



HAL
open science

The p -rank epsilon-conjecture on class groups is true for p -extensions

Georges Gras

► **To cite this version:**

Georges Gras. The p -rank epsilon-conjecture on class groups is true for p -extensions. 2020. hal-02444876v1

HAL Id: hal-02444876

<https://hal.science/hal-02444876v1>

Preprint submitted on 19 Jan 2020 (v1), last revised 22 Feb 2020 (v2)

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.

THE p -RANK ε -CONJECTURE ON CLASS GROUPS IS TRUE FOR p -EXTENSIONS

GEORGES GRAS

ABSTRACT. We prove the p -rank ε -conjecture on the class groups \mathcal{C}_F for the p -extensions F/κ of degree p^e and, more generally, for a tower of degree p cyclic fields: $\#(\mathcal{C}_F \otimes \mathbb{F}_p) \ll_{\kappa, p^e, \varepsilon} (\sqrt{|D_F|})^\varepsilon$, where D_F is the discriminant and κ any base field (Theorem 3.5). This Note generalizes the case $e = 1$ and $\kappa = \mathbb{Q}$ (*Genus theory and ε -conjectures on p -class groups*, J. Number Theory **207** (2020), 423–459), whose techniques appear to be “universal” for all relative p -cyclic-extensions. We prove the p -rank ε -conjecture for the F/κ and the cohomology groups $H^2(\mathcal{G}_F, \mathbb{Z}_p)$ of Galois p -ramification theory (Theorem 4.3).

1. INTRODUCTION

For any prime number p and any number field F , we denote by \mathcal{C}_F the p -class group of F in the restricted sense; to avoid any ambiguity, we shall write $\mathcal{C}_F \otimes \mathbb{F}_p$ for the “ p -torsion group”, also denoted $\mathcal{C}_F[p]$ in the literature, giving the p -rank $\text{rk}_p(\mathcal{C}_F) := \dim_{\mathbb{F}_p}(\mathcal{C}_F/\mathcal{C}_F^p)$ of \mathcal{C}_F .

We refer to our paper [3] for an introduction with some history about the notion of ε -conjecture, initiated by Ellenberg–Venkatesh [2], the related density results of Koymans–Pagano [9], and also for the large bibliography that we shall not reproduce in this Note. We prove, unconditionally:

Main results. *Let \mathcal{C}_F denotes the p -class group of a number field F and D_F its discriminant. The general p -rank ε -conjecture is true for the family of p -extensions F/κ of degree p^e over a fixed number field κ : for all $\varepsilon > 0$, there exists a constant $C_{\kappa, p^e, \varepsilon}$, such that $\#(\mathcal{C}_F \otimes \mathbb{F}_p) \leq C_{\kappa, p^e, \varepsilon} \cdot (\sqrt{|D_F|})^\varepsilon$, for all such p -extensions of κ . The result is true for any (non-necessary Galois) p -tower F/κ , $\kappa = F_0 \subset \cdots \subset F_{i-1} \subset F_i \cdots \subset F_e = F$ for which F_i/F_{i-1} is Galois for all $i \in [1, e]$, which is equivalent to consider towers (called “ p -cyclic-towers”) of successive degree p cyclic extensions. In Section 4 we obtain a similar statement for the cohomology groups $H^2(\mathcal{G}_F, \mathbb{Z}_p)$ of Galois p -ramification theory.*

Note. After the writing of this article, we have been informed of papers by Wang [13] and Klüners–Wang [10] containing similar results on class groups with other information (e.g., Cornell paper [1] using genus theory in elementary p -extensions with some restriction on the ramification, then generalized in [10]). We thank Jiuya Wang for these communications. It is interesting to see that the two methods in [3, 10] use classical analytical results on prime numbers and refer to [12]. Our result is unconditional contrary to [10] where the “ ε -inequality” is valid for $D_F \gg 0$.

Date: January 16, 2020.

2010 Mathematics Subject Classification. 11R29, 11R37.

Key words and phrases. p -class groups; ε -conjectures; class field theory; genus theory; discriminants; prime numbers.

2. PRINCIPLE OF THE METHOD

We will perform an induction in the successive degree p cyclic extensions, the general method for such p -cyclic steps having been given in [3]. The method involves using genus theory and minimal relative discriminants. This is of course the trivial part of the proof of the general ε -conjecture in degree d number fields, but $p \mid d$ may give large p -class groups as explained in [3, §2].

