbb{Q}(\ell^n)}$, $\#\mathscr{R}_{\mathbb{Q}(\ell^n)}$, $\#\mathscr{C}_{\mathbb{Q}(\ell^n)}$ increase as soon as appear relative submodules in $\mathbb{Q}(\ell^n)/\mathbb{Q}(\ell^{n-1})$.

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

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

Put $K=\mathbb{Q}(\ell^n)$, $n\geq 1$, and $k_i:=\mathbb{Q}(\ell^i)$, $0\leq i\leq n$; since $G_n=\mathrm{Gal}(K/\mathbb{Q})$ 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:

$$\mathscr{M}_K=\bigoplus_{i=1}^{n}\mathscr{M}_K^{\chi_i}=\bigoplus_{i=1}^{n}\mathscr{M}_{k_i}^{*}=\bigoplus_{i=1}^{n}\Big[\bigoplus_{\theta_i\mid\chi_i}\mathscr{M}_{k_i}^{\theta_i}\Big].$$

Then $\mathscr{M}_K^*$ (or any of its component $\mathscr{M}_K^{\theta_n}$) is a module over $\mathbb{Z}[\mu_{\ell^n}]$, hence isomorphic to a product of $\mathbb{Z}[\mu_{\ell^n}]$-modules of the form:

$$\mathbb{Z}[\mu_{\ell^n}]/\mathfrak{p}_n^e,\quad \mathfrak{p}_n\mid p \text{ in } \mathbb{Q}(\mu_{\ell^n}),\ e\geq 1,$$

whose p-rank is a multiple of the residue degree ρ_n of p in the extension $\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}$ (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. *p-class groups in $\mathbb{Q}(\ell^\infty)$.* 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) 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 $n\gg 0$. But this does not give an heuristic for $\mathrm{Prob}(\#\mathscr{C}_K^*=1)$ when n varies.

2.4.3. *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 $\#\mathscr{T}_K^*\equiv 0 \pmod p$ fulfill the relation $p\equiv 1 \pmod{\ell^n}$, 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 $L_n:=K(\mu_p)$, the p-rank of $\mathscr{T}_K^*$ is bounded by that of $\mathscr{C}_{L_n}^*$ (in fact of the ω-component where ω is the Teichmüller character). Thus Washington's theorem may be fulfilled by the torsion groups in the $\mathbb{Z}_\ell$-cyclotomic tower of $\mathbb{Q}$.

2.4.4. *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 (loc. cit.):

$$\mathrm{Prob}\left(\mathscr{R}_K^\theta\equiv 0 \pmod p\right)=\frac{O(1)}{p^{\,\rho\,\delta^2}},$$

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 $K := \mathbb{Q}(\ell^n)$ (for n 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 primes p 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 $\mathscr{T}_K$.

2.5. **Logarithmic class group.** We may also consider another p-adic invariant, the Jaulent's logarithmic class group $\widetilde{\mathscr{C}}_K$ [39] which is linked to 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 $\widetilde{\mathscr{C}}_K$ 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 $p \neq \ell$.

We have computed (for $\ell^n \in \{2^6, 3^3, 5^3, 7, 11, 13, 17, 19, 23, 29\}$) the order of $\widetilde{\mathscr{C}}_{\mathbb{Q}(\ell^n)}$ for all $p \in [2, 2 * 10^5]$ (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 the $\mathscr{T}_K$, 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 and apply them in the particular case of the fields $\mathbb{Q}(\ell^n)$, $\ell \geq 2$ prime, $n \geq 1$, with $p \geq 2$ prime distinct from ℓ.

3.1. **General definition of the Stickelberger elements.** Let $f > 1$ be any conductor and let $\mathbb{Q}(\mu_f)$ be the corresponding cyclotomic field. We define (where the integers a are prime to f and where Artin symbols are taken over $\mathbb{Q}$):

$$\mathscr{S}_{\mathbb{Q}(\mu_f)} := -\sum_{a=1}^{f} \Big(\frac{a}{f} - \frac{1}{2}\Big) \cdot \Big(\frac{\mathbb{Q}(\mu_f)}{a}\Big)^{-1}.$$

The properties of annihilation need to multiply $\mathscr{S}_{\mathbb{Q}(\mu_f)}$ by an element of the annihilator of μ_f, which contains f and the multipliers $1 - c \cdot \big(\frac{\mathbb{Q}(\mu_f)}{c}\big)^{-1}$, for c odd prime to f. This shall give integral elements in the group algebra.

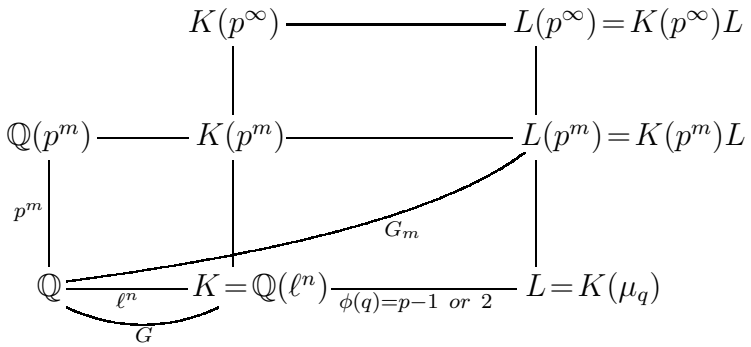
Definition 3.1. *Since* $\frac{f-a}{f} - \frac{1}{2} = -\big(\frac{a}{f} - \frac{1}{2}\big)$, $\mathscr{S}_{\mathbb{Q}(\mu_f)} = \mathscr{S}'_{\mathbb{Q}(\mu_f)} \cdot (1 - s_\infty)$, *where* $s_\infty := \big(\frac{\mathbb{Q}(\mu_f)}{-1}\big)$ *is the complex conjugation and:*

$$\mathscr{S}'_{\mathbb{Q}(\mu_f)} := -\sum_{a=1}^{f/2} \Big(\frac{a}{f} - \frac{1}{2}\Big) \cdot \Big(\frac{\mathbb{Q}(\mu_f)}{a}\Big)^{-1}.$$

Put $q = p$ (resp. 4) if $p \neq 2$ (resp. $p = 2$). For any real abelian number field K, let $L = K(\mu_q)$; we consider $K(p^m) := K\mathbb{Q}(p^m)$ then put $L(p^m) := K(p^m)L = K(\mu_{qp^m})$ for all $m \geq 0$; so $K(p^\infty) = \cup_m K(p^m)$ is the cyclotomic $\mathbb{Z}_p$-extension of K and $L(p^\infty) = \cup_m L(p^m)$ the cyclotomic $\mathbb{Z}_p$-extension of L.

