



**HAL**  
open science

# ON THE $p$ -CLASS GROUP STABILITY ALONG CYCLIC $p$ -TOWERS OF A NUMBER FIELD

Georges Gras

► **To cite this version:**

Georges Gras. ON THE  $p$ -CLASS GROUP STABILITY ALONG CYCLIC  $p$ -TOWERS OF A NUMBER FIELD. 2021. hal-03155190v4

**HAL Id: hal-03155190**

**<https://hal.science/hal-03155190v4>**

Preprint submitted on 19 May 2021 (v4), last revised 12 Aug 2021 (v5)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# ON THE $p$ -CLASS GROUP STABILITY ALONG CYCLIC $p$ -TOWERS OF A NUMBER FIELD

GEORGES GRAS

ABSTRACT. Let  $k$  be a number field,  $p \geq 2$  a prime and  $S$  any set of finite places of  $k$ . We call  $K/k$  a totally  $S$ -ramified cyclic  $p$ -tower if  $\text{Gal}(K/k) \simeq \mathbb{Z}/p^N\mathbb{Z}$  and if  $S \neq \emptyset$  is totally ramified. Using analogues of Chevalley's formula (Gras, Proc. Math. Sci. **127**(1) (2017)), we give an elementary proof of a stability theorem (Theorem 3.1) for generalized  $p$ -class groups  $\mathcal{X}_n$  of the layers  $k_n \subseteq K$ : let  $\lambda = \max(0, \#S - 1 - \rho)$  given in Definition 1.1; then  $\#\mathcal{X}_n = \#\mathcal{X}_0 \cdot p^{\lambda \cdot n}$  for all  $n \in [0, N]$ , if and only if  $\#\mathcal{X}_1 = \#\mathcal{X}_0 \cdot p^\lambda$ . This improves the case  $\lambda = 0$  of Fukuda (1994), Li–Ouyang–Xu–Zhang (2020), Mizusawa–Yamamoto (2020), whose techniques are based on Iwasawa's theory or Galois theory of pro- $p$ -groups. We deduce capitulation properties of  $\mathcal{X}_0$  in the tower. Finally we apply our principles to the torsion groups  $\mathcal{T}_n$  of abelian  $p$ -ramification theory. Numerical examples are given.

## CONTENTS

1. Introduction	1
2. Around Chevalley's ambiguous class number formula	4
3. Introduction of Hasse's norm symbols – Main theorem	5
4. Numerical examples	7
4.1. Cyclic $p$ -towers over $k = \mathbb{Q}(\sqrt{\pm m})$	7
4.2. Cyclic $p$ -towers over $\mathbb{Q}$ with modulus	9
4.3. Cyclic $p$ -towers over a cyclic cubic field $k$	9
5. Other examples of applications	10
6. Behavior in $p$ -cyclic towers of other invariants	11
6.1. Case of the cyclotomic $\mathbb{Z}_p$ -extensions $\tilde{k}/k$ of $k$ real	13
6.2. Case of real cyclic $p$ -towers with tame ramification	13
References	14

## 1. INTRODUCTION

The behavior of  $p$ -class groups in a  $\mathbb{Z}_p$ -extension gives rise to many theoretical and computational results; a main observation is the unpredictability of these groups in the first layers of the  $\mathbb{Z}_p$ -extension, then their regularization from some ineffective level, Iwasawa's theory giving the famous formula of the orders by means

---

*Date:* May 19, 2021.

*2020 Mathematics Subject Classification.* Primary 11R23; 11R29; 11R37.

*Key words and phrases.*  $p$ -class groups, class field theory, Chevalley's formula, cyclic  $p$ -extensions.

of the invariants  $\lambda, \mu, \nu$ ; nevertheless, this algebraic context is not sufficient to estimate these parameters (e.g., Greenberg's conjecture [10]). Our purpose is to see, more generally, what is the behavior of the  $p$ -class groups (and some other arithmetic invariants) in cyclic  $p$ -extensions in which one allows tame ramification.

Let  $k$  be a number field,  $p \geq 2$  a prime number and  $K$  a cyclic extension of degree  $p^N$  of  $k$ ,  $N \geq 2$ , and let  $k_n$ ,  $n \in [0, N]$ , be the degree  $p^n$  extension of  $k$  in  $K$ . We speak of cyclic  $p$ -towers  $K/k$  and put  $G = \text{Gal}(K/k)$ . Let  $S$  be the set of places of  $k$ , ramified in  $K/k$ . We will assume  $S \neq \emptyset$  and  $S$  totally ramified in  $K/k$ ; in general,  $S$  contains tame places, except if  $K$  is contained in a  $\mathbb{Z}_p$ -extension of  $k$ , in which case  $S = S_p$ , a set of  $p$ -places of  $k$ . Due to the very nature of a tower, there will never be "complexification=ramification" of infinite real places (i.e.,  $S_\infty = \emptyset$ ).

Let  $\mathfrak{m} \neq 0$  be an integer ideal of  $k$ , of support  $T$  disjoint from  $S$ ; let  $\mathcal{C}_{k, \mathfrak{m}}$  and  $\mathcal{C}_{k_n, \mathfrak{m}}$ , denoted simply  $\mathcal{C}_{0, \mathfrak{m}}$  and  $\mathcal{C}_{n, \mathfrak{m}}$ , be the  $p$ -Sylow subgroups of the ray class groups modulo  $\mathfrak{m}$ , of  $k$  and  $k_n$ , respectively (for  $n > 0$ ,  $\mathfrak{m}$  is seen as extended ideal in  $k_n$ ). The class of an ideal  $\mathfrak{a}$  of  $k_n$  is denoted  $\mathcal{C}_{n, \mathfrak{m}}(\mathfrak{a})$ .

Let  $N_{K/k_n}$  be the arithmetic norm in  $K/k_n$ , defined on class groups from norms of ideals. Since  $\mathfrak{m}$  is prime to  $S \neq \emptyset$  totally ramified, the corresponding  $p$ -Hilbert's ray class fields  $H_{n, \mathfrak{m}}$ , of the  $k_n$ 's are linearly disjoint from the relative  $p$ -towers  $K/k_n$ ; since, by class field theory,  $N_{K/k_n}$  corresponds to the restriction of automorphisms  $\text{Gal}(H_{N, \mathfrak{m}}/K) \rightarrow \text{Gal}(H_{n, \mathfrak{m}}/k_n)$ , we get  $N_{K/k_n}(\mathcal{C}_{N, \mathfrak{m}}) = \mathcal{C}_{n, \mathfrak{m}}$ , for all  $n \in [0, N]$ .

Let  $\mathcal{H}_N$  be a sub- $\mathbb{Z}[G]$ -module of  $\mathcal{C}_{N, \mathfrak{m}}$ ; we represent a minimal set of  $\mathbb{Z}[G]$ -generators of  $\mathcal{H}_N$  with prime ideals  $\mathfrak{Q}_1, \dots, \mathfrak{Q}_t \notin S \cup T$ . Let  $\mathcal{I}_N$  be the  $\mathbb{Z}[G]$ -module generated by these ideals; thus  $N_{K/k}(\mathcal{I}_N)$  is of minimal  $\mathbb{Z}$ -rank  $t$  since  $N_{K/k}(\mathcal{I}_N) \otimes \mathbb{Q} = \langle \mathfrak{q}_1, \dots, \mathfrak{q}_t \rangle \otimes \mathbb{Q}$ . We set, for all  $n \in [0, N]$ :

$$(1.1) \quad \mathcal{I}_n := N_{K/k_n}(\mathcal{I}_N), \quad \mathcal{H}_n := N_{K/k_n}(\mathcal{H}_N), \quad \mathcal{X}_{n, \mathfrak{m}} := \mathcal{C}_{n, \mathfrak{m}}/\mathcal{H}_n.$$

This defines the family  $\{\mathcal{X}_{n, \mathfrak{m}}\}_{n \in [0, N]}$  ("generalized  $p$ -class groups") such that:

$$N_{K/k_n}(\mathcal{X}_{N, \mathfrak{m}}) = \mathcal{X}_{n, \mathfrak{m}}, \text{ for all } n \in [0, N].$$

Any place  $\mathfrak{Q}$  of  $K$ , such that  $\mathcal{C}_{N, \mathfrak{m}}(\mathfrak{Q}) \in \mathcal{H}_N$ , totally splits in the subfield of  $H_{N, \mathfrak{m}}$  fixed by the image of  $\mathcal{H}_N$  in  $\text{Gal}(H_{N, \mathfrak{m}}/K)$ ; so this general definition allows to enforce decomposition conditions in the ray class fields.

To simplify, we shall remove the indices  $\mathfrak{m}$ , except necessity.

One speaks of " $\lambda$ -stability" of these  $\mathcal{X}_n$  along the cyclic  $p$ -tower  $K/k$  when there exists  $\lambda \geq 0$  such that  $\#\mathcal{X}_n = \#\mathcal{X}_0 \cdot p^{\lambda \cdot n}$ , for all  $n \in [0, N]$ . Of course, this is not a workable definition, both theoretically (classical context of  $\mathbb{Z}_p$ -extensions or less familiar case of  $p$ -towers with tame ramification) and computationally (inability to use PARI/GP [25] beyond some level  $n = 3$  or  $4$ , and almost nothing for  $p > 5$ ). So we intend to get an accessible criterion likely to give information in all the tower.

**Definition 1.1.** Let  $\Lambda := \{x \in k^\times, x \equiv 1 \pmod{\mathfrak{m}}, (x) \in N_{K/k}(\mathcal{I}_N)\}$ . For instance,  $\mathcal{I}_N = 1$  yields  $\{\mathcal{X}_n\} = \{\mathcal{C}_n\}$  and  $\Lambda = E$ , the group of units  $\varepsilon \equiv 1 \pmod{\mathfrak{m}}$  of  $k$ . We have the exact sequence  $1 \rightarrow \Lambda/E \rightarrow \mathcal{I}_0 \rightarrow \mathcal{H}_0 \rightarrow 1$ . Since  $\Lambda/E$  is free (of  $\mathbb{Z}$ -rank  $t$  because  $\mathcal{H}_0$  is finite), one can write, with representatives  $\alpha_j$  of  $\Lambda/E$ :

$$\Lambda = \text{tor}_{\mathbb{Z}}(E) \oplus \langle \varepsilon_1, \dots, \varepsilon_r; \alpha_1, \dots, \alpha_t \rangle_{\mathbb{Z}} =: \text{tor}_{\mathbb{Z}}(E) \oplus X, \quad \varepsilon_i \in E,$$

$r := r_1 + r_2 - 1$ , where  $(r_1, r_2)$  is the signature of  $k$  and where  $X$  is  $\mathbb{Z}$ -free of  $\mathbb{Z}$ -rank  $\rho := r + t$ ; we define the parameter  $\lambda := \max(0, \#S - 1 - \rho)$ .

We shall see that the norm properties, in  $K/k$ , of  $\text{tor}_{\mathbb{Z}}(E) \otimes \mathbb{Z}_p$  are specific and may give some obstructions that are elucidated by the following Lemma.