2.1. Tower of degree p cyclic fields. Let κ be any fixed number field and let:

$$F_0 = \kappa \subset F_1 \cdots \subset F_e = F, \quad e \geq 1,$$

be a p -cyclic-tower of fields with $\text{Gal}(F_i/F_{i-1}) \simeq \mathbb{Z}/p\mathbb{Z}$, for $1 \leq i \leq e$ (by abuse, we use the word of tower even if the fields F_i are not necessarily Galois over κ). Put $k = F_{i-1}$, $K = F_i$, $G = \text{Gal}(K/k) =: \langle \sigma \rangle$. We shall use the obvious general exact sequence:

$$1 \rightarrow \mathcal{C}_K^* \rightarrow \mathcal{C}_K \xrightarrow{\nu} \mathcal{C}_K^\nu,$$

where ν is the algebraic norm $1 + \cdots + \sigma^{p-1}$ and $\mathcal{C}_K^* = \text{Ker}(\nu)$.

Recall that $\nu = \text{J} \circ \text{N}$, where N is the arithmetic norm (or the restriction $\text{Gal}(H_K/K) \rightarrow \text{Gal}(H_k/k)$ of automorphisms in the corresponding Hilbert's class fields H_K, H_k), which yields $\text{N}(\mathcal{C}_K) \subseteq \mathcal{C}_k$ and where $\text{J} : \mathcal{C}_k \rightarrow \mathcal{C}_K$ comes from the extension of ideals of k to K (or is the transfer map $\text{Gal}(H_k/k) \rightarrow \text{Gal}(H_K/K)$); so $\mathcal{C}_K^\nu \simeq \mathcal{C}_k$ if and only if N is surjective (equivalent to $H_k \cap K = k$) and J injective (no capitulation).

Whence the obvious inequalities for the p -ranks:

$$(1) \quad \text{rk}_p(\mathcal{C}_K) \leq \text{rk}_p(\mathcal{C}_k) + \text{rk}_p(\mathcal{C}_K^*).$$

So, the main problem is to estimate $\text{rk}_p(\mathcal{C}_K^*)$ by giving an explicit upper bound only depending on \mathcal{C}_k , p and the number of ramified prime numbers.

2.2. $\mathbb{Z}_p[G]$ -modules annihilated by ν [6]. Let $G = \langle \sigma \rangle \simeq \mathbb{Z}/p\mathbb{Z}$. We consider a finite $\mathbb{Z}_p[G]$ -module M^* annihilated by $\nu = 1 + \cdots + \sigma^{p-1}$ (which will be later of the form $\mathcal{C}_{F_i}^*$) for which we define the following filtration, for $h \geq 0$ and $M_0^* = 1$:

$$M_{h+1}^*/M_h^* := (M^*/M_h^*)^G.$$

For all $h \geq 0$, $M_h^* = \{x \in M^*, x^{(1-\sigma)^h} = 1\}^1$, the p -groups M_{h+1}^*/M_h^* are elementary and the maps $M_{h+1}^*/M_h^* \xrightarrow{1-\sigma} M_h^*/M_{h-1}^*$ are injective, giving a decreasing sequence for the orders $\#(M_{h+1}^*/M_h^*)$ as h grows; whence:

$$\#(M_{h+1}^*/M_h^*) \leq \#M_1^*, \quad \text{for all } h.$$

Since M^* is a $\mathbb{Z}_p[G]/(\nu)$ -module and since $\mathbb{Z}_p[G]/(\nu) \simeq \mathbb{Z}_p[\zeta]$, where ζ is a primitive p th root of unity, we may write for $\mathfrak{p} = (1 - \zeta)\mathbb{Z}_p[\zeta]$ and $s \geq 0$:

$$M^* \simeq \bigoplus_{j=1}^s \mathbb{Z}_p[\zeta]/\mathfrak{p}^{n_j}, \quad n_1 \leq n_2 \leq \cdots \leq n_s,$$

and the sub-modules M_h^* are, in this $\mathbb{Z}_p[\zeta]$ -structure, the following ones:

$$M_h^* \simeq \bigoplus_{j, n_j \leq h} \mathbb{Z}_p[\zeta]/\mathfrak{p}^{n_j}, \quad \text{for all } h \geq 1.$$

¹Note that if M is a $\mathbb{Z}_p[G]$ -module and $M^* = \text{Ker}(\nu)$, we have, in an obvious meaning, $(M^*)_h = (M_h)^*$, whence the writing M_h^* .