Note, once for all, that the index m is relative to layers in cyclotomic $\mathbb{Z}_p$-extensions contrary to the index n used for the cyclotomic $\mathbb{Z}_\ell$-extension, $\ell \neq p$; indeed, in the particular case $K = \mathbb{Q}(\ell^n)$, $K(p^m) = \mathbb{Q}(\ell^n)\mathbb{Q}(p^m)$.

When $K = \mathbb{Q}(\ell^n)$, all this is summarized by the following diagram where $G_m := \mathrm{Gal}(L(p^m)/\mathbb{Q}) \simeq \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/\phi(q)\mathbb{Z}$, ϕ being the Euler function:



3.2. **Multipliers of Stickelberger elements.** For $K = \mathbb{Q}(\ell^n)$, put for short $L_m := L(p^m) = K\mathbb{Q}(p^m)$; the conductor of L_m is $f_{L_m} = \ell^{n+1} \cdot qp^m$ for $\ell \neq 2$ and $2^{n+2} \cdot p^{m+1}$ for $\ell = 2$. To simplify, put $f_n^m := f_{L_m}$. Let c be an integer, prime to f_n^m, and 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 $a'_c \cdot c = a + \lambda_a^m(c) f_n^m$, $\lambda_a^m(c) \in \mathbb{Z}$; then, using the bijection $a \mapsto a'_c$ in the summation of the second term in [ ] and the fact that $\left(\frac{L_m}{a'_c}\right)\left(\frac{L_m}{c}\right) = \left(\frac{L_m}{a}\right)$, this yields:

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

Lemma 3.2. *We have the relations* $\lambda^m_{f_n^m - a}(c) + \frac{1-c}{2} = -\big(\lambda_a^m(c) + \frac{1-c}{2}\big)$ *for all* $a \in [1, f_n^m]$ *prime to* f_n^m. *Then:*

$$\mathscr{S}'^c_{L_m} := \sum_{a=1}^{f_n^m/2} \Big[\lambda_a^m(c) + \frac{1-c}{2}\Big]\left(\frac{L_m}{a}\right)^{-1} \in \mathbb{Z}[G_m] \tag{1}$$

is such that $\mathscr{S}_{L_m}^c = \mathscr{S}'^c_{L_m} \cdot (1 - s_\infty)$.

Proof. By definition, the integer $(f_n^m - a)'_c$ is in $[1, f_n^m]$ and congruent modulo f_n^m to $(f_n^m - a)\, c^{-1} \equiv -ac^{-1} \equiv -a'_c \pmod{f_n^m}$; thus $(f_n^m - a)'_c = f_n^m - a'_c$ and

$$\lambda^m_{f_n^m - a}(c) = \frac{(f_n^m - a)'_c\, c - (f_n^m - a)}{f_n^m} = \frac{(f_n^m - a'_c)\, c - (f_n^m - a)}{f_n^m} = c - 1 - \lambda_a^m(c),$$

whence $\lambda^m_{f_n^m - a}(c) + \frac{1-c}{2} = -\big(\lambda_a^m(c) + \frac{1-c}{2}\big)$ and the result. □

3.3. **Spiegel involution.** Let $\kappa_m : G_m \to (\mathbb{Z}/qp^m\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\mu_{qp^m})/\mathbb{Q})$ be the *cyclotomic character of level* m, of kernel $\mathrm{Gal}(L_m/\mathbb{Q}(\mu_{qp^m}))$, defined by:

$$\zeta^s = \zeta^{\kappa_m(s)}, \text{ for all } s \in G_m \text{ and all } \zeta \in \mu_{qp^m}.$$

The Spiegel involution is the involution of $(\mathbb{Z}/qp^m\mathbb{Z})[G_m]$ defined by:

$$x := \sum_{s\in G_m} a_s \cdot s \;\longmapsto\; x^* := \sum_{s\in G_m} a_s \cdot \kappa_m(s) \cdot s^{-1}.$$

Thus, if s is the Artin symbol $\left(\frac{L_m}{a}\right)$, then $\left(\frac{L_m}{a}\right)^* \equiv a \cdot \left(\frac{L_m}{a}\right)^{-1} \pmod{qp^m}$.
We shall use the case $m = 0$ for which we have the congruence $\kappa_m(s) \equiv \omega(s) \pmod q$, where ω is the usual Teichmüller character $\omega : G_0 = \mathrm{Gal}(L/\mathbb{Q}) \to \mathbb{Z}_p^\times$.
Thus, from Lemma 3.2, we have obtained $\mathscr{S}^{c\,*}_{L_m} = \mathscr{S}^{\prime c\,*}_{L_m} \cdot (1+s_\infty)$ in $(\mathbb{Z}/qp^m\mathbb{Z})[G_m]$.

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

Recall that $K_m := K(p^m)$ and $L_m := L(p^m) = LK(p^m)$. 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 $L_m^\times$ defining the maximal sub-extension of $H^{\mathrm{pr}}_{K_m}$ whose Galois group is of exponent p^m, then to use the mirror 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 formula 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 $K = \mathbb{Q}(\ell^n)$. For all $m \geq e$, the $(\mathbb{Z}/qp^m\mathbb{Z})[G_m]$-module $\mathscr{T}_K$ is annihilated by $\mathscr{S}^{\prime c\,*}_{L_m}$.*

From the expression (1) of $\mathscr{S}^{\prime c}_{L_m}$, the image by the Spiegel involution yields:

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

defining a coherent family $(\mathscr{S}^{\prime c\,*}_{L_m})_m \in \varprojlim_{m\geq e} (\mathbb{Z}/qp^m\mathbb{Z})[G_m]$ of annihilators of $\mathscr{T}_K$.

One obtains, by restriction of $\mathscr{S}^{\prime c\,*}_{L_m}$ to K, a coherent family of annihilators of $\mathscr{T}_K$, in $\varprojlim_{m\geq e} (\mathbb{Z}/qp^m\mathbb{Z})[\mathrm{Gal}(K/\mathbb{Q})]$, whose p-adic limit:

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

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

Remark 4.2. *Let* $\alpha^*_{L_m} := \left[\sum_{a=1}^{f_n^m} \left(\frac{L_m}{a}\right)^{-1}\right]^* \equiv \sum_{a=1}^{f_n^m} a^{-1}\left(\frac{L_m}{a}\right) \pmod{qp^m}$*; then:*

$$\alpha^*_{L_m} := \sum_{a=1}^{f_n^m/2} a^{-1}\left(\frac{L_m}{a}\right) + (f_n^m - a)^{-1}\left(\frac{L_m}{f_n^m - a}\right) \equiv \sum_{a=1}^{f_n^m/2} a^{-1}\left(\frac{L_m}{a}\right)(1 - s_\infty) \pmod{f_n^m},$$

which annihilates $\mathscr{T}_K$ and is such that, by restriction to K, $\alpha^*_{L_m} \mapsto 0 \pmod{qp^m}$ since K is real. We shall neglect in $\mathscr{A}^c_K$ the term $\frac{1-c}{2}\cdot\alpha^*_{L_m}$ and we still denote:

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

Lemma 4.3. *For $K=\mathbb{Q}(\ell^n)$, ψ_n of order ℓ^n and conductor ℓ^{n+1} (or 2^{n+2}),*

$$\psi_n(\mathscr{A}^c_K) = (1-\psi_n(c))\cdot\tfrac{1}{2}L_p(1,\psi_n).$$

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

Proposition 4.4. *Let $K:=\mathbb{Q}(\ell^n)$ of Galois group $G\simeq\mathbb{Z}/\ell^n\mathbb{Z}$ and conductor ℓ^{n+1} (or 2^{n+2}), $n\geq 1$. Then, for the p-adic character θ_n above a character ψ_n, of order ℓ^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.*

Since in the practice, taking $c=2$ in the programs, 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 ℓ^n, $(1-\psi_n(2))$ is in general invertible modulo p, except for $\psi_1(2)=1$ and $\ell=1093$, $3511,\ldots$ In these cases, one must choose another c. If $p=2$ an odd c must be chosen.

Lemma 4.5. *We have $\mathscr{A}^c_K \equiv \sum_{a=1}^{f_n^0/2}\lambda_a^0(c)\,a^{-1}\Big(\frac{K}{a}\Big) \pmod p$ [22, Corollary 7.3 (iii)], where $f_n^0=\ell^{n+1}\cdot q$ for $\ell\neq 2$ and $2^{n+2}\cdot p$ for $\ell=2$.*

Thus, we have obtained, putting $f_n^0=:f_n$, a computable characterization of non-triviality of $\mathscr{T}_K$:

Theorem 4.6. *For $p\geq 2$, $\ell\neq p$, $n\geq 1$ fixed, let $K=\mathbb{Q}(\ell^n)$, $L=K(\mu_q)$, $q=p$ or 4. The conductor of L is $f_n:=\ell^{n+1}q$ for $\ell\neq 2$ (resp. $2^{n+2}p$ for $\ell=2$). 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 $\mathscr{A}^c_K := \sum_{a=1}^{f_n/2}\lambda_a(c)\,a^{-1}\Big(\frac{K}{a}\Big)$; let ψ_n be a character of K of order ℓ^n and let θ_n be the p-adic character above ψ_n. If $\psi_n(\mathscr{A}^c_K)$ is not a p-adic unit, then 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 OF #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=3,2000,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)/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=Mod(S,Q);vp=valuation(norm(s),p);
if(vp>0,print("el=",el," n=",n," p=",p)))))}
```

```
el=3   n=1  p=7          el=5    n=2  p=1151       el=47   n=1  p=283
el=3   n=1  p=73         el=5    n=2  p=2251       el=67   n=1  p=269
el=3   n=3  p=109        el=5    n=3  p=2251       el=83   n=1  p=499
el=3   n=4  p=487        el=17   n=1  p=239        el=101  n=1  p=607
el=3   n=4  p=1621       el=23   n=1  p=47         el=107  n=1  p=857
el=5   n=1  p=11         el=29   n=1  p=59         el=109  n=1  p=50359
el=5   n=2  p=101        el=43   n=1  p=173
```

We find 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 $\mathbb{Z}/2251\mathbb{Z} \times \mathbb{Z}/2251\mathbb{Z}$.

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 an huge computer memory; we get as expected:

```
el=3   n=3   p=109    rk(T)=1     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 $\mathsf{z} \equiv \mathsf{r} \pmod{\mathfrak{p}_\mathsf{n}}$, where z denotes in the program a generator of μ_{ℓ^n} and r a rational integer, then avoiding the previous computation of $\mathsf{N} = \mathsf{norm}(\mathsf{s})$ in Programs III-IV which takes too much time. We then find supplementary examples, taking $n = 1$ for $\ell > 11$:

```
PROGRAM IV. TEST OF #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))))))}
```

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

```
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)))))}
```

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, the character ψ_1 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 $\mathbb{Q}(\mu_\ell)$ but in the inert case, one finds $\psi_1(\mathscr{A}_K^c) \in 2 \cdot \mathbb{Z}[\mu_\ell]$.

```
PROGRAM V. TEST OF #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 writes:

```
el=11  n=1  p=2       el=1093  n=1  p=2       el=3511  n=1  p=2
```

For the case of $\ell = 1093$, 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 OF #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))))}
```

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

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., $\ell^n = 2^{10}$, $p = 114689$):

```
PROGRAM VII. TEST OF #T*>1 MODULO (zeta-r) WHEN p=1 (mod el^n) FOR el=2, p>3
el=2 n=3 p=3         el=2 n=5 p=3617         el=2 n=5 p=4513
el=2 n=8 p=18433     el=2 n=10 p=114689

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=1,2):
{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*10^4,f=p*el^(n+2);cm=Mod(C,f)^-1;Qp=Mod(1,p)*Q;
F=factor(Q+O(p));R=lift(component(F,1));d=matsize(F)[1];
g=znprimroot(p);G=lift(g);gm=g^-1;
e=lift(Mod((1-H)*el^(-n-2),p));H=H+e*el^(n+2);h=Mod(H,f);
e=lift(Mod((1-G)*p^-1,el^(n+2)));G=G+e*p;g=Mod(G,f);
S=0;hh=1;gg=1;ggm=1;for(u=1,el^n,hh=hh*h;
T=0;for(v=1,p-1,gg=gg*g;ggm=ggm*gm;a=lift(hh*gg);A=lift(a*cm);
T=T+(A*C-a)/f*ggm);S=S+lift(T)*x^u);s=lift(Mod(S,Qp));
for(k=1,d,t=Mod(s,R[k]);if(t==0,print("el=",el," n=",n," p=",p)))))}
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 $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P}, 1)$), 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 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 $\mathrm{rank}(M) = \ell^n - 1$:

```
PROGRAM VIII. TEST ON THE REGULATOR R FOR el>2, n=1
{el=17;p=239;dr=el;if(Mod(p^(el-1),el^2)==1,dr=1);P=polsubcyclo(el^2,el);
Pp=P*Mod(1,p^2);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*e^p);le=lift(e-nu);LogE=0;
for(i=0,el-1,c=lift(polcoeff(le,i))/p;LogE=LogE+c*x^i);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=el^n;P=x;for(j=1,n,P=P^2-2);
Pp=P*Mod(1,p^2);K=bnfinit(P,1);E=K.fu;L=List;for(k=1,2^n-1,e0=E[k];
e=Mod(lift(e0),Pp);for(u=1,dr,e=e^p);le=lift(e*e0^-1-1);LogE=0;
for(i=0,el^n-1,c=lift(polcoeff(le,i))/p;LogE=LogE+c*x^i);listinsert(L,LogE,1));
M=matrix(el^n-1,el^n,i,j,Mod(polcoeff(L[i],j),p));R=matrank(M);
print("el^n=",el^n," p=",p," rk(M)=",R);if(R<el^n-1,print("R_K non-trivial"))}
el^n=2 p=13 rk(M)=0  R_K non-trivial    el^n=4 p=29  rk(M)=2  R_K non-trivial
el^n=2 p=31 rk(M)=0  R_K non-trivial    el^n=4 p=37  rk(M)=2  R_K non-trivial
el^n=4 p=13 rk(M)=1  R_K non-trivial    el^n=8 p=521 rk(M)=6  R_K non-trivial
```

In each case, one verifies that $\mathsf{K.no} = 1$ (trivial class group).

4.5. **Conjecture about the p-torsion groups $\mathscr{T}$.** The annihilation Theorem 4.6 allows us to test the non-triviality of $\mathscr{T}_K$, for the fields $K := \mathbb{Q}(\ell^n)$, 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 and conductor ℓ^{n+1} (or 2^{n+2}).

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 $\mathscr{T}^*_{\mathbb{Q}(\ell^n)}$ 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, in general, the solutions p are 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, $\ell = 2$ being not specific. But one may easily conjecture that the counterexamples (if any) are of zero density.

5. Reflection theorem

The reflection theorem can be used to compare directly the p-class group $\mathscr{C}_K$ of $K = \mathbb{Q}(\ell^n)$ 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).

Denote by $\mathrm{rk}_p(A)$ the $\mathbb{F}_p$-dimension of A/A^p for an abelian group A of finite type.

5.1. **Case $p = 2$ for class groups and 2-torsion groups.** Consider, once for all, the case $p = 2$ with $\ell > 2$. The reflection theorem works in K, with the trivial character; applied with the set $S_{K,2}$ 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 $K=\mathbb{Q}(\ell^n)$, for any $\ell>2$, $n\geq 1$ and $p=2$:*

$$\mathrm{rk}_2(\mathscr{T}_K^{\mathrm{ord}})=\mathrm{rk}_2\big[\mathscr{C}_K^{\mathrm{res}}/\mathscr{cl}_K^{\mathrm{res}}(S_{K,2})\big]+\#S_{K,2}-1, \tag{2}$$

$$\mathrm{rk}_2(\mathscr{T}_K^{\mathrm{ord}})=\mathrm{rk}_2\big[\mathscr{C}_K^{\mathrm{ord}}/\mathscr{cl}_K^{\mathrm{ord}}(S_{K,2})\big]+\#S_{K,2}-1, \tag{3}$$

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

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

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

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

Remarks 5.2. *Let $K=\mathbb{Q}(\ell^n)$, for any $\ell>2$ and $n\geq 1$.*

(*i*) *If $p=2$ is inert in K, $\mathrm{rk}_2(\mathscr{T}_K^{\mathrm{ord}})=\mathrm{rk}_2(\mathscr{C}_K^{\mathrm{res}})=\mathrm{rk}_2(\mathscr{C}_K^{\mathrm{ord}})$ (from (2), (3)). This does not apply for $\ell=1093$, 3511 and (unknown) primes ℓ such that the Fermat quotient of 2 modulo ℓ is non-trivial. For $\ell=1093$ and from:*

$$\mathrm{rk}_2(\mathscr{T}_K^{\mathrm{ord}})=\mathrm{rk}_2(\mathscr{C}_K^{\mathrm{res}}/\mathscr{cl}_K^{\mathrm{res}}(S_{K,2}))+1092=\mathrm{rk}_2(\mathscr{C}_K^{\mathrm{ord}}/\mathscr{cl}_K^{\mathrm{ord}}(S_{K,2}))+1092,$$

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 $\mathscr{T}_K^{\mathrm{ord}}$, whence that $\mathscr{C}_K^{S_{K,2}\ \mathrm{res}}=\mathscr{C}_K^{S_{K,2}\,\mathrm{ord}}=1$ and that $\mathscr{T}_K^{\mathrm{ord}}\simeq(\mathbb{Z}/2\mathbb{Z})^{1092}$. 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 $\mathscr{T}_K^{\mathrm{res}}\simeq\mathscr{T}_K^{\mathrm{ord}}\bigoplus\mathbb{F}_2^{\ell^n}$* [15, Theorem III.4.1.5]*, valid under Leopoldt's conjecture for $p=2$.*

5.2. **Case $p\neq 2$ for class groups and p-torsion groups.** The application of the reflection theorem needs to consider $L=K\mathbb{Q}(\mu_p)$ for $K=\mathbb{Q}(\ell^n)$ with the group $\mathrm{Gal}(L/K)$.

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

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

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

Theorem 5.3. *Let $p>2$ be a prime distinct from ℓ. Consider, for $n\geq 1$, the layer $K:=\mathbb{Q}(\ell^n)$ and put $L:=K(\mu_p)$. We have the following equalities:*

$$\mathrm{rk}_p(\mathscr{T}_K)=\mathrm{rk}_\omega(\mathscr{C}_L) \tag{6}$$

$$\mathrm{rk}_p\big[\mathscr{C}_K/\mathscr{cl}_K(S_{K,p})\big]=\mathrm{rk}_\omega(\mathscr{T}_L)+1-\#S_{K,p} \tag{7}$$

$$\mathrm{rk}_p(\mathscr{C}_K)=\mathrm{rk}_\omega(\mathscr{C}_L^{\mathfrak{P}^*})+1-\ell^n \tag{8}$$

$$\mathrm{rk}_p\big[\mathrm{N}_{L/K}(\mathscr{C}_L^{\mathfrak{P}^*})\big]=\mathrm{rk}_\omega(\mathscr{C}_L)+1 \tag{9}$$

where $\mathfrak{P}^* = \big(\prod_{\mathfrak{P}\vert p}\mathfrak{P}\big)^p = (p)\cdot(1-\zeta_p)$ *in* L, *and* $\mathscr{C}\!\ell_L^{\mathfrak{P}^*}$ *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 (7) of the theorem and computes:

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

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 $\mathrm{rk}_3(\mathscr{C}\!\ell_K) = \mathrm{rk}_{\omega}(\mathscr{T}_L)$. Of course, the program does not consider the cases where $\mathscr{T}_L = 1$ ($\mathsf{LL} = \mathsf{List}([\,])$); but we have no counterexamples ($\mathsf{Delta} = \mathsf{0}$ 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 $\mathsf{bnfinit}(\mathsf{Q},\mathsf{1})$ 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** (8) **of Theorem 5.3.** We can compute, for $p \neq 2$, the structure of the whole group:

$$\mathscr{C}\!\ell_L^{\mathfrak{P}^*} = \bigoplus_{i=1}^{p-1} \mathscr{C}\!\ell_L^{\mathfrak{P}^*,\omega^i}.$$

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 (8) for ω. This suggests that these ω^{2i+1}-ranks may be nontrivial for any i 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]

PROGRAM XII. ILLUSTRATION OF FORMULA (8) FOR el>2
{el=3;for(n=1,2,print("el=",el," n=",n);P=polsubcyclo(el^(n+1),el^n);
forprime(p=5,19,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=3  n=1
p=5  rk(Hp)=6  #zp=7  Hp=[5,5,5,5,5,5]
p=7  rk(Hp)=10 #zp=10 Hp=[49,7,7,7,7,7,7,7,7,7]
p=11 rk(Hp)=15 #zp=16 Hp=[11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11]
p=13 rk(Hp)=18 #zp=19 Hp=[13,13,13,13,13,13,13,13,13,13,13,13,13,13,13,13,13,
                                                          13,13,13]
p=17 rk(Hp)=24 #zp=25 Hp=[17,17,17,17,17,17,17,17,17,17,17,17,17,
                                      17,17,17,17,17,17,17,17,17,17,17,17]
p=19 rk(Hp)=27 #zp=28 Hp=[19,19,19,19,19,19,19,19,19,19,19,19,19,19,19,19,19,
                                      19,19,19,19,19,19,19,19,19,19,19,19]
el=3  n=2
p=5  rk(Hp)=18 #zp=19 Hp=[5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5]
p=7  rk(Hp)=28 #zp=28 Hp=[49,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,
                                                          7,7,7,7,7,7]
el=3  n=1
p=5  rk(Hp)=6  #zp=7  Hp=[5,5,5,5,5,5]
p=7  rk(Hp)=10 #zp=10 Hp=[49,7,7,7,7,7,7,7,7,7]
p=11 rk(Hp)=15 #zp=16 Hp=[11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11]
p=13 rk(Hp)=18 #zp=19 Hp=[13,13,13,13,13,13,13,13,13,13,13,13,13,13,13,13,13,
                                                          13,13,13]
```