**Lemma 1.2.** *(Albert's Theorem for  $K/k$ ; for a proof, see [6, Exercise I.6.2.3]). If  $k$  contains the group  $\mu_{p^e}$  of  $p^e$ th roots of unity, then  $\mu_{p^e} \subset N_{K/k}(K^\times)$  if and only if there exists a degree  $p^e$  cyclic extension  $L/K$  such that  $L/k$  is cyclic.*

**Remark 1.3.** *We shall restrict ourselves to the case  $\text{tor}_{\mathbb{Z}}(E) \otimes \mathbb{Z}_p \subset N_{K/k}(K^\times)$ . If necessary, it suffices to restrict the tower  $K/k$  to the sub-tower  $K'/k$  such that  $[K : K'] = \#\mu_p(k)$  ( $\mu_p(k)$  being the group of  $p$ th roots of unity of  $k$ ) or to notice that  $L/K/k$  does exist (recall that no arithmetic condition is required on  $L/K$ ).*

Thus, the norm properties of  $\Lambda$  are assigned to  $X$ .

We put to simplify  $\mathcal{C}_0 =: \mathcal{C}$ ,  $\mathcal{H}_0 =: \mathcal{H}$ ,  $\mathcal{I}_0 =: \mathcal{I}$ ,  $\mathcal{X}_0 =: \mathcal{X}$ , and so on in the sequel,  $\mathfrak{m}$  being implied. Under the assumptions on  $S$ ,  $\mathfrak{m}$ , we will prove the following result (see Theorem 3.1 and Corollary 3.2 for more complete statements):

**Main Result.** *Assume that  $\text{tor}_{\mathbb{Z}}(E) \subset N_{K/k}(K^\times)$  (Remark 1.3). Let  $\rho \geq 0$  be the  $\mathbb{Z}$ -rank of the  $\mathbb{Z}$ -module  $X$  and let  $\lambda := \max(0, \#S - 1 - \rho)$  (Definition 1.1). Then  $\#\mathcal{X}_n = \#\mathcal{X} \cdot p^{\lambda n}$  for all  $n \in [0, N]$ , if and only if  $\#\mathcal{X}_1 = \#\mathcal{X} \cdot p^\lambda$ . If the criterion applies with  $\lambda = 0$  (i.e.,  $\#\mathcal{X}_1 = \#\mathcal{X}$ ) and if  $p^N \geq \#\mathcal{X}$ , then  $\mathcal{X}$  capitulates in  $K$ .*

**Remark 1.4.** (a) *If  $\lambda = \max(0, \#S - 1 - \rho)$  fulfills the criterion of  $\lambda$ -stability from the base field  $k$ , it fulfills the same  $\lambda$ -stability criterion in any relative  $p$ -tower  $K/k'$ ,  $k' := k_{n_0}$ ,  $n_0 \in [0, N]$ , since (with  $\mathcal{X}'_n := \mathcal{X}_{n_0+n}$ ,  $n \geq 0$ ) we get  $\#\mathcal{X}'_n = \#\mathcal{X}' \cdot p^{\lambda n}$  since  $\#\mathcal{X}'_n = \#\mathcal{X}_{n_0+n} = \#\mathcal{X} \cdot p^{\lambda(n_0+n)} = (\#\mathcal{X} \cdot p^{\lambda n_0}) \cdot p^{\lambda n} = \#\mathcal{X}' \cdot p^{\lambda n}$ .*

(b) *If  $\lambda = \max(0, \#S - 1 - \rho)$  is not suitable for the criterion in  $k_1/k$  (which shall be equivalent to  $\#\mathcal{X}_1 > \#\mathcal{X} \cdot p^\lambda$  due to Chevalley's formula), we can consider a relative tower  $K/k'$ ; then  $\#S' = \#S$  and  $\lambda' := \max(0, \#S - 1 - \rho')$  is a strictly decreasing function of  $[k' : k]$  (indeed, from Definition 1.1, we compute that  $\rho' - \rho = r' - r = (r_1 + r_2) \cdot ([k' : k] - 1)$ ), so that two cases may arise:*

(i) *For some  $k' \subset K$ , we have  $\#\mathcal{X}'_1 = \#\mathcal{X}' \cdot p^{\lambda'}$  giving the  $\lambda'$ -stability in  $K/k'$  with regular linear increasing orders from  $k'$ .*

(ii) *Whatever  $k' \subset K$ ,  $\lambda'$  is not suitable (i.e.,  $\#\mathcal{X}'_1 > \#\mathcal{X}' \cdot p^{\lambda'}$ ), which means that  $\#\mathcal{X}'_n$  is strictly increasing from some level  $n_0$ , which is illustrated by many numerical examples and suggests non-linear increasing (in a  $\mathbb{Z}_p$ -extension this means " $\mu \neq 0$ "). It is important to note that a  $\tilde{\lambda}$ -stability may exist from some level, with  $\tilde{\lambda} > \lambda'$ ; this is the case in a  $\mathbb{Z}_p$ -extension with non-zero Iwasawa's invariants  $\tilde{\lambda}$ ,  $\tilde{\mu}$ , the parameter  $\lambda'$  being 0 in some  $k'$  high enough in the tower.*

Numerical experiments are out of reach as soon as  $n > 3$  or 4, but a reasonable heuristic is a tendency to stabilization in totally real  $p$ -towers, by analogy with the study of Greenberg's conjecture carried out in [9]. In a different framework, let  $k_n$  be the  $n$ th layer of the cyclotomic  $\mathbb{Z}_p$ -extension  $\tilde{k}$  of  $k$  and let  $C_n$  be the whole class group of  $k_n$ ; then, for  $\ell \neq p$ ,  $\#(C_n \otimes \mathbb{Z}_\ell)$  stabilizes in  $\tilde{k}$  (a deep result in the abelian case [28], extended in [3] to Iwasawa context in the  $\mathbb{Z}_p \times \mathbb{Z}_\ell$ -extension of  $k$ ).

(c) *For  $k$  fixed,  $\lambda$  is unbounded (which only depends on the tower via  $S$ ) and the condition  $\#\mathcal{C}_1 = \#\mathcal{C}$  of the literature ( $\lambda = 0$ , thus  $\#S \leq r_1 + r_2$ ) is empty as soon as  $\lambda \geq 1$ , whence the interest of the factor  $p^\lambda$  to get examples whatever  $S$ . For known results (all relative to  $\lambda = 0$ ), one may cite Fukuda [4] using Iwasawa's theory, Li-Ouyang-Xu-Zhang [20, §3] working in a non-abelian Galois context, in*

*Kummer towers, via the use of the fixed points formulas [5, 7], then Mizusawa [22] above  $\mathbb{Z}_2$ -extensions, and Mizusawa–Yamamoto [23] for generalizations, including ramification and splitting conditions, via the Galois theory of pro- $p$ -groups.*

To conclude, we will show that the behavior, in  $K/k$ , of the finite torsion groups  $\mathcal{T}_n$  of  $p$ -ramification theory (as “dual” invariants of  $p$ -class groups) gives much strongly increasing groups with possibly non-zero  $\tilde{\mu}$ -invariant in  $\mathbb{Z}_p$ -extensions.

## 2. AROUND CHEVALLEY’S AMBIGUOUS CLASS NUMBER FORMULA

The well-known Chevalley’s formula [1, p. 402] is the pivotal element for a great lot of “fixed points formulas”. For the ordinary sense, it takes into account the complexification of real infinite places, which does not occur for us as explained in the Introduction. Let  $L/F$  be a cyclic  $p$ -extension of Galois group  $G$ ,  $S$ -ramified, non-complexified at infinity if  $p = 2$ , and let  $e_v(L/F)$  be the ramification index of  $v \in S$ ; we have  $\#\mathcal{C}_L^G = \frac{\#\mathcal{C}_F \cdot \prod_{v \in S} e_v(L/F)}{[L:F] \cdot (E_F : E_F \cap N_{L/F}(L^\times))}$ , where  $\mathcal{C}_F, \mathcal{C}_L$  denote the  $p$ -class groups of  $F, L$ , respectively, and  $E_F$  the group of global units of  $F$ .

Various generalizations of this formula were given (Gras [5, Théorème 2.7, Corollaire 2.8], [7, Theorem 3.6, Corollaries 3.7, 3.9], Jaulent [13, Chap. II, § 3]); mention their recent idelic proof by Li–Yu [21, Theorem 2.1 & § 2.3, Examples]. We shall use the following one for the layers of a  $p$ -cyclic tower  $K/k$ :

**Proposition 2.1.** *Assume  $S \neq \emptyset$  totally ramified in  $L/F$ . Let  $\mathfrak{m}$  of support  $T$  be a prime-to- $S$  modulus of  $F$  and let  $\mathcal{C}_F, \mathcal{C}_L$ , be the  $p$ -Sylow subgroups of the ray class groups modulo  $\mathfrak{m}$ , of  $F$  and  $L$ , respectively. For any  $\mathbb{Z}[G]$ -module  $\mathcal{I}_L$ , of prime-to- $T \cup S$  ideals of  $L$ , defining  $\mathcal{H}_L := \mathcal{d}_L(\mathcal{I}_L)$ ,  $\mathcal{H}_F := N_{L/F}(\mathcal{H}_L) := \mathcal{d}_F(N_{L/F}(\mathcal{I}_L))$ , we have with  $\Lambda_{L/F} := \{x \in F^\times, x \equiv 1 \pmod{\mathfrak{m}}, (x) \in N_{L/F}(\mathcal{I}_L)\}$ :*

$$(2.1) \quad \#(\mathcal{C}_L/\mathcal{H}_L)^G = \#(\mathcal{C}_F/\mathcal{H}_F) \times \frac{(\#G)^{\#S-1}}{(\Lambda_{L/F} : \Lambda_{L/F} \cap N_{L/F}(L^\times))}.$$

**Lemma 2.2.** *Let  $K/k$  be a cyclic  $p$ -tower of degree  $p^N$ , of Galois group  $G =: \langle \sigma \rangle$ . Let  $\mathcal{H}_N =: \mathcal{d}_N(\mathcal{I}_N) \subseteq \mathcal{C}_N$  and  $\Lambda := \{x \in k^\times, x \equiv 1 \pmod{\mathfrak{m}}, (x) \in N_{K/k}(\mathcal{I}_N)\}$  (see Definition 1.1):*

- (i)  $\Lambda = \{x \in k^\times, x \equiv 1 \pmod{\mathfrak{m}}, (x) \in N_{k_n/k}(\mathcal{I}_n)\}$  (i.e.,  $\Lambda_{K/k} = \Lambda_{k_n/k}$ ),
- (ii)  $\Lambda \subseteq \Lambda_1 := \{x_1 \in k_1^\times, x_1 \equiv 1 \pmod{\mathfrak{m}}, (x_1) \in N_{K/k_1}(\mathcal{I}_N)\}$ .