Proposition 2.1. *Under the condition $M^{*\nu} = 1$, the p -rank of M^* fulfills the inequality $\text{rk}_p(M^*) \leq (p-1) \cdot \text{rk}_p(M_1^*)$.*

Proof. Let $M^*[p] := \{x \in M^*, x^p = 1\}$; since $p\mathbb{Z}_p[\zeta] = \mathfrak{p}^{p-1}$, we obtain that $M^*[p] = M_{p-1}^*$; then $\#M_{p-1}^* = \prod_{h=0}^{p-2} \#(M_{h+1}^*/M_h^*) \leq (\#M_1^*)^{p-1}$. Since M_{p-1}^* and M_1^* are elementary p -groups, the inequality on the p -ranks follows. \square

Corollary 2.2. *Let K/k be a degree p cyclic extension of number fields and let $G = \text{Gal}(K/k)$. Then $\text{rk}_p(\mathcal{C}_K^*) \leq (p-1) \text{rk}_p(\mathcal{C}_K^{G*}) = (p-1) \text{rk}_p(\mathcal{C}_K^G)$.*

2.3. Majoration of the $\text{rk}_p(\mathcal{C}_{F_i}^G)$. As above, put $k = F_{i-1}$, $K = F_i$, $1 \leq i \leq e$, and $G = \text{Gal}(K/k) =: \langle \sigma \rangle$. Consider $M = \mathcal{C}_K$. Then Corollary 2.2 gives $\text{rk}_p(\mathcal{C}_K^*) \leq (p-1) \text{rk}_p(\mathcal{C}_K^G)$ and we obtain the following upper bound:

Proposition 2.3. *We have $\text{rk}_p(\mathcal{C}_K^G) \leq \text{rk}_p(\mathcal{C}_k) + t_k + \text{rk}_p(E_k/E_k^p)$, where t_k is the number of prime ideals of k ramified in K/k and E_k the group of (totally positive) units of k .*

Proof. We have the classical exact sequence:

$$1 \rightarrow \mathcal{C}_K(I_K^G) \longrightarrow \mathcal{C}_K^G \xrightarrow{\theta} E_k \cap N_{K/k}(K^\times)/N_{K/k}(E_K) \rightarrow 1,$$

where I_K is the $\mathbb{Z}[G]$ -module of ideals of K and where θ associates with $\mathcal{C}_K(\mathfrak{A})$, such that $\mathfrak{A}^{1-\sigma} = (\alpha)$, $\alpha \in K^\times$, the class of the unit $N_{K/k}(\alpha)$ of k , modulo $N_{K/k}(E_K)$. The surjectivity and the kernel are immediate.

The $\mathbb{Z}[G]$ -module I_K^G is generated by the extension in K of the ideals of k and by the t_k prime ideals of K ramified in K/k . Thus, using the obvious inequality $\text{rk}_p(E_k \cap N_{K/k}(K^\times)/N_{K/k}(E_K)) \leq \text{rk}_p(E_k/E_k^p)$, we obtain:

$$\text{rk}_p(\mathcal{C}_K^G) \leq \text{rk}_p(\mathcal{C}_K(I_K^G)) + \text{rk}_p(E_k/E_k^p) \leq \text{rk}_p(\mathcal{C}_k) + t_k + \text{rk}_p(E_k/E_k^p),$$

which proves the claim. \square

Denote by $\{\ell_1, \dots, \ell_N\}$, $N \geq 0$, the set of tame primes ramified in K/k (for such an ℓ , there exist prime ideals $\mathfrak{l}_u \mid \ell$ in k , $u \in [1, t_{k,\ell}]$, $t_{k,\ell} \geq 1$, ramified in K/k).