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

Proposition 5.4. *For $K=\mathbb{Q}(\ell^n)$, $\ell\geq 2$, $n\geq 1$, and $L=K(\mu_p)$, $p>2$, we have $\mathrm{rk}_p(\mathscr{C}_K)=\mathrm{rk}_p(Y^\omega_{L,\mathrm{prim}})$, where $Y^\omega_{L,\mathrm{prim}}\subseteq Y^\omega_L:=\big(\{\alpha\in L^\times,\ (\alpha)=\mathfrak{A}^p\}\cdot L^{\times p}/L^{\times p}\big)^\omega$ is the ω-component of the subset of Y_L 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 $\mathfrak{A}$. The 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 $\ell^n=3$ 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. Generalizations and open problems

A natural generalization of the previous study is to consider the composite of N fields $\mathbb{Q}(\ell_i^{n_i})$, $n_i\geq 1$, ℓ_i distinct prime numbers, and to fix a prime p (see [47] for analytic results of non-divisibility). Such a composite can be written:

$$\mathbb{Q}(\mathscr{L}^{\mathscr{N}}),\quad \mathscr{L}=\{\ell_1,\dots,\ell_N\},\ \mathscr{N}=\{n_1,\dots,n_N\},\tag{10}$$

with an obvious meaning; 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 $\mathbb{Q}(\ell^\infty)$. 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: the question of the p-class groups of $\mathbb{Q}(\mathscr{L}^{\mathscr{N}})$ when $p\notin\mathscr{L}$ and the opposite case that we shall write as composite $\mathbb{Q}(\mathscr{L}^{\mathscr{N}})\cdot\mathbb{Q}(p^m)$, $m\geq 1$.

In the first case, we are in the strict generalization of classical conjectures related to Weber's problem and we may think that the result is analogous.

In the second one the problem is in some sense related to Greenberg's conjecture [29] for which one very strongly admits that, for n fixed, $\#\mathscr{C}_{\mathbb{Q}(\ell^n)\mathbb{Q}(p^m)}$ is constant for all $m\gg 0$ (i.e., the invariants λ,μ of $\mathbb{Q}(\ell^n)$ for the prime p are zero); see for instance [9, 28, 40] for some developments.

6.1. **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 $\mathbb{Q}(\mathscr{L}^{\mathscr{N}})$. 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 $D_2 = \mathbb{Q}(1093)\,\mathbb{Q}(3511)$. Of course, if p varies for ℓ fixed, the integers g_p are unbounded (e.g., $p = 1 + \lambda\,\ell^{1+r}$, with arbitrary $r \gg 0$).

6.2. **The p-torsion group of $\mathbb{Q}(\mathscr{L}^{\mathscr{N}})$.** Since there exist many fields $\mathbb{Q}(\ell^n)$ with non-trivial groups $\mathscr{T}_{\mathbb{Q}(\ell^n)}$, these p-torsion groups remain subgroups of $\mathscr{T}_K$ for the composite $K = \mathbb{Q}(\mathscr{L}^{\mathscr{N}})$ and give larger groups. We give some computations of the structure of $\mathscr{T}_K$ for composite fields $K = \mathbb{Q}(q_1)\mathbb{Q}(q_2)$, for which one gets always $C_K = 1$; then we give the case of the sole computation of $\mathscr{T}_K^*$. The general programs are the following, with suitable polynomials of definition; after each program the reader may verify the result (for not to large degrees), using the basic PROGRAMS I, II, § 2.3.

```
PROGRAM XIII. COMPUTATION OF T IN COMPOSITE FIELDS F - SOME EXAMPLES
{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," rk(T)=",R," T=",L)))}

F=Q(2)Q(7)   C=1
p=13   rk(T)=1  T=[13]                p=113  rk(T)=1  T=[113]
p=31   rk(T)=1  T=[31]

F=Q(2)Q(3)   C=1
p=7    rk(T)=2  T=[7,7]               p=43   rk(T)=1  T=[43]
p=13   rk(T)=2  T=[13,13]             p=73   rk(T)=1  T=[73]
p=31   rk(T)=1  T=[31]

F=Q(2)Q(3)Q(5)   C=1
p=7    rk(T)=2  T=[7,7]               p=31   rk(T)=3  T=[31,31,31]
p=11   rk(T)=2  T=[11,11]             p=43   rk(T)=1  T=[43]
p=13   rk(T)=2  T=[13,13]             p=73   rk(T)=1  T=[73]

F=Q(2)Q(3)Q(7)   C=1
p=7    rk(T)=4  T=[49,49,7,7]         p=13   rk(T)=2  T=[13,13]

F=Q(3)Q(7)   C=1
p=7    rk(T)=2  T=[49,7]

F=Q(2)Q(3)   C=1
p=3    rk(T)=2  T=[9,9]               p=31   rk(T)=1  T=[31]
p=7    rk(T)=2  T=[7,7]               p=37   rk(T)=1  T=[37]
p=13   rk(T)=4  T=[169,169,13,13]     p=43   rk(T)=1  T=[43]
p=29   rk(T)=1  T=[29]                p=73   rk(T)=1  T=[73]

F=Q(3)Q(5)   C=1
p=7    rk(T)=1  T=[7]                 p=31   rk(T)=2  T=[31,31]
p=11   rk(T)=2  T=[11,11]             p=73   rk(T)=1  T=[73]
```