*Proof.* Point (i) comes from  $\mathcal{I}_n = N_{K/k_n}(\mathcal{I}_N)$ . Let  $x \in \Lambda$  seen in  $k_1$ ; then  $(x) = N_{K/k}(\mathfrak{A}) = N_{K/k_1}(\mathfrak{A}^\Theta)$ , where  $\Theta = 1 + \sigma + \dots + \sigma^{p-1}$ , and  $\mathfrak{A}^\Theta \in \mathcal{I}_N$  since  $\mathcal{I}_N$  is a  $\mathbb{Z}[G]$ -module, whence (ii). Notice that  $(x) \in N_{K/k}(\mathcal{I}_N)$  expresses that  $x$  is local norm in  $K/k$  at every  $v \notin S$ ; if moreover  $x$  is local norm at  $S$  it is a global one (Hasse norm theorem).  $\square$

In what follows, throughout the article, only the invariant  $\rho = \text{rk}_{\mathbb{Z}}(X)$  is needed (Definition 1.1 giving  $\lambda := \max(0, \#S - 1 - \rho)$ ) and never  $\mathcal{I}_N, \Lambda, \dots$ . However,  $\rho = r + t$  may be unknown because of the minimal number  $t$  of generators of the  $\mathbb{Z}[G]$ -module  $\mathcal{I}_N$  if it is too general; but, in practice,  $\rho$  is known (e.g.,  $\rho = r_1 + r_2 - 1$  for ray class groups modulo  $\mathfrak{m}$ ).

**Lemma 2.3.** *Let  $X = \langle x_1, \dots, x_\rho \rangle_{\mathbb{Z}}$  be a free  $\mathbb{Z}$ -module of  $\mathbb{Z}$ -rank  $\rho \geq 0$ , let  $\Omega := (\mathbb{Z}/p^n\mathbb{Z})^\delta$ ,  $n \geq 1$ ,  $\delta \geq 0$ , and let  $f : X \rightarrow \Omega$  be an homomorphism such that*

the image of  $X \rightarrow \Omega/\Omega^p$  is of  $\mathbb{F}_p$ -dimension  $\min(\rho, \delta)$ . Then  $\#f(X) = p^{\min(\rho, \delta) \cdot n}$  and for all  $m \in [0, n]$ ,  $\#f^{p^m}(X) = p^{\min(\rho, \delta) \cdot (n-m)}$  (where  $f^{p^m}(x) := f(x)^{p^m}$ ).

*Proof.* From  $f : X \rightarrow \Omega$ , let  $\bar{f} : X/X^p \rightarrow \Omega/\Omega^p$ ; by assumption,  $\dim_{\mathbb{F}_p}(\text{Im}(\bar{f})) = \min(\rho, \delta)$ . Let  $M = \langle e_1, \dots, e_\delta \rangle_{\mathbb{Z}_p}$  be a free  $\mathbb{Z}_p$ -module of  $\mathbb{Z}_p$ -rank  $\delta$ , and replace  $\Omega$  by  $M/M^{p^n}$ . Let  $q : X \rightarrow X/X^p$ ,  $\pi_n : M \rightarrow M/M^{p^n}$ ,  $\pi : M/M^{p^n} \rightarrow M/M^p$ , and  $\pi_1 = \pi \circ \pi_n : M \rightarrow M/M^p$ , be the canonical maps. Then, let  $F : X \rightarrow M$  be any map such that  $\pi_n \circ F = f$ . We have, since  $n \geq 1$ , the commutative diagram:

$$\begin{array}{ccc} X \simeq \mathbb{Z}^\rho & \xrightarrow{F} & M \simeq \mathbb{Z}_p^\delta \\ & \searrow f & \downarrow \pi_n \\ & & \Omega \simeq M/M^{p^n} \\ & & \downarrow \pi \\ X/X^p & \xrightarrow{\bar{f}} & \Omega/\Omega^p \simeq M/M^p \end{array} \quad \left. \begin{array}{c} \downarrow q \\ \downarrow \pi_1 \end{array} \right\} \pi_1$$

(i) Case  $\rho \geq \delta$  (surjectivity of  $\bar{f}$ ). Let  $y \in M$ ; there exists  $x \in X$  such that  $\pi_1(y) = \bar{f}(q(x)) = \pi_1(F(x))$ , whence  $y = F(x) \cdot y^p$ ,  $y^p \in M$ ; so, by a finite induction,  $M = F(X) \cdot M^{p^n}$  and  $\pi_n(M) = \Omega = f(X)$  is of order  $p^{\delta \cdot n}$ .

(ii) Case  $\rho < \delta$  (injectivity of  $\bar{f}$ ). Let  $y \in M$  such that  $y^p = F(x)$ ,  $x \in X$ ; then  $1 = \pi_1(y^p) = \pi_1(F(x)) = \bar{f}(q(x))$ , whence  $q(x) = 1$  and  $x = x^p$ ,  $x^p \in X$ , giving  $y^p = F(x^p)$  in  $M$  thus  $y = F(x^p)$ , proving that  $F(X)$  is direct factor in  $M$ ; thus  $f(X) = \pi_n(F(X))$  is a direct factor, in  $\Omega$ , isomorphic to  $(\mathbb{Z}/p^n\mathbb{Z})^\rho$ .

Since  $f^{p^m}(X) = f(X)^{p^m}$ , this gives  $f(X)^{p^m} = \Omega^{p^m} \simeq ((\mathbb{Z}/p^n\mathbb{Z})^\delta)^{p^m}$  in case (i) and  $((\mathbb{Z}/p^n\mathbb{Z})^\rho)^{p^m}$  in case (ii). Whence the orders.  $\square$

### 3. INTRODUCTION OF HASSE'S NORM SYMBOLS – MAIN THEOREM

Let  $K/k$  be a cyclic  $p$ -tower of degree  $p^N$ ,  $N \geq 2$ . Let  $\omega_{k_n/k}$  be the map which associates with  $x \in \Lambda$  the family of Hasse's norm symbols  $(\frac{x, k_n/k}{v}) \in I_v(k_n/k)$  (inertia groups of  $v \in S$ ), where  $\Lambda := \{x \in k^\times, x \equiv 1 \pmod{\mathfrak{m}}, (x) \in N_{K/k}(\mathcal{J}_N)\}$ . Since  $x$  is local norm at the places  $v \notin S$ , the image of  $\omega_{k_n/k}$  is contained in  $\Omega_{k_n/k} := \{(\tau_v)_{v \in S} \in \bigoplus_{v \in S} I_v(k_n/k), \prod_{v \in S} \tau_v = 1\}$  (from the product formula); then  $\text{Ker}(\omega_{k_n/k}) = \Lambda \cap N_{k_n/k}(k_n^\times)$ .

Assume  $S \neq \emptyset$  totally ramified; so, fixing any  $v_0 \in S$ ,  $\Omega_{k_n/k} \simeq \bigoplus_{v \neq v_0} G_n$ , with  $G_n := \text{Gal}(k_n/k)$ . We consider formulas (2.1) in  $k_n/k$ , using Lemma 2.2 (i):

$$(3.1) \quad \#\mathcal{X}_n^{G_n} = \#\mathcal{X} \cdot \frac{p^{n(\#S-1)}}{(\Lambda : \Lambda \cap N_{k_n/k}(k_n^\times))} = \#\mathcal{X} \cdot \frac{p^{n(\#S-1)}}{\#\omega_{k_n/k}(\Lambda)},$$

where  $\mathcal{X}_n := \mathcal{C}_n/\mathcal{H}_n$  for the family  $\{\mathcal{H}_n\}$  (cf. (1.1) with a prime-to- $S$  modulus  $\mathfrak{m}$ ).

**Theorem 3.1.** *Set  $\Lambda =: \text{tor}_{\mathbb{Z}}(E) \oplus X$ , with  $X = \langle x_1, \dots, x_\rho \rangle_{\mathbb{Z}}$  free of  $\mathbb{Z}$ -rank  $\rho$ , and let  $\lambda := \max(0, \#S-1-\rho)$ . Assume that  $\text{tor}_{\mathbb{Z}}(E) \subset N_{K/k}(K^\times)$  (see Lemma 1.2 and Remark 1.3). We then have the following properties of  $\lambda$ -stability:*

(i) *If  $\#\mathcal{X}_1 = \#\mathcal{X} \cdot p^\lambda$ , then,  $\#\mathcal{X}_n = \#\mathcal{X} \cdot p^{\lambda \cdot n}$  and  $\mathcal{X}_n^{G_n} = \mathcal{X}_n$  for all  $n \in [0, N]$ .*

(ii) *If  $\#\mathcal{X}_1 = \#\mathcal{X} \cdot p^\lambda$ , then  $J_{k_n/k}(\mathcal{X}) = \mathcal{X}_n^{p^n}$  and  $\text{Ker}(J_{k_n/k}) = N_{k_n/k}(\mathcal{X}_n[p^n])$ , for all  $n \in [0, N]$ , where the  $J_{k_n/k}$ 's are the transfer maps in  $k_n/k$ . If  $\lambda = 0$ , the norm maps  $N_{k_n/k} : \mathcal{X}_n \rightarrow \mathcal{X}$  are isomorphisms.*

*Proof.* Put  $N_n := N_{k_n/k}$ ,  $J_n := J_{k_n/k}$ ,  $G_n := \langle \sigma_n \rangle$ ,  $\Omega_n := \Omega_{k_n/k}$ ,  $\omega_n := \omega_{k_n/k}$ ,  $s := \#S$ . By assumption,  $\omega_n(\Lambda) = \omega_n(X)$  for all  $n \in [1, N]$ . From (3.1),  $\#\mathcal{X}_1^{G_1} = \#\mathcal{X} \cdot \frac{p^{s-1}}{\#\omega_1(X)} \geq \#\mathcal{X} \cdot p^\lambda$  since  $\#\omega_1(X) \leq p^{\min(\rho, s-1)}$ ; thus, with  $\#\mathcal{X}_1 = \#\mathcal{X} \cdot p^\lambda$ , we obtain  $\mathcal{X}_1^{G_1} = \mathcal{X}_1$ , whence  $\#\mathcal{X}_1^{G_1} = \#\mathcal{X} \cdot p^\lambda$  and  $\#\omega_1(X) = p^{\min(\rho, s-1)}$ .