Thus, $t_k = t_{k,p} + \sum_{j=1}^N t_{k,\ell_j}$. We shall replace $\text{rk}_p(E_k/E_k^p)$ then $t_{k,p}$, t_{k,ℓ_j} by the rough upper bound $d_k := [k : \mathbb{Q}]$, which gives, using inequality (1), Corollary 2.2 and Proposition 2.3:

Corollary 2.4. *Put $d_k = [k : \mathbb{Q}]$; then we have the inequalities:*

$$\begin{aligned} \text{rk}_p(\mathcal{C}_K^*) &\leq (p-1) \cdot [\text{rk}_p(\mathcal{C}_k) + (N+2)d_k], \\ \text{rk}_p(\mathcal{C}_K) &\leq p \cdot \text{rk}_p(\mathcal{C}_k) + (p-1)(N+2)d_k. \end{aligned}$$

3. ABOUT THE DISCRIMINANTS IN THE TOWER $(F_i)_{1 \leq i \leq e}$

Now, the purpose is to give lower bounds for discriminants, contrariwise for the previous case of p -ranks. Give some essential explanations:

Remark 3.1. We have given, in the previous section, an upper bound for the difference of p -ranks in K/k , where the number of ramified primes is crucial because of genus theory, so that any *real* p -ranks at the step K/k (whatever the p -cyclic tower F/κ having the same parameter N) will be *smaller*.

In the present section, we shall give a definition of the “minimal tame relative discriminant $D_N^* \in \mathbb{N}$ ” with N tame primes ℓ_j , possibly ramified in K/k (so that any *real* relative discriminant $D_{K/k} \in \mathbb{N}$ (whatever F/κ), eventually with a non-trivial p -part, will be *larger*). Then we shall apply: $D_K = D_k^p D_{K/k} \geq D_k^p D_N^*$. Thus, under this facts, if an “ ε -inequality” does exist between such fictitious p -ranks and discriminants, a fortiori, any real situation will fulfill the p -rank ε -inequality at this step.

3.1. The tame relative discriminant. As above, let $k = F_{i-1}$, $K = F_i$, for $1 \leq i \leq e$, and let \tilde{D}_k and \tilde{D}_K be the absolute values of *the tame parts* of the discriminants of k and K , respectively; then let $\tilde{D}_{K/k} \in \mathbb{N}$ be *the tame part* of the relative discriminant of K/k . If N is the number of tame prime numbers ℓ ramified in K/k , let $\mathfrak{l}_1, \dots, \mathfrak{l}_{t_{k,\ell}}$ be the prime ideals of k above ℓ , ramified in K/k . Taking the norm of the different of K/k , the tame part of the relative discriminant

is $\tilde{D}_{K/k} = \prod_{j=1}^N \prod_{u=1}^{t_{k,\ell_j}} \ell_{j,u}^{p-1}$, and, taking its norm, the “tame discriminant formula” [11, Ch. IV, Prop. 4, Ch. III, Prop. 8] is ($f_{k,\mathfrak{l}_{j,u}}$ is the residue degree of $\mathfrak{l}_{j,u}$ in k/\mathbb{Q}):

$$(2) \quad \tilde{D}_K = \tilde{D}_k^p \cdot N_{k/\mathbb{Q}}(\tilde{D}_{K/k}) = \tilde{D}_k^p \cdot \prod_{j=1}^N \prod_{u=1}^{t_{k,\ell_j}} \ell_j^{(p-1)f_{k,\mathfrak{l}_{j,u}}}.$$

We put $\tilde{D}_{K/k} := \prod_{j=1}^N \prod_{u=1}^{t_{k,\ell_j}} \ell_j^{(p-1)f_{k,\mathfrak{l}_{j,u}}} = \prod_{j=1}^N \ell_j^{(p-1) \cdot \sum_{u=1}^{t_{k,\ell_j}} f_{k,\mathfrak{l}_{j,u}}}$ and call it the tame relative discriminant.

3.2. Minimal tame relative discriminant. We fix $N \geq 0$ and intend to determine an absolute lower bound D_N^* of $\tilde{D}_{K/k}$, only depending on N , so that for every concrete ramification in K/k , with N tame primes ℓ_j and possibly that of p , the effective relative discriminant $D_{K/k} \geq \tilde{D}_{K/k}$ will be necessarily larger than D_N^* as explained in Remark 3.1. So we can state:

Lemma 3.2. *An universal lower bound of the tame relative discriminant $\tilde{D}_{K/k}$ is obtained when $t_{k,\ell_j} = f_{k,\mathfrak{l}_j} = 1$ for all $j = 1, \dots, N$; thus the “fictive” minimum of $\tilde{D}_{K/k}$ is then $D_N^* := \prod_{j=1}^N \ell_j^{p-1}$, taking the N successive prime numbers $\neq p$.*

By abuse, we call $D_N^* = \prod_{j=1}^N \ell_j^{p-1}$ the minimal tame relative discriminant (for $p = 2$, $D_N^* = 3 \cdot 5 \cdot 7 \cdot 11 \cdots \ell_N$); whence, an analogous framework as for the case of degree p cyclic number fields K/\mathbb{Q} given in [3], which allows an induction process in the p -cyclic-tower F/κ . Note that, when $\kappa \neq \mathbb{Q}$ the primes ℓ ramified in K/k are not necessarily $\equiv 1 \pmod{p}$; this shall not modify the nature of the results.