Remark 6.1. *The composite F of $K = \mathbb{Q}(2)\mathbb{Q}(3)$ with $\mathbb{Q}(7)$ for $p = 7$ has some interest since $\mathscr{T}_K \simeq (\mathbb{Z}/7\mathbb{Z})^2$ (from the second example above); so we know that $\mathscr{T}_F^{\mathrm{Gal}(F/K)} \simeq \mathscr{T}_K$, but with $\mathscr{T}_F \simeq (\mathbb{Z}/7\mathbb{Z})^2 \times (\mathbb{Z}/7^2\mathbb{Z})^2$, 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 Subsection.*

Since $\mathrm{N}_{F/K}(\mathscr{T}_F) = \mathscr{T}_K$, we have $\mathscr{T}_F^* \simeq (\mathbb{Z}/7^2\mathbb{Z})^2$. The groups $\mathscr{T}_K$ and $\mathscr{T}_F$, annihilated by $\mathrm{N}_{F/\mathbb{Q}(2)\mathbb{Q}(7)}$, are modules over $\mathbb{Z}[\mu_3]$ in which $p = 7$ is inert; whence the residue degree 2 and the structures obtained.

```
TEST OF #T*>1 FOR ANY NUMBER d OF p-PLACES USING THE FACTORIZATION OF Q mod p
{q1=3;q2=19;h1=znprimroot(q1^2);H1=lift(h1);h2=znprimroot(q2^2);H2=lift(h2);
Q=polcyclo(q1*q2);forprime(p=3,2*10^5,if(p==q1 || p==q2,next);f=p*q1^2*q2^2;
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];
g=znprimroot(p);G=lift(g);gm=g^-1;
e=lift(Mod((1-H1)*q1^-2,p*q2^2));H1=H1+e*q1^2;h1=Mod(H1,f);
e=lift(Mod((1-H2)*q2^-2,p*q1^2));H2=H2+e*q2^2;h2=Mod(H2,f);
e=lift(Mod((1-G)*p^-1,q1^2*q2^2));G=G+e*p;g=Mod(G,f);
S=0;hh1=1;hh2=1;gg=1;ggm=1;
for(u1=1,q1*(q1-1),hh1=hh1*h1;for(u2=1,q2*(q2-1),hh2=hh2*h2;
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*q2+u2*q1,q1*q2));
S=S+lift(t)*x^e));s=lift(Mod(S,Qp));
for(k=1,d,t=Mod(s,R[k]);if(t==0,print("q1=",q1," q2=",q2," p=",p))))}

{q1=3;q2=5;p=1291;P1=polsubcyclo(q1^2,q1);P2=polsubcyclo(q2^2,q2);
P=polcompositum(P1,P2)[1];K=bnfinit(P,1);KpN=bnrinit(K,p^2);
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("h=",K.no," q1=",q1," q2=",q2," p=",p," rk(T)=",R," T=",L))}
q1=3  q2=5   p=31    h=1  rk(T*)=2   T*=[31,31]
q1=3  q2=5   p=241   h=1  rk(T*)=1   T*=[241]
q1=3  q2=5   p=1291  h=1  rk(T*)=1   T*=[1291]
q1=3  q2=11  p=397   h=1  rk(T*)=1   T*=[241]
q1=3  q2=11  p=397   h=1  rk(T*)=1   T*=[397]
q1=3  q2=13  p=157
q1=7  q2=17  p=953
{q1=2;q2=3;h1=Mod(5,8);H1=lift(h1);h2=znprimroot(q2^2);H2=lift(h2);
Q=polcyclo(q1*q2);forprime(p=7,2*10^5,if(p==q1 || p==q2,next);f=p*q1^3*q2^2;
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];
g=znprimroot(p);G=lift(g);gm=g^-1;
e=lift(Mod((1-H1)*q1^-3,p*q2^2));H1=H1+e*q1^3;h1=Mod(H1,f);
e=lift(Mod((1-H2)*q2^-2,p*q1^3));H2=H2+e*q2^2;h2=Mod(H2,f);
e=lift(Mod((1-G)*p^-1,q1^3*q2^2));G=G+e*p;g=Mod(G,f);
S=0;hh1=1;hh2=1;gg=1;ggm=1;
for(u1=1,q1,hh1=hh1*h1;for(u2=1,q2*(q2-1),hh2=hh2*h2;
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*q2+u2*q1,q1*q2));
S=S+lift(t)*x^e));s=lift(Mod(S,Qp));
for(k=1,d,t=Mod(s,R[k]);if(t==0,print("q1=",q1," q2=",q2," p=",p))))}

{q1=2;q2=11;p=2729;P1=x^2-2;P2=polsubcyclo(q2^2,q2);
P=polcompositum(P1,P2)[1];K=bnfinit(P,1);
KpN=bnrinit(K,p^3);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("h=",K.no," q1=",q1," q2=",q2," p=",p," rk(T)=",R," T=",L))}
```

```
q1=2  q2=3   p=7    h=1  rk(T*)=2  T*=[7, 7]          q1=2  q2=11  p=397
q1=2  q2=3   p=13   h=1  rk(T*)=2  T*=[13,13]        q1=2  q2=11  p=2729
q1=2  q2=3   p=43   h=1  rk(T*)=1  T*=[43]           q1=2  q2=11  p=5479
q1=2  q2=7   p=113  h=1  rk(T*)=1  T*=[113]          q1=2  q2=19  p=2357
```

6.3. **The p-class group of $\mathbb{Q}(\mathscr{L}^{\mathscr{N}})\,\mathbb{Q}(p^m)$.** In this part, the set $\mathscr{L}$ can contain p (subject to having m large enough); but, in practice, we shall only consider the case $p \notin \mathscr{L}$ and $m = 1$.