By restriction of Hasse's symbols,  $\omega_1 = \pi \circ \omega_n$ , with  $\pi : \Omega_n \rightarrow \Omega_n/\Omega_n^p \simeq G_1^{s-1}$ . Since we have proven that  $\dim_{\mathbb{F}_p}(\omega_1(X)) = \min(\rho, s-1)$ , Lemma 2.3 applies to  $X = \langle x_1, \dots, x_\rho \rangle_{\mathbb{Z}}$ ,  $\delta = s-1$ ,  $f = \omega_n$ ; so,  $\#\omega_n(X) = p^{\min(\rho, s-1)n}$  and, from (3.1):

$$(3.2) \quad \#\mathcal{X}_n^{G_n} = \#\mathcal{X} \cdot p^{\lambda \cdot n}, \text{ for all } n \in [0, N].$$

Consider the extension  $k_n/k_1$ , of Galois group  $G_n^p = \langle \sigma_n^p \rangle$ , and the corresponding map  $\omega'_n$  on  $k_1^\times$  with values in  $\Omega_{k_n/k_1} \simeq \Omega_n^p$ ; then  $\#\mathcal{X}_n^{G_n^p} = \#\mathcal{X}_1 \cdot \frac{p^{(n-1)(s-1)}}{\#\omega'_n(\Lambda_1)}$ ,  $\Lambda_1 := \{x \in k_1^\times, x \equiv 1 \pmod{\mathfrak{m}}, (x) \in N_{K/k_1}(\mathcal{J}_N)\}$ . Since  $\Lambda \subseteq \Lambda_1$  (Lemma 2.2 (ii)), the functorial properties of Hasse's symbols on  $X$  imply (where  $v_1 \mid v$  in  $k_1$ ):

$$\omega'_n(x_i) = \left( \left( \frac{x_i, k_n/k_1}{v_1} \right) \right)_v = \left( \left( \frac{N_1(x_i), k_n/k}{v} \right) \right)_v = \left( \left( \frac{x_i^p, k_n/k}{v} \right) \right)_v = \left( \left( \frac{x_i, k_n/k}{v} \right)^p \right)_v,$$

giving  $\omega'_n = \omega_n^p$  on  $X$ . Then,  $\omega'_n(X) \subseteq \omega'_n(\Lambda_1)$  yields:

$$\#\mathcal{X}_n^{G_n^p} = \#\mathcal{X}_1 \cdot \frac{p^{(n-1)(s-1)}}{\#\omega'_n(\Lambda_1)} \leq \#\mathcal{X}_1 \cdot \frac{p^{(n-1)(s-1)}}{\#\omega_n^p(X)} = \#\mathcal{X}_1 \cdot \frac{p^{(n-1)(s-1)}}{\#\omega_n^p(X)};$$

Lemma 2.3, for  $\omega_n^p$ , gives  $\#\omega_n^p(X) = p^{(n-1)\min(\rho, s-1)}$ , then, with  $\#\mathcal{X}_1 = \#\mathcal{X} \cdot p^\lambda$ :

$$\#\mathcal{X}_n^{G_n^p} \leq \#\mathcal{X}_1 \cdot \frac{p^{(n-1)(s-1)}}{p^{(n-1)\min(\rho, s-1)}} = \#\mathcal{X}_1 \cdot p^{\lambda \cdot (n-1)} = \#\mathcal{X} \cdot p^{\lambda \cdot n}.$$

Since  $\mathcal{X}_n^{G_n^p} \supseteq \mathcal{X}_n^{G_n}$  and  $\#\mathcal{X}_n^{G_n} = \#\mathcal{X} \cdot p^{\lambda \cdot n}$  from (3.2), we get  $\mathcal{X}_n^{G_n} = \mathcal{X}_n^{G_n^p}$ , equivalent to  $\mathcal{X}_n^{1-\sigma_n} = \mathcal{X}_n^{1-\sigma_n^p} = \mathcal{X}_n^{(1-\sigma_n) \cdot \theta}$ , where  $\theta = 1 + \sigma_n + \dots + \sigma_n^{p-1} \in (p, 1-\sigma_n)$ , a maximal ideal of  $\mathbb{Z}_p[G_n]$  since  $\mathbb{Z}_p[G_n]/(p, 1-\sigma_n) \simeq \mathbb{F}_p$ ; so  $\mathcal{X}_n^{1-\sigma_n} = 1$ , thus  $\mathcal{X}_n = \mathcal{X}_n^{G_n}$ . Whence (i).

From  $N_n(\mathcal{X}_n) = \mathcal{X}$ ,  $\mathcal{X}_n = \mathcal{X}_n^{G_n}$  and  $J_n \circ N_n = \nu_n$  (the algebraic norm), one obtains  $J_n(\mathcal{X}) = J_n(N_n(\mathcal{X}_n)) = \mathcal{X}_n^{\nu_n} = \mathcal{X}_n^{p^n}$ . Let  $x \in \text{Ker}(J_n)$  and put  $x = N_n(y)$ ,  $y \in \mathcal{X}_n$ ; then  $1 = J_n(x) = J_n(N_n(y)) = y^{p^n}$ , so  $\text{Ker}(J_n) \subseteq N_n(\mathcal{X}_n[p^n])$  and if  $x = N_n(y)$ ,  $y^{p^n} = 1$ , then  $J_n(x) = J_n(N_n(y)) = y^{p^n} = 1$ . Whence (ii).  $\square$

**Corollary 3.2.** *Let  $p^e$  be the order of  $\mathcal{X}$  in  $k$  and let  $K$  be a totally  $S$ -ramified  $p$ -cyclic tower of degree  $p^N$ , with  $N \geq e$ , such that  $\lambda = 0$  (i.e.,  $\#S \leq 1 + \rho$ , namely  $\#S \leq r_1 + r_2$  for class groups). If  $\#\mathcal{X}_1 = p^e$ , then  $\mathcal{X}$  capitulates in  $k_e$ . In particular, this applies in a  $\mathbb{Z}_p$ -extension  $\tilde{k}/k$  with  $\lambda = 0$  and  $S = S_p$  totally ramified.*

*Proof.* Since  $\lambda = 0$ ,  $\mathcal{X}_e \simeq \mathcal{X}$  from the isomorphism induced by  $N_e : \mathcal{X}_e \rightarrow \mathcal{X}$ , whence  $\text{Ker}(J_e) = N_e(\mathcal{X}_e[p^e]) \simeq \mathcal{X}[p^e] = \mathcal{X}$ .  $\square$

Section 4 will give many examples of such capitulations of  $p$ -class groups of real fields  $k$  in  $K \subseteq k(\mu_\ell)$ ; for instance, for  $k = \mathbb{Q}(\sqrt{4409})$ , the capitulation of the 3-class group  $\mathcal{C} \simeq \mathbb{Z}/9\mathbb{Z}$  occurs in  $k_2$  for  $\ell \in \{19, 37, 73, 109, 127, 271, 307, 379, 397, 523, 541, 577, 739, 883, 919, 937, \dots\}$ . The 3-class group  $\mathcal{C} \simeq \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$  of the cyclic cubic field of conductor 5383, defined by  $P = x^3 + x^2 - 1794x + 17744$ , capitulates in  $k_3$  for  $\ell = 109, 163, 919, \dots$ . The 2-class group  $\mathcal{C} \simeq \mathbb{Z}/16\mathbb{Z}$  of

$\mathbb{Q}(\sqrt{2305})$  capitulates in in  $k_4$  for  $\ell = 97, 193, 353, 449, 929, \dots$ . The 5-class group  $\mathcal{C} \simeq \mathbb{Z}/25\mathbb{Z}$  of  $\mathbb{Q}(\sqrt{24859})$  capitulates in in  $k_2$  for  $\ell = 101, 151, 251, 401, \dots$

Totally real fields  $k$  give  $\lambda = 0$  whatever  $S = S_\ell$ , but some non-totally real fields may give  $\lambda = 0$ ; for instance, let  $P = x^6 + x^5 - 5x^4 - 4x^3 + 6x^2 + 2x + 7$  defining  $k$ , of signature  $(0, 3)$ , of Galois group  $S_6$ ; so  $\lambda = \max(0, \#S - 1 - (r_1 + r_2 - 1)) = \max(0, \#S - 3)$ . For  $p = 3$ ,  $\mathcal{C} \simeq \mathbb{Z}/3\mathbb{Z}$  capitulates in  $k_1$  for  $\ell = 37, 61, 67, 73, 97, 103, 109, 127, 181, 193, \dots$ . For all these primes,  $\#S \in \{1, 2, 3\}$ , giving  $\lambda = 0$  as expected. This criterion allows to recover many numerical examples of abelian capitulations given in the literature with intricate methods (Gras (1997), Kurihara (1999), Bosca (2009), Jaulent (2017, 2019); see [15] for more history about these references).

The existence of primes  $\ell \equiv 1 \pmod{2p^e}$  such that  $\#\mathcal{C}_1 = \#\mathcal{C}$ , in the corresponding  $p$ -cyclic tower of a totally real field  $k$ , enforce the capitulation of the  $p$ -class group of  $k$  in  $k(\mu_\ell)/k$ . Since this only depends on norm symbols having obviously uniform distributions, we propose the following conjecture which would be obtained after some efforts with the techniques used in the classical approaches and especially those of [26], [18] and their subsequent articles):

**Conjecture 3.3.** *Let  $k$  be a totally real number field with generalized  $p$ -class group  $\mathcal{X}_{k,m} = \mathcal{C}_{k,m}/\mathcal{H}_k$  (cf. (1.1)), of order  $p^e$ . There are infinitely many primes  $\ell \equiv 1 \pmod{2p^e}$ , prime to  $\mathfrak{m}$  and unramified in  $k$ , such that  $\mathcal{X}_{k,m}$  capitulates in  $k(\mu_\ell)$ .*

**Remark 3.4.** *To simplify, let's consider the family  $\{\mathcal{C}_n\}$  assuming the context of Lemma 1.2 and Remark 1.3; so  $\lambda = \max(0, \#S - 1 - \rho)$  with  $\rho = r_1 + r_2 - 1$ .*

(a) *The condition of  $\lambda$ -stability,  $\#\mathcal{C}_1 = \#\mathcal{C} \cdot p^\lambda$ , implies  $\mathcal{C}_n^{G_n} = \mathcal{C}_n$  for all  $n \geq 1$ , but is not equivalent. Indeed, let  $k = \mathbb{Q}(\sqrt{m})$ ,  $m > 0$ , and let  $K = kL$ , where  $L$  is the subfield of  $\mathbb{Q}(\mu_{17})$  of degree 8, with 17 split in  $k$ ; whence  $\rho = 1$ ,  $\lambda = 0$ . Assume that  $\omega_1(\varepsilon) = 1$  ( $\varepsilon$  norm in  $k_1/k$ ); then, from Chevalley's formula,  $\#\mathcal{C}_1^{G_1} = \#\mathcal{C} \cdot p \neq \#\mathcal{C}$ . For  $m = 26$ ,  $\varepsilon = 3 + \sqrt{26} \equiv 5^2 \pmod{17}$  in the completion  $\mathbb{Q}_{17}$ ; one obtains the structures [2], [2, 2], [4, 2] giving  $\#\mathcal{C} = 2$  and  $\#\mathcal{C}_1 = \#\mathcal{C}_1^{G_1} = 4$ .*