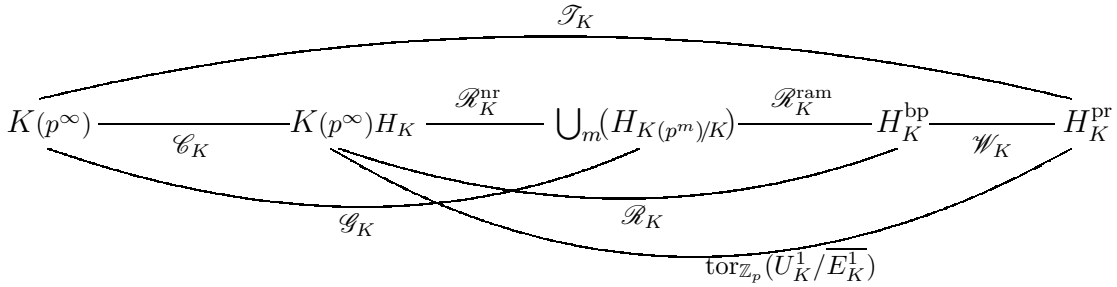
6.3.1. *Use of genus theory.* The analog of Weber's problem in $\widehat{\mathbb{Q}}$ is very doubtful in that case because of the Chevalley formula (or genus theory in the cyclic case) in the extension F/K with $K := \mathbb{Q}(\mathscr{L}^{\mathscr{N}})$ fixed in $\widehat{\mathbb{Q}}$ and $F := K\mathbb{Q}(p^m)$, in which p is totally ramified ($m \geq m_0 + 1$ if $K \cap \mathbb{Q}(p^\infty) = \mathbb{Q}(p^{m_0})$):

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

where t_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 $t_p > 1$ the right factor of the formula may be a power of p.

Consider the general diagram [28, Diagram 3] in which $\mathscr{G}_K$ is the union of the genus fields $H_{K(p^m)/K}$ (maximal abelian p-extensions of K, unramified over $K(p^m)$):



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

Theorem 6.2. *Let $K = \mathbb{Q}(\mathscr{L}^{\mathscr{N}})$ fixed in $\widehat{\mathbb{Q}}$ with $p \notin \mathscr{L}$ and let $F := K\mathbb{Q}(p^m)$. Then the factor $\dfrac{p^{m\,(t_p-1)}}{(E_K^{\rm pos} : E_K^{\rm pos} \cap {\rm N}_{F/K}(F^\times))}$ divides $\#\mathscr{R}_K^{\rm nr}$. If p totally split in K, then for all m large enough there is equality (*[28, Theorem 1]*).*

Corollary 6.3. *If $p \neq \ell$ totally splits in $K = \mathbb{Q}(\ell^n)$ (i.e., $p^{\ell-1} \equiv 1 \pmod{\ell^{n+1}}$ or $\pm p \equiv 1 \pmod{2^{n+2}}$), 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 6.4.

(*i*) *When p totally splits in K, the subgroup $\mathscr{R}_K^{\rm ram}$ is generated by the inertia groups $U^1_{K_\mathfrak{p}}/\overline{E_K^1} \cap U^1_{K_\mathfrak{p}}$, $\mathfrak{p} \mid p$; 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 $\mathscr{C}_K^{\rm res} = 1$, the condition $\mathscr{C}_F^{\rm res} \neq 1$ is equivalent to $\dfrac{p^{m\,(t_p-1)}}{(E_K^{\rm pos} : E_K^{\rm pos} \cap {\rm N}_{F/K}(F^\times))} \neq 1$; 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* $p \equiv 1 \pmod{\ell^n}$, *which may give smallest p-ranks, but* $p \not\equiv 1 \pmod{\ell^{n+1}}$ *(or* $\pmod{2^{n+2}}$*), 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 where* $(\ell^n, p) = (2^8, 18433), (2^{10}, 114689), (3, 73), (3^4, 487), (5^2, 2251)$.

Any composite gives huge conductors limiting computations of class numbers. We have done the following ones (in the restricted sense when 2 intervenes):

```
PROGRAM XIV. COMPUTATION OF C 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
```

(*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 $\dfrac{7}{(E_K : E_K \cap \mathrm{N}_{F/K}(F^\times))} = 1$. 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 $\mathbb{Q}(2)\mathbb{Q}(3)$ and $\#\mathscr{T}_{\mathbb{Q}(3)} = 7$.

(*iv*) $K = \mathbb{Q}(11)$, $F = \mathbb{Q}(11)\mathbb{Q}(3)$, $p = 3$ splits in K, $\dfrac{3^{10}}{(E_K : E_K \cap \mathrm{N}_{F/K}(F^\times))} = 1$. 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 in $K/\mathbb{Q}$, $\dfrac{7^4}{(E_K : E_K \cap \mathrm{N}_{F/K}(F^\times))} = 1$; 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 the use of $\mathsf{F} = \mathsf{bnfinit}(\mathsf{Q}, 1)$ limiting degrees and conductors. But in fact the literature does contain few counterexamples (see Coates [8, Section 3], from Fukuda–Komatsu, Horie [32, 33], also using genus theory). We shall examine these cases by computing Hasse's normic symbols in F/K in the Chevalley formula.

6.3.2. *Numerical counterexamples.* 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 $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P}, 1)$ instead of $\mathsf{F} = \mathsf{bnfinit}(\mathsf{Q}, 1)$ to get the units of K. The Remark 6.4 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, for each $\mathfrak{p} \mid p$, 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 the result ($(E_K : E_K \cap \mathrm{N}_{F/K}(F^\times)) = p^{\ell-1}$ 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 (6.3.2) 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 $\mathsf{bnfinit}(\mathsf{P}, 1)$, unfeasible for $\ell > 17$; thus we can compute the $\mathbb{F}_p$-rank of the matrix M for larger primes p.

```
PROGRAM XV. 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," rankM=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," rankM=0")))}

el=2  p=31 rankM=0            el=2  p=1546463  rankM=0

PROGRAM XVI. 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," rankM=",r)))}

el=3   p=73    rankM=1
```

We note that for these three 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 as expected.

In the case $\ell = 5$, $n = 2$, $p = 2251$ of total splitting, some partial computations in E_K/E_K^{2251} (of order 2251^{24}) indicate, as expected from the previous matrix rank computation, that the $(\varepsilon_i)^{2250}$ are of the form $1 + 2251 \cdot \alpha_i$, 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 $1 \le i \le 24$, generate $\mathscr{T}_K = \mathscr{R}_K$ of order p.

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

```
PROGRAM XVII. 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 XVIII. RANK OF THE MATRIX OF NORMIC SYMBOLS FOR POWERS OF el=2
(computations with cyclotomic units)
{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
```

For $n > 3$, the case $p = 31$ no longer appears since $31 \equiv -1 \pmod{2^5 = 2^{3+2}}$.

We have performed such computations (for $\ell = 2, 3, 5, 7, 11$ up to $p \leq 10^9$, $\ell = 13, 17, 19, 23$, up to $p \leq 2 \cdot 10^5$, 41 up to $p \leq 7211$, and some other in smaller intervals, for instance for some powers of 2, when p splits in K) without finding new solutions. This enforces [8, Conjecture D] in $\widehat{\mathbb{Q}}$. 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 suggesting solutions in finite number with the particularity of giving very few solutions, including sometimes a huge one !

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

Theorem 6.5. *Let $K = \mathbb{Q}(\mathscr{L}^{\mathscr{N}}) \subset \widehat{\mathbb{Q}}$, $\mathscr{L} = \{\ell_1, \ldots, \ell_N\}$, $\mathscr{N} = \{n_1, \ldots, n_N\}$ and let $K_m := K\mathbb{Q}(p^m)$ be a layer in the cyclotomic $\mathbb{Z}_p$-extension of K ($\ell, p \geq 2$, $p \neq \ell$; under the Leopoldt and Gross–Kuz'min conjectures for p). Since the extension is unramified, in the logarithmic sense, we have $\widetilde{\mathscr{C}}_{K_m}^{\mathrm{Gal}(K_m/K)} \simeq \widetilde{\mathscr{C}}_K$. Whence $\widetilde{\mathscr{C}}_{K_m} = 1$, for all m, if and only if $\widetilde{\mathscr{C}}_K = 1$.*

This gives many cases of triviality; moreover, we know that $\widetilde{\mathscr{C}}_K = 1$ implies that Greenberg's conjecture holds true in $K(p^\infty)$ 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:

```
{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 $K_1 = \mathbb{Q}(2)\,\mathbb{Q}(31)$ and $K_1 = \mathbb{Q}(3)\,\mathbb{Q}(73)$, the ordinary class groups $\mathscr{C}_{K_1}$ are non-trivial for $p = 31$ and 73, respectively, it follows that the $\widetilde{\mathscr{C}}_{K_1}$ are trivial for all the tested primes p, including $31, 73$.

6.4. **Conclusion and questions.** The use of genus theory has succeeded to give few non-trivial class groups in *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 $\widehat{\mathbb{Q}}$; for fixed p, we shall consider the composite $\widehat{\mathbb{Q}}^*$ of the $\mathbb{Z}_\ell$-extensions for $\ell \neq p$ and study $\widehat{\mathbb{Q}}/\widehat{\mathbb{Q}}^* = \widehat{\mathbb{Q}}^*\mathbb{Q}(p^\infty)/\widehat{\mathbb{Q}}^*$:

(*i*) Let p fixed; is the decomposition group of p in $\widehat{\mathbb{Q}}/\mathbb{Q}$ of finite index in $\mathrm{Gal}(\widehat{\mathbb{Q}}/\mathbb{Q})$? We have conjectured this property in (loc. cit.). Of course, this seems linked to the order of magnitude of p since, taking a prime $p = 1 + \lambda\, q_1^{a_1} \cdots q_s^{a_s}$, with primes q_i, $a_i > 1$, this gives unbounded indices; but for $p = 2$, only two primes ℓ are known such that 2 splits in $\mathbb{Q}(\ell)$.

(*ii*) Let $K \subset \widehat{\mathbb{Q}}^*$ of finite degree and let $F := K\,\mathbb{Q}(p^m)$, $m \geq 1$; is the set of primes p such that $(E_K^{\rm pos} : E_K^{\rm pos} \cap \mathrm{N}_{F/K}(F^\times)) < p^{m\,(t_p - 1)}$ finite in number, where t_p is the number of p-places of K ?

If so, this gives new heuristic/conjecture about the behavior of the units in $\widehat{\mathbb{Q}}$ and is related to Greenberg's conjecture [29] for the subfields $K \subset \widehat{\mathbb{Q}}^*$.

(*iii*) In the context of (ii), we have obtained in previous sections that in the following cases, where $\mathscr{T}_K$ is non-trivial with a trivial p-class group (see Subsections 4.1 4.3:

$$\begin{aligned} &\ell = 3, \quad n = 4, \quad p = 487 \qquad \equiv 1 \pmod{3^5},\\ &\ell = 2, \quad n = 8, \quad p = 18433 \quad \equiv 1 \pmod{2^{11}},\\ &\ell = 2, \quad n = 10, \quad p = 114689 \quad \equiv 1 \pmod{2^{14}}, \end{aligned}$$

p splits totally in $K := \mathbb{Q}(\ell^n)$ and the p-class group of $K_1 := \mathbb{Q}(\ell^n)\mathbb{Q}(p)$ is divisible by $\dfrac{p^{\ell^n - 1}}{(E_K : E_K \cap \mathrm{N}_{K/K_1}(K_1^\times))}$, only depending of the p-adic properties of E_K (or of the group of cyclotomic units), but our PARI/GP programs do not succeed in proving if p divides or not $\#C_{K_1}$.

What is for instance the order of the logarithmic class group $\widetilde{\mathscr{C}}_K$ for the above three fields of too large degrees ?

(*iv*) Let $K \subset \widehat{\mathbb{Q}}$ of finite degree and consider $K\mathbb{Q}(p^m)$; what are the Iwasawa invariants of $\varprojlim_m \mathscr{T}_{K\mathbb{Q}(p^m)}$?

(v) In [54], Silverman proves, after some other contributions (Cusick, Pohst, Remak), an inequality between R_K (regulator) and D_K (discriminant) of the form (in the context $K = \mathbb{Q}(\ell^n)$): $R_K > c_K(\log(\gamma_K|D_K|))^{\ell^{n-1}(\ell-1)}$. 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 $\#\mathscr{R}_K$, by means of $\mathscr{T}_K$ equal to $\mathscr{R}_K$ for all p large enough, and justified by extensive computations:

Conjecture 6.6. *Let $\mathscr{K}$ be the set of number fields; for $K \in \mathscr{K}$, let D_K be its discriminant and $\mathscr{R}_K := \mathrm{tor}_{\mathbb{Z}_p}(\log(U_K^1)/\log(\overline{E_K^1}))$ be its normalized p-adic regulator (see § 2.1). There exists a constant $C_p > 0$ such that:*

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

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**, (1965-1966), no. 2, 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), Tome **20** (1978–1979), no. 2 , 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. http://www.sciencedirect.com/science/article/pii/0022314X86900776
[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
[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) 2018/2019 (2019). https://arxiv.org/abs/1709.06388 https://pmb.centre-mersenne.org/article/PMB_2019__2_29_0.pdf
[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
English translation: Local θ-regulators of an algebraic number: p-adic Conjectures (2017). https://arxiv.org/pdf/1701.02618
[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. https://arxiv.org/pdf/1612.00718.pdf 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/ User's Guide to PARI/GP, version 2.11.1. https://pari.math.u-bordeaux.fr/pub/pari/manuals/2.11.1/users.pdf

[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