(b) *When  $\#\mathcal{C}_1 = \#\mathcal{C} \cdot p^\lambda$  does not hold (whence  $\#\mathcal{C}_1 > \#\mathcal{C} \cdot p^\lambda$ ), we observe that orders and  $p$ -ranks are unpredictable and possibly unlimited in the tower; indeed, put  $\mathcal{C}_n^i := \{c \in \mathcal{C}_n, c^{(1-\sigma_n)^i} = 1\} =: \mathcal{C}_n(\mathcal{I}_n^i)$ ,  $i \geq 1$ ; we have, from (2.1),  $\#(\mathcal{C}_n^{i+1}/\mathcal{C}_n^i) = \frac{\#\mathcal{C}}{\#\mathcal{N}_n(\mathcal{C}_n^i)} \times \frac{p^n(\#S-1)}{\#\omega_n(\Lambda^i)}$ , where  $\Lambda^i := \{x \in k^\times, (x) \in \mathcal{N}_n(\mathcal{I}_n^i)\}$ ; in general these two factors are non-trivial giving  $\#\mathcal{C}_n^{i+1} > \#\mathcal{C}_n^i$  and the filtration increases.*

(c) *If Lemma 1.2 does not apply, some counterexamples can arise. For instance, let  $k = \mathbb{Q}(\sqrt{-55})$ ,  $p = 2$ ,  $K = k(\mu_{17})$  of degree  $2^4$  over  $k$  ( $-1 \notin \mathcal{N}_{K/k}(K^\times)$ ,  $\#S = 2$ ,  $\lambda = 1$ ); the successive 2-structures are [4], [8], [16], [32], [32], for which  $\#\mathcal{C}_n = \#\mathcal{C} \cdot 2^n$  holds for  $n \in [0, 3]$ , since  $-1$  is norm in  $k_3/k$ , but not for  $n = 4$ .*

#### 4. NUMERICAL EXAMPLES

**4.1. Cyclic  $p$ -towers over  $k = \mathbb{Q}(\sqrt{\pm m})$ .** Consider, for  $\ell \equiv 1 \pmod{p^N}$  (in ell), the cyclic  $p$ -tower contained in  $k(\mu_\ell)/k$ , for  $k = \mathbb{Q}(\sqrt{s m})$ ,  $m > 0$  square free (in m),  $s = \pm 1$ . The following PARI/GP program computes  $\mathcal{C}_{k_n, m} =: \mathcal{C}_n$  for any prime-to- $\ell$  modulus  $\mathfrak{m}$  (in mod). The polynomial  $P_n$  (in Pn) defines the layer  $k_n$ . The computations up to 3 or 4 (in N) are only for verification when a  $\lambda$ -stability



exists; otherwise some examples do not  $\lambda$ -stabilize in the interval considered and no conclusion is possible (the execution time becomes unaffordable for large degrees). If  $s = -1$  (resp.  $s = 1$ ),  $\lambda = \#S - 1 - \rho \in \{0, 1\}$  (resp.  $\lambda = 0$ ) in  $k$  but decreases in the tower (Remark 1.4). Then  $v_n$  denotes the  $p$ -valuation of the order of  $\mathcal{C}_n$  whose structure  $C_{kn}$  is given by the list L.

```
{p=2;ell=257;mod=5;s=-1;N=3;bm=2;Bm=10^3;for(m=bm,Bm,if(core(m)!=m,next);
P=x^2-s*m;lambda=0;if(s=-1 & kronecker(-m,ell)==1,lambda=1);\\lambda
print();print("p=",p," mod=",mod," ell=",ell," m=",s*m," lambda=",lambda);
for(n=0,N,Pn=polcompositum(polsubcyclo(ell,p^n),P)[1];kn=bnfinit(Pn,1);\\layer kn
knmod=bnrinit(kn,mod);v=valuation(knmod.no,p);Ckn=knmod.cyc;\\ray class field (mod)
C=List;e=matsize(Ckn)[2];for(k=1,e,c=Ckn[e-k+1];\\ray class groups Cn
w=valuation(c,p);if(w>0,listinsert(C,p^w,1));print("v",n,"=",v," ",C))}
IMAGINARY QUARATIC FIELDS, p=2, ell=257, mod=1:
m=-2,lambda=1      m=-11,lambda=1      m=-14,lambda=0      m=-17,lambda=1      m=-15,lambda=1
v0=0 []            v0=0 []            v0=2 [4]            v0=2 [4]            v0=1 [2]
v1=3 [8]           v1=2 [4]           v1=4 [4,4]          v1=5 [8,2,2]        v1=2 [4]
v2=7 [16,4,2]      v2=7 [8,8,2]       v2=8 [4,4,4,4]      v2=10[16,2,2,2,2,2,2] v2=3 [8]
v3=13 [32,8,2,2]   v3=10 [16,16,4]    v3=16 [8,8,8,4,4,2,2,2] v3=19[32,2,2,2,2,2,2,2] v3=4 [16]
                2,2,2,2]                4,2,2,2]          2,2,2,2,2,2,2,2,2]
m=-782,lambda=1      m=-858,lambda=0
v0=3 [4,2]           v0=4 [4,2,2]
v1=8 [4,4,4,2,2]     v1=12 [128,2,2,2,2,2]
v2=22[32,32,4,4,4,2,2,2,2,2,2] v2=22 [256,16,8,2,2,2,2,2,2,2]
v3=35[64,64,8,8,8,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2] v3=32 [512,32,16,4,4,4,2,2,2,2,2,2,2,2,2,2]
m=-15,mod=5,lambda=1 m=-35,mod=5,lambda=1 m=-253,mod=5,lambda=1
v0=2 [4]             v0=2 [4]           v0=4 [4,2,2]
v1=3 [4,2]           v1=3 [4,2]         v1=12 [64,4,2,2,2,2]
v2=4 [8,2]           v2=4 [8,2]         v2=22 [128,8,4,4,2,2,2,2,2,2,2,2]
v3=34 [256,16,8,4,4,4,4,4,4,2,2,2,2,2,2,2,2,2,2,2,2]
IMAGINARY QUARATIC FIELDS, p=3, ell=163, mod=1:
m=-2,lambda=1      m=-293,lambda=1      m=-983,lambda=1      m=-3671,lambda=0
v0=0 []            v0=2 [9]            v0=3 [27]            v0=4 [81]
v1=1 [3]           v1=3 [27]           v1=4 [81]            v1=7 [243,3,3]
v2=2 [9]           v2=4 [81]           v2=5 [243]           v2=11 [729,9,9,3]
REAL QUARATIC FIELDS, p=2, lambda=0:
mod=7,ell=12289:
m=2                m=19                m=89                m=15                m=39
v0=0 []            v0=1 [2]            v0=0 []             v0=2 [2,2]          v0=2 [2,2]
v1=1 [2]           v1=2 [2,2]          v1=0 []             v1=5 [2,2,2,2,2]    v1=5 [2,2,2,2,2]
v2=1 [2]           v2=2 [2,2]          v2=0 []             v2=9 [8,4,4,2,2]    v2=10 [8,4,2,2,2,2,2]
mod=17,ell=7340033
m=17                m=19                m=21                m=38                m=26                m=226
v0=2 [4]            v0=6 [16,4]         v0=4 [16]           v0=5 [16,2]         v0=6 [16,2,2]        v0=5 [8,8]
v1=2 [4]            v1=6 [16,4]         v1=4 [16]           v1=5 [16,2]         v1=8 [16,4,2,2]      v1=10 [32,8,8]
REAL QUARATIC FIELDS, p=3, lambda=0:
mod=1,ell=109,m=326      ell=109,m=4409      mod=7,ell=163,m=5      ell=163,m=6
v0=1 [3]                v0=2 [9]            v0=1 [3]              v0=1 [3]
v1=1 [3]                v1=2 [9]            v1=1 [3]              v1=2 [3,3]
v2=1 [3]                v2=2 [9]            v2=1 [3]              v2=2 [3,3]
mod=7,ell=163,m=22      ell=163,m=15        mod=19,ell=163,m=2     ell=163,m=11
v0=2 [3,3]              v0=1 [3]            v0=2 [9]              v0=3 [9,3]
v1=2 [3,3]              v1=3 [3,3,3]        v1=3 [27]              v1=4 [27,3]
v2=2 [3,3]              v2=5 [9,9,3]        v2=3 [27]              v2=4 [27,3]
```

One finds examples of  $\lambda$ -stabilities taking for instance  $\#S = 6$  with three primes split in  $k = \mathbb{Q}(\sqrt{\pm m})$  and any of the 1024 totally  $S$ -ramified cyclic 2-towers  $K/k$  of

degree  $2^6$  contained in  $k(\mu_{257 \cdot 449 \cdot 577})$  but, unfortunately, only computing in  $k$  and  $k_1 = k(\sqrt{257 \cdot 449 \cdot 577})$  with  $\lambda = 4$  (resp. 5) for  $k$  real (resp. imaginary):

m=193	m=1591	m=2669	m=-527	m=-1739
v0=0 []	v0=1 [2]	v0=2 [4]	v0=1 [2]	v0=2 [4]
v1=4 [2,2,2,2]	v1=5 [2,2,2,2,2]	v1=6 [4,2,2,2,2]	v1=6 [4,2,2,2,2]	v1=7 [8,2,2,2,2]

**4.2. Cyclic  $p$ -towers over  $\mathbb{Q}$  with modulus.** In a cyclic  $p$ -tower  $K/\mathbb{Q}$  for  $S = \{\ell\}$ ,  $\mathfrak{m} = 1$ , (2.1) shows that  $\lambda = 0$  and  $\#\mathcal{C}_n = 1$  for all  $n$ . For  $\mathfrak{m} \neq 1$ , a stability may occur (possibly from a stage  $n_0 > 0$ ) as shown by the following examples ( $p = 2, 3$ ) analogous to [23, Example 4.1]:

```
{p=2;ell=257;mod=17;N=5;print("p=",p," ell=",ell," mod=",mod);for(n=0,N,
Pn=polsubcyclo(ell,p^n);kn=bnfinit(Pn,1);\\layer kn
knmod=bnrinit(kn,mod);v=valuation(knmod.no,p);Ckn=knmod.cyc;\\ray class field
C=List;e=matsize(Ckn)[2];for(k=1,e,c=Ckn[e-k+1];w=valuation(c,p);
if(w>0,listinsert(C,p^w,1)));print("v",n,"=",v," Ck",n,"=",C))}
p=2,ell=257,mod=17  ell=257,mod=4*17  p=3,ell=163,mod=19  ell=163,mod=9*19
v0=3 [8]  v0=4 [16]  v0=2 [9]  v0=3 [9,3]
v1=4 [16]  v1=5 [16,2]  v1=3 [27]  v1=5 [27,3,3]
v2=4 [16]  v2=7 [16,2,2,2]  v2=3 [27]  v2=6 [81,3,3]
v3=4 [16]  v3=11 [16,2,2,2,2,2,2,2]  v3=3 [27]  v3=6 [81,3,3]
v4=4 [16]  v4=12 [32,2,2,2,2,2,2,2]  v3=6 [81,3,3]
v5=4 [16]  v5=12 [32,2,2,2,2,2,2,2]
```

**4.3. Cyclic  $p$ -towers over a cyclic cubic field  $k$ .** Let  $K \subset k(\mu_\ell)$  be a  $p$ -tower. An interesting fact is that, in most cases, the stability occurs (with  $\lambda = 0$  in the case  $S = S_\ell$ ); we give an excerpt with the defining polynomial  $P$  of  $k$  of conductor  $f \in [\text{bf}, \text{Bf}]$ :

```
{p=2;ell=257;N=3;bf=7;Bf=10^3;for(f=bf,Bf,h=valuation(f,3);if(h!=0 & h!=2,next);
F=f/3^h;if(core(F)!=F,next);F=factor(F);Div=component(F,1);d=matsize(F)[1];for(j=1,d,
D=Div[j];if(Mod(D,3)!=1,break));for(b=1,sqrt(4*f/27),if(h==2 & Mod(b,3)==0,next);
A=4*f-27*b^2;if(issquare(A,&a)==1,\\computation of a and b such that f=(a^2+27b^2)/4
if(h==0,if(Mod(a,3)==1,a=-a);P=x^3+x^2+(1-f)/3*x+(f*(a-3)+1)/27);
if(h==2,if(Mod(a,9)==3,a=-a);P=x^3-f/3*x-f*a/27);print();print("f=",f," P=",P);
\\end of computation of P defining k
for(n=0,N,Pn=polcompositum(polsubcyclo(ell,p^n),P)[1];kn=bnfinit(Pn,1);
v=valuation(kn.no,p);Ckn=kn.cyc;C=List;e=matsize(Ckn)[2];for(k=1,e,c=Ckn[e-k+1];
w=valuation(c,p);if(w>0,listinsert(C,p^w,1)));print("v",n,"=",v," Ck",n,"=",C))}}
p=2,ell=257,lambda=0
f=63  f=163  f=277  f=279
P=x^3-21*x-35  P=x^3+x^2-54*x-169  P=x^3+x^2-92*x+236  P=x^3-93*x+217
v0=0 []  v0=2 [2,2]  v0=2 [2,2]  v0=0 []
v1=2 [2,2]  v1=4 [4,4]  v1=4 [2,2,2,2]  v1=2 [2,2]
v2=2 [2,2]  v2=4 [4,4]  v2=6 [2,2,2,2,2,2]  v2=4 [4,4]
v3=2 [2,2]  v3=4 [4,4]  v3=6 [2,2,2,2,2,2]  ?
f=333  f=349  f=397  f=547
P=x^3-111*x+37  P=x^3+x^2-116*x-517  P=x^3+x^2-132*x-544  P=x^3+x^2-182*x-81
v0=0 []  v0=2 [2,2]  v0=2 [2,2]  v0=2 [2,2]
v1=4 [4,4]  v1=4 [2,2,2,2]  v1=2 [2,2]  v1=4 [2,2,2,2]
v2=4 [4,4]  v2=4 [2,2,2,2]  v2=2 [2,2]  v2=6 [4,4,2,2]
p=3,ell=109,lambda=0
f=1687  f=1897  f=2359  f=5383
x^3+x^2-562*x-4936  x^3+x^2-632*x-4075  x^3+x^2-786*x+7776  x^3+x^2-1794*x+17744
v0=1 [3]  v0=1 [3]  v0=2 [3,3]  v0=3 [9,3]
v1=1 [3]  v1=1 [3]  v1=2 [3,3]  v1=3 [9,3]
```

As for the quadratic case, we may use  $k_1 = k(\sqrt{257 \cdot 449 \cdot 577})$  for  $p = 2$  with  $\#S = 9$ ,  $\rho = 2$ ,  $\lambda = 6$ . The contribution of the 2-tower over  $\mathbb{Q}$  is given by the 2-stability from the structures  $[\ ]$ ,  $[2, 2]$ . We find a great lot of  $\lambda$ -stabilities with the structures  $[\ ]$ ,  $[2, 2, 2, 2, 2, 2]$  or  $[2, 2]$ ,  $[4, 4, 2, 2, 2, 2]$  and very few exceptions for which one does not know if a  $\lambda$ -stabilization does exist for  $n > 1$  (case of  $f = 1531$  below):

$f=171, P=x^3-57*x-152$	$f=349, P=x^3+x^2-116*x-517$	$f=1531, P=x^3+x^2-510*x-567$
$Ck0=[]$	$Ck0=[2, 2]$	$Ck0=[]$
$Ck1=[2, 2, 2, 2, 2, 2]$	$Ck1=[4, 4, 2, 2, 2, 2]$	$Ck1=[4, 4, 2, 2, 2, 2]$

## 5. OTHER EXAMPLES OF APPLICATIONS

Assume the total ramification of  $S \neq \emptyset$  in the cyclic  $p$ -tower  $K/k$  and the main condition  $\#\mathcal{X}_1 = \#\mathcal{X} \cdot p^\lambda$  with  $\lambda = \max(0, \#S - 1 - \rho)$  (Definition 1.1); remember that it is easy to ensure that  $\text{tor}_{\mathbb{Z}}(E) \subset N_{K/k}(K^\times)$  (Remark 1.3):

(a) Let  $\tilde{k}/k$  be a  $\mathbb{Z}_p$ -extension with Iwasawa's invariants  $\tilde{\lambda}, \tilde{\mu}, \tilde{\nu}$ . We then have  $S = S_p$  with  $\#S_p \leq [k : \mathbb{Q}] = r_1 + 2r_2$  and  $\lambda = \max(0, \#S_p - r_1 - r_2) \in [0, r_2]$ ; one gets the formula  $\#\mathcal{C}_n = \#\mathcal{C} \cdot p^{\lambda \cdot n}$  for all  $n$ , as soon as  $\#\mathcal{C}_1 = \#\mathcal{C} \cdot p^\lambda$  holds, and in that case,  $\tilde{\lambda}$  is equal to  $\lambda$  and  $\tilde{\mu} = 0$ ; the Iwasawa formula being  $\#\mathcal{X}_n = p^{\lambda \cdot n + \nu}$  with  $p^\nu := \#\mathcal{X}$ . For CM-fields  $k$  with  $p$  totally split in  $k$ ,  $\lambda = \frac{1}{2}[k : \mathbb{Q}]$ .

When  $k$  is totally real, Greenberg's conjecture [10] ( $\tilde{\lambda} = \tilde{\mu} = 0$ ) holds if and only if  $\#\mathcal{C}_{n_0+1} = \#\mathcal{C}_{n_0}$  is fulfilled for some  $n_0 \geq 0$  ( $\lambda$ -stabilization with  $\lambda = \tilde{\lambda} = 0$ ), which may be checked if  $n_0$  is not too large by chance (as in [19] for real quadratic fields,  $p = 3$  non-split, or in various works of Taya [27], Fukuda, Komatsu).

(b) Taking  $\mathcal{H}_N = \mathcal{C}_N^{p^e}$  may give the  $\lambda$ -stability of the  $\mathcal{C}_n/\mathcal{C}_n^{p^e}$ 's, for some  $\lambda(e)$ , whence  $\text{rk}_p(\mathcal{C}_n) = \text{rk}_p(\mathcal{C}) + \lambda(1) \cdot n$  for all  $n$ , as soon as this equality holds for  $n = 1$  (where  $\text{rk}_p(A) := \dim_{\mathbb{F}_p}(A/A^p)$ ). For instance, let  $k = \mathbb{Q}(\sqrt{-m})$  and  $K \subset k(\mu_{257})$  and consider the stability of the 2-ranks when  $\text{rk}_2(\mathcal{C}) \geq 1$  ( $\lambda(1) = 0$  since  $\#S \leq 2$  and  $\rho = t \geq 1$  since  $\mathcal{C} \neq 1$ ); we find many examples:

For  $m \in \{-15, -35, -95, -111, -123, -159, -215, -235, -259, -287, -291, -303, -327, -355, -371, -415, -447, \dots\}$  the 2-rank is 1 and stable from  $n = 0$ .

For  $m \in \{-39, -87, -91, -155, -183, -195, -203, -247, -267, -295, -339, -395, -399, -403, -427, -435, -455, -471, \dots\}$  the 2-rank (2 or 3) is stable from  $n_0 = 1$ .

For  $m = -55$  (successive structures  $[4], [4, 4], [8, 4, 4, 2], [16, 8, 8, 4]$ ),  $m = -115$  (structures  $[2], [2, 2], [2, 2, 2, 2], [8, 8, 8, 8]$ ), we have two examples of stabilization from  $n_0 = 2$  (rank 4); the computations for the 4th stages are rapidly out of reach.

We see that the orders are not necessarily  $\lambda'$ -stable from  $n = 0$  ( $\lambda' = \#S - 1$ ):

$m=-15$	$m=-403$	$m=-259$	$m=-95$	$m=-195$	$m=-895$
$v0=1 [2]$	$v0=1 [2]$	$v0=2 [4]$	$v0=3 [8]$	$v0=2 [2, 2]$	$v0=4 [16]$
$v1=2 [4]$	$v1=5 [8, 2, 2]$	$v1=3 [8]$	$v1=4 [16]$	$v1=4 [4, 2, 2]$	$v1=5 [32]$
$v2=3 [8]$	$v2=8 [16, 4, 4]$	$v2=4 [16]$	$v2=5 [32]$	$v2=9 [8, 8, 8]$	$v2=6 [64]$
$v3=4 [16]$	$v3=11 [32, 8, 8]$	$v3=5 [32]$	$v3=6 [64]$	$v3=12 [16, 16, 16]$	$v3=7 [128]$

(c) If  $K/\mathbb{Q}$  is abelian with  $p \nmid [k : \mathbb{Q}]$ ,  $\lambda$ -stabilities may hold for the isotopic  $\mathbb{Z}_p[\text{Gal}(k/\mathbb{Q})]$ -components of the  $\mathcal{X}_n$ 's, using fixed points formulas [13, 14].

6. BEHAVIOR IN  $p$ -CYCLIC TOWERS OF OTHER INVARIANTS

In relation with class field theory and the cohomology of the Galois group  $\mathcal{G}_{k,S_p}$  of the maximal  $p$ -ramified pro- $p$ -extension of  $k$  and of its local analogues  $\mathcal{G}_{k_p}$ , the fundamental Tate–Chafarevich groups [17, Theorem 3.74], [24, § 1]:

$$\text{III}_k^i(S_p) := \text{Ker}[\text{H}^i(\mathcal{G}_{k,S_p}, \mathbb{F}_p) \rightarrow \bigoplus_{\mathfrak{p} \in S_p} \text{H}^i(\mathcal{G}_{k_p}, \mathbb{F}_p)], \quad i = 1, 2,$$

can be examined in the same way, in towers, as for generalized class groups. This is possible for  $\text{III}_k^1(S_p) \simeq (\mathcal{C}_k/\mathcal{d}_k(S_p)) \otimes \mathbb{F}_p$ , but  $\text{III}_k^2(S_p)$  does not appear immediately as a generalized class group and is not of easy computational access (see [12] for a thorough study of  $\text{III}_k^2(S)$  when  $S_p \not\subseteq S$ ). Nevertheless, we have an arithmetic interpretation, much more easily computable and having well-known properties, with the key invariant, closely related to  $\text{III}_k^2(S_p)$ ,

$$\mathcal{T}_k := \text{tor}_{\mathbb{Z}_p}(\mathcal{G}_{k,S_p}^{\text{ab}}) \simeq \text{H}^2(\mathcal{G}_{k,S_p}, \mathbb{Z}_p)^* \quad [24, \text{Théorème 1.1}]$$

(see other rank computations in [6, Theorem III.4.2 and Corollaries]). Nevertheless,  $\mathcal{T}_k$ , linked to the residue at  $s = 1$  of  $p$ -adic  $\zeta$ -functions [2], gives rise to some analogies with generalized class groups (due to reflection theorems [6, Theorem II.5.4.5]). See in [8] the interpretation of  $\mathcal{T}_k$  with the  $p$ -class group  $\mathcal{C}_k$  and the normalized  $p$ -adic regulator  $\mathcal{R}_k$ . Since the deep aspects of these cohomology groups are due to the  $p$ -adic properties of global units we shall restrict ourselves to the totally real case under Leopoldt’s conjecture. For any field  $\kappa$ , let  $\tilde{\kappa}$  be its cyclotomic  $\mathbb{Z}_p$ -extension.

Let  $K/k$  be a totally real,  $S$ -ramified, cyclic  $p$ -tower; denote by  $S^{\text{ta}} \subseteq S$  the subset of tame places ( $S^{\text{ta}} \neq \emptyset$  is assumed totally ramified, but the subset  $S_p$  of  $p$ -places may be arbitrary). For all extensions  $L/F$  contained in  $K/k$ , the transfer maps  $\text{J}_{L/F} : \mathcal{T}_F \rightarrow \mathcal{T}_L$  are injective [6, Theorem IV.2.1] and the norm maps  $\text{N}_{L/F} : \mathcal{T}_L \rightarrow \mathcal{T}_F$  are surjective since  $\tilde{L}/\tilde{F}$  is totally  $S^{\text{ta}}$ -ramified. When  $L/F \subset \tilde{k}/k$ ,  $\text{N}_{L/F}$  is also surjective (indeed,  $\tilde{F} = \tilde{L} = \tilde{k}$ ).

**Lemma 6.1.** *Let  $K/k$  be a totally real cyclic  $p$ -tower of degree  $qp^N$ ,  $p$ -ramified or else totally ramified at  $S^{\text{ta}} \neq \emptyset$ , where  $q = p$  or  $4$ ; we assume that  $k \cap \mathbb{Q} = \mathbb{Q}$ . Then, for any  $L/F$ ,  $k \subseteq F \subseteq L \subseteq K$  and  $G := \text{Gal}(L/F)$ ,  $\#\mathcal{T}_F^G = \#\mathcal{T}_L \cdot \#G^{\#S^{\text{ta}}}$ .*

*Proof.* The fixed points formula is  $\#\mathcal{T}_L^G = \#\mathcal{T}_F \cdot \#G^{\#S^{\text{ta}}} \cdot p^{\rho-r}$  [6, Theorem IV.3.3, Exercise 3.3.1], where  $p^r = [L : F]$ ,  $\rho = \min_{\mathfrak{l} \in S^{\text{ta}}}(r; \dots, \nu_{\mathfrak{l}} + \varphi_{\mathfrak{l}} + \gamma_{\mathfrak{l}}, \dots)$  ( $p^{\nu_{\mathfrak{l}}} \sim q^{-1} \log(\ell)$  where  $\mathfrak{l} \cap \mathbb{Z} = \ell \mathbb{Z}$ ,  $p^{\varphi_{\mathfrak{l}}} =$  residue degree of  $\mathfrak{l}$  in  $k/\mathbb{Q}$ ,  $\gamma_{\mathfrak{l}} = 0$  by hypothesis). When  $S^{\text{ta}} \neq \emptyset$ , the existence (see [6, V, Theorem 2.9] for a characterization using explicit governing fields) of the cyclic  $p$ -tower  $K/k$  implies  $\mathcal{N}(\mathfrak{l}) \equiv 1 \pmod{qp^N}$ , for all  $\mathfrak{l} \in S^{\text{ta}}$ , where  $\mathcal{N}$  is the absolute norm; indeed, the inertia group of the local extension  $K_{\mathfrak{L}}/k_{\mathfrak{l}}$ ,  $\mathfrak{L} \mid \mathfrak{l}$ , is isomorphic to a subgroup of the multiplicative group of the residue field  $F_{\mathfrak{l}} \simeq \mathbb{F}_{\mathcal{N}(\mathfrak{l})}$  of  $\mathfrak{l}$ . So, we have  $\nu_{\mathfrak{l}} + \varphi_{\mathfrak{l}} \geq N$ . This explains the limitation of the level  $n$  to get the given fixed points formula in any case.  $\square$

If a  $\lambda$ -stability does exist, we have  $\mathcal{T}_1 = \mathcal{T}_1^{G^1}$  of order  $\#\mathcal{T} \cdot p^{\lambda}$ , whence  $\lambda = \#S^{\text{ta}}$  which is compatible with  $\mathcal{T}_n = \mathcal{T}_n^{G^n}$  of order  $\#\mathcal{T} \cdot p^{\lambda n}$ , for all  $n \in [0, N]$ .

However, the properties of the groups  $\mathcal{T}_n$  will give non-trivial Iwasawa’s  $\tilde{\mu}$ -invariants in  $\tilde{k}/k$  and very large ranks in cyclic  $p$ -towers with tame ramification; moreover  $\tilde{\lambda}$  may be much larger than  $\#S^{\text{ta}}$  which explain that the  $\lambda$ -stability problem is not pertinent in this framework. A reason (based on the properties, in

$k_{n+m}/k_n$ ,  $m \geq 1$ , of the norms  $N_n^m$  (surjectivity) and transfer maps  $J_n^m$  (injectivity) is the following, where  $g_n^m := \text{Gal}(k_{n+m}/k_n)$ :

From  $1 \rightarrow J_n^m \mathcal{T}_n \rightarrow \mathcal{T}_{n+m} \rightarrow \mathcal{T}_{n+m}/J_n^m \mathcal{T}_n \rightarrow 1$ , we get:

$$1 \rightarrow \mathcal{T}_{n+m}^{g_n^m} / J_n^m \mathcal{T}_n \rightarrow (\mathcal{T}_{n+m} / J_n^m \mathcal{T}_n)^{g_n^m} \rightarrow H^1(g_n^m, J_n^m \mathcal{T}_n) \rightarrow H^1(g_n^m, \mathcal{T}_{n+m}),$$

where  $H^1(g_n^m, J_n^m \mathcal{T}_n) = (J_n^m \mathcal{T}_n)[p^m] \simeq \mathcal{T}_n[p^m]$  and:

$$\#H^1(g_n^m, \mathcal{T}_{n+m}) = \#H^2(g_n^m, \mathcal{T}_{n+m}) = \#(\mathcal{T}_{n+m}^{g_n^m} / J_n^m \mathcal{T}_n) = p^{m \cdot \#S^{\text{ta}}}.$$

We then obtain  $\#\mathcal{T}_{n+m} \geq \#\mathcal{T}_{n+m}^{g_n^m} = \#\mathcal{T}_n \cdot p^{m \cdot \#S^{\text{ta}}}$ , which seems less precise than the following one, because of the fact that  $\#S^{\text{ta}}$  is independent of  $n$ :

$$(6.1) \quad \#\mathcal{T}_{n+m} \geq \#\mathcal{T}_n \cdot \#\mathcal{T}_n[p^m].$$

For  $m = 1$  one gets  $\#\mathcal{T}_{n+1} \geq \#\mathcal{T}_n \cdot p^{\text{rk}_p(\mathcal{T}_n)}$ . This tendency to give large orders and  $p$ -ranks is enforced by the presence of tame ramification (see §6.2 for numerical illustrations) and leads to the vast theory of pro- $p$ -extensions and Galois cohomology of pro- $p$ -groups in a broader context than  $p$ -ramification theory, which is not our purpose (see [11] for more information). This explains that Corollary 3.2 never applies for the invariant  $\mathcal{T}$  (except  $\mathcal{T} = 1$ ). It would be interesting to give an analogous study for the Jaulent logarithmic class group [16] since its capitulation in the cyclotomic  $\mathbb{Z}_p$ -extension of  $k$  (real) characterizes Greenberg's conjecture.

**Remark 6.2.** For  $p$ -class groups  $\mathcal{C}_n$  in totally real  $p$ -towers, one obtains an inequality similar to (6.1) provided one replaces  $\mathcal{C}_n$  by  $J_n^m \mathcal{C}_n$ , where  $J_n^m$  is in general non-injective, a crucial point in this comparison. But for CM-fields  $k$ ,  $J_n$  is injective on the "minus parts", giving  $\#\mathcal{C}_{n+m}^- \geq \#\mathcal{C}_n^- \cdot \#\mathcal{C}_n^-[p^m]$ , which explains the results for imaginary quadratic fields in §4.1, especially for  $m = -782$  and  $m = -858$ , for which we can predict  $\#\mathcal{C}_4$  larger than  $2^{54}$  and  $2^{46}$ , respectively.

**Remark 6.3.** One can wonder about the contribution of the  $p$ -towers contained in  $\mathbb{Q}(\mu_\ell)$ ,  $\ell \equiv 1 \pmod{qp^N}$ , used in the compositum with  $k$ ; in  $\tilde{\mathbb{Q}}$ , it is clear that  $\mathcal{T}_n = 1$  for all  $n \geq 0$ , which is not the case in a finite cyclic  $p$ -tower when tame ramification is allowed; we have the following examples of  $\mathcal{T}_n$  for  $p = 2, 3$  and  $\#S^{\text{ta}} = 1$ ; let  $\text{vn}, \text{rk}_n$  denote the  $p$ -valuation, the  $p$ -rank, of  $\mathcal{T}_n$ , respectively; the parameter  $E$  must be chosen such that  $E > e + 1$ , where  $p^e$  is the exponent of  $\mathcal{T}_n$ . Then the structure follows:

```
{p=3;e11=17497;E=8;print("p=",p," e11=",e11);for(n=0,4,
Qn=polsubcyclo(e11,p^n);kn=bnfinit(Qn,1);\ layer kn
KpEn=bnrinit(kn,p^E);HpEn=KpEn.cyc;\computation of Tn
T=List;e=matsize(HpEn)[2];Rn=0;vn=0;for(k=1,e-1,c=HpEn[e-k+1];w=valuation(c,p);
if(w>0,vn=vn+w;Rn=Rn+1;listinsert(T,p^w,1));)\computation of vn and rk
print("v",n,"=",vn," rk",n,"=",Rn," ",T)}}

p=2,e11=17          p=2,e11=7681          p=2,e11=257
v0=0 rk0=0 []      v0=0 rk0=0 []      v0=0 rk0=0 []
v1=1 rk1=1 [2]     v1=1 rk1=1 [2]     v1=3 rk1=1 [8]
v2=2 rk2=1 [4]     v2=2 rk2=1 [4]     v2=7 rk2=3 [16,4,2]
v3=3 rk3=1 [8]     v3=3 rk3=1 [8]     v3=13 rk3=7 [32,8,2,2,2,2,2]
v4=4 rk4=1 [16]    v4=4 rk4=1 [16]    v4=23 rk4=15 [64,16,2,2,2,2,2,2,2,2,2,2,2,2]
v5=38 rk5=15 [128,32,4,4,4,4,4,4,4,4,4,4,4,4,4,4]
```

```
p=3,e11=109        p=3,e11=163          p=3,e11=487          p=3,e11=17497
v0=0 rk0=0 []      v0=0 rk0=0 []      v0=0 rk0=0 []      v0=0 rk0=0 []
v1=1 rk1=1 [3]     v1=1 rk1=1 [3]     v1=2 rk1=2 [3,3]    v1=3 rk1=2 [9,3]
v2=2 rk2=1 [9]     v2=2 rk2=1 [9]     v2=4 rk2=2 [9,9]    v2=6 rk2=3 [27,9,3]
```

v3=3 rk3=1 [27]    v3=3 rk3=1 [27]

**6.1. Case of the cyclotomic  $\mathbb{Z}_p$ -extensions  $\tilde{k}/k$  of  $k$  real.** The Iwasawa invariants  $\tilde{\lambda}, \tilde{\mu}, \tilde{\nu}$ , attached to  $\lim_{\leftarrow} \mathcal{T}_n$  satisfy  $\tilde{\lambda} = \tilde{\mu} = 0$  if and only if  $\mathcal{T} = 1$  (in which case  $\tilde{\nu} = 0$ ). Indeed, if  $\tilde{\lambda} = \tilde{\mu} = 0$ ,  $\#\mathcal{T}_n = p^{\tilde{\nu}}$  for all  $n \gg 0$ ; but (6.1) gives  $\tilde{\nu} \geq \tilde{\nu} + r_n$ , where  $r_n := \text{rk}_p(\mathcal{T}_n)$ , whence  $r_n = 0$ ; but  $r_n \geq r$ , so  $r = 0$  ( $J_n$  is injective). The reciprocal comes from  $\mathcal{T}_n^{G_n} \simeq \mathcal{T}$  since  $S^{\text{ta}} = \emptyset$ . Thus a  $\lambda$ -stability does exist only for  $\lambda = 0$ , which is excluded if  $\mathcal{T} \neq 1$ . Computations suggest that the true Iwasawa parameters  $\tilde{\lambda}, \tilde{\mu}$  may be often non-zero, even if few levels are accessible with PARI/GP ( $\#\text{Sp}$  is the number of  $p$ -places of  $k$ ):

```
{p=3;E=8;N=4;bm=2;Bm=10^3;for(m=bm,Bm,if(core(m)!=m,next);P=x^2-m;
S=1;if(kronecker(m,p)==1,S=2);print();print("p=",p," m=",m," #Sp=",S);
for(n=0,N,if(p==2,Qn=x;for(k=1,n,Qn=Qn^2-2));if(p!=2,Qn=polsubcyclo(p^(n+1),p^n));
Pn=polcompositum(Qn,P)[1];kn=bnfinit(Pn,1);Cn=kn.cyc;\\class group Cn
knp=bnrinit(kn,p^E);Rn=0;vn=0;Ckn=knp.cyc;\\computation of Tn
T=List;e=matsize(Ckn)[2];for(k=1,e-1,c=Ckn[e-k+1];w=valuation(c,p);
if(w>0,vn=vn+w;Rn=Rn+1;listinsert(T,p^w,1));\\computation of vn and rk
print("v",n,"=",vn," rk",n,"=",Rn," ",T," C",n,"=",Cn)))}
m=33,#Sp=2                    m=41,#Sp=2                    m=217,#Sp=2
v0=1 rk0=1 [2]    C0=[]    v0=4 rk0=1 [16]    C0=[]    v0=2 rk0=2 [2,2]                    C0=[]
v1=4 rk1=1 [16]    C1=[]    v1=5 rk1=1 [32]    C1=[2]    v1=4 rk1=3 [4,2,2]                    C1=[2]
v2=5 rk2=1 [32]    C2=[]    v2=6 rk2=1 [64]    C2=[4]    v2=8 rk2=5 [4,4,4,2,2]                    C2=[2]
v3=6 rk3=1 [64]    C3=[]    v3=7 rk3=1 [128]    C3=[8]    v3=15 rk3=9 [8,8,8,2,2,2,2,2,2]                    C3=[2]
v4=7 rk4=1 [128]    C4=[]    v4=8 rk4=1 [256]    C4=[8]    v4=24 rk4=9 [16,16,16,4,4,4,4,4,4]                    C4=[2]
m=193,#Sp=2                    m=69,#Sp=1
v0=1 rk0=1 [2]    C0=[]    v0=2 rk0=1 [4]                    C0=[]
v1=2 rk1=2 [2,2]    C1=[]    v1=4 rk1=2 [4,4]                    C1=[]
v2=4 rk2=4 [2,2,2,2]    C2=[]    v2=6 rk2=2 [8,8]                    C2=[]
v3=8 rk3=8 [2,2,2,2,2,2,2,2]    C3=[]    v3=8 rk3=2 [16,16]                    C3=[]
v4=16 rk4=15 [4,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2]    C4=[]
m=62,#Sp=1                    m=103,#Sp=2                    m=1714,#Sp=2
v0=1 rk0=[3]    C0=[]    v0=1 rk0=1 [3]    C0=[]    v0=2 rk0=2 [3,3]                    C0=[3]
v1=3 rk1=[9,3]    C1=[]    v1=3 rk1=2 [9,3]    C1=[3,3]    v1=5 rk1=4 [9,3,3,3]                    C1=[3,3]
v2=5 rk2=[27,9]    C2=[]    v2=5 rk2=2 [27,9]    C2=[3,3]    v2=9 rk2=4 [27,9,9,9]                    C2=[9,3]
```

Formula (6.1) predicts  $\#\mathcal{T}_5 \geq 2^{16+15} = 2^{31}$  for  $m = 193$ , giving probably  $\tilde{\mu} = 1$ .

**6.2. Case of real cyclic  $p$ -towers with tame ramification.** In the case of  $S_\ell$ -ramified cyclic  $p$ -towers, one gets spectacular groups  $\mathcal{T}_n$  (with  $\#\mathcal{T}_{n+1} \geq \#\mathcal{T}_n \cdot \#\mathcal{T}_n[p]$  for  $n \in [0, N]$ ); for example let  $k = \mathbb{Q}(\sqrt{m})$ ,  $K = k(\mu_{257})$  with  $p = 2$ , then  $K = k(\mu_{109})$  and  $K = k(\mu_{163})$  with  $p = 3$ :

```
{p=2;ell=257;N=3;E=8;bm=2;Bm=10^3;for(m=bm,Bm,if(core(m)!=m,next);P=x^2-m;S=1;
if(kronecker(m,ell)==1,S=2);print();print("p=",p," ell=",ell," m=",m," #S=",S);
for(n=0,N,Pn=polcompositum(polsubcyclo(ell,p^n),P)[1];kn=bnfinit(Pn,1);\\layer kn
Ckn=kn.cyc;C=List;e=matsize(Ckn)[2];for(k=1,e,c=Ckn[e-k+1];w=valuation(c,p);
if(w>0,listinsert(C,p^w,1));\\structure of the p-class group Cn
Kpn=bnrinit(kn,p^E);Hpn=Kpn.cyc;T=List;e=matsize(Hpn)[2];\\computation of Tn
Rn=0;vn=0;for(k=1,e-1,c=Hpn[e-k+1];w=valuation(c,p);if(w>0,Rn=Rn+1;vn=vn+w;
listinsert(T,p^w,1));print("v",n,"=",vn," rk",n,"=",Rn," ",T," C",n,"=",C))}

p=2,ell=257,m=17 #S=2
v0=1 rk0=1 [2]    C0=[]
v1=7 rk1=3 [16,4,2]    C1=[]
v2=16 rk2=7 [32,8,8,4,2,2,2]    C2=[]
v3=31 rk3=15 [64,16,16,4,4,4,4,2,2,2,2,2,2,2,2]    C3=[]
```



- [17] H. Koch, *Galois theory of  $p$ -extensions* (English translation of “*Galoissche Theorie der  $p$ -Erweiterungen*”, 1970), Springer Monographs in Math., Springer, 2002. 11
- [18] P. Koymans, C. Pagano, *On the distribution of  $Cl(K)[\ell^\infty]$  for degree  $\ell$  cyclic fields*, J. Eur. Math. Soc. (to appear). <https://arxiv.org/pdf/1812.06884> 7
- [19] J.S. Kraft, R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. **97**(1-2) (1995), 135–155. <http://eudml.org/doc/90370> 10
- [20] J. Li, Y. Ouyang, Y. Xu, S. Zhang,  *$\ell$ -Class groups of fields in Kummer towers* (2020). <https://arxiv.org/pdf/1905.04966v2.pdf> 3
- [21] J. Li, C.F. Yu, *The Chevalley–Gras formula over global fields*, J. Théor. Nombres Bordeaux **32**(2) (2020), 525–543. <https://doi.org/10.5802/jtnb.1133> 4
- [22] Y. Mizusawa, *Tame pro-2 Galois groups and the basic  $\mathbb{Z}_2$ -extension*, Trans. Amer. Math. Soc. **370**(4) (2018), 2423–2461. <https://doi.org/10.1090/tran/7023> 4
- [23] Y. Mizusawa, K. Yamamoto, *On  $p$ -class groups of relative cyclic  $p$ -extensions*, Arch. Math. (2021). <https://doi.org/10.1007/s00013-021-01619-8> 4, 9
- [24] T. Nguyen Quang Do, *Sur la  $\mathbb{Z}_p$ -torsion de certains modules galoisiens*, Ann. Inst. Fourier **36**(2) (1986), 27–46. <https://doi.org/10.5802/aif.1045> 11
- [25] The PARI Group, *PARI/GP, version 2.9.0*, Université de Bordeaux (2016). <http://pari.math.u-bordeaux.fr/> 2
- [26] A. Smith,  *$2^\infty$ -Selmer groups,  $2^\infty$ -class groups and Goldfeld’s conjecture* (2017). <https://arxiv.org/abs/1702.02325> 7
- [27] H. Taya, *Computation of  $\mathbb{Z}_3$ -invariants of real quadratic fields*, Math. Comp. **65**(214), 779–784. <https://doi.org/10.1090/S0025-5718-96-00721-1> 10
- [28] 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> 3

VILLA LA GARDETTE, CHEMIN CHÂTEAU GAGNIÈRE, F-38520 LE BOURG D’OISANS  
Email address: g.mm.gras@wanadoo.fr