3.3. Induction. The case $i = 0$ ($k = \kappa$) is obvious since to get $p^{\text{rk}_p(\mathcal{O}_\kappa)} \leq C_{\kappa,p,\varepsilon} \cdot (\sqrt{D_\kappa})^\varepsilon$ it suffices to take $C_{\kappa,p,\varepsilon} = \frac{p^{\text{rk}_p(\mathcal{O}_\kappa)}}{\sqrt{D_\kappa}}$, a constant independent of ε , subject to state the ε -conjecture with $0 < \varepsilon < 1$ which is natural.

By induction, we assume (for $k := F_{i-1}$) that for all $\varepsilon > 0$ there exists a constant $C_{k,p,\varepsilon}$ such that $p^{\text{rk}_p(\mathcal{O}_k)} \leq C_{k,p,\varepsilon} \cdot (\sqrt{D_k})^\varepsilon$ independently of the number N_i of tame ramified primes ℓ_j in F_i/F_{i-1} ; then we shall prove the property at the level i .

From Corollary 2.4 we obtain the following inequality ($k = F_{i-1}$, $K = F_i$, $N = N_i$, $d_k := [k : \mathbb{Q}]$):

$$(3) \quad p^{\text{rk}_p(\mathcal{A}_K)} \leq p^{p \cdot \text{rk}_p(\mathcal{A}_k) + (p-1)(N+2)d_k} \leq C_{k,p,\varepsilon}^p \cdot \left(\sqrt{D_k^p}\right)^\varepsilon \cdot p^{(p-1)(N+2)d_k}.$$

Then, as explained in Remark 3.1, we will compare $p^{(p-1)(N+2)d_k}$ and $(\sqrt{D_N^*})^\varepsilon$, where (Lemma 3.2) $D_N^* = \prod_{j=1}^N \ell_j^{p-1}$, the ℓ_j being the N consecutive primes $\neq p$. But we have the required computations in [3, § 2.3, Formulas (4, 5), p. 10] that we give again with some obvious modifications.

Lemma 3.3. *There exists $c_{k,p,\varepsilon}$ such that $p^{(p-1)(N+2)d_k} \leq c_{k,p,\varepsilon} \cdot (\sqrt{D_N^*})^\varepsilon$.*

Proof. For $N = 0$, $D_N^* = 1$, so that the result (independent of ε) is true since the constant $c_{k,p,\varepsilon}$ will be much larger than $p^{2(p-1)d_k}$; we assume $N > 0$ in what follows. The existence of $c_{k,p,\varepsilon}$ is equivalent to the fact that, a fortiori:

$$p^{(p-1)(N+2)d_k} \cdot (\sqrt{D_N^*})^{-\varepsilon}$$

is bounded over N , whence $(p-1)(N+2)d_k \log(p) - \varepsilon \cdot \frac{p-1}{2} \sum_{j=1}^N \log(\ell_j) < \infty$. We have, replacing the consecutive primes $\ell_j \neq p$ by the lower bounds:

$$\ell'_j = \frac{1}{2} j \log\left(\frac{\ell_j}{2}\right), \quad j \geq 2, \quad \ell'_1 = 2,$$

(cf. [12, Notes on Chapitre I, x 4.6]), to verify that:

$$X(N) := (p-1)(N+2)d_k \log(p) - \varepsilon \cdot \frac{p-1}{2} \left(-\log(p) + \log_2 + \sum_{j=2}^N \left[\log\left(\frac{1}{2} \cdot j\right) + \log_2\left(\frac{\ell_j}{2}\right) \right] \right) < \infty.$$

We check that $\log(2) + \sum_{j=2}^N \log\left(\frac{1}{2}\right) + \log_2\left(\frac{\ell_j}{2}\right)$ can be neglected subject to adding -1 to the global sum, and we consider, instead:

$$X(N) = (p-1)(N+2)d_k \log(p) - \varepsilon \cdot \frac{p-1}{2} \left(-1 - \log(p) + \sum_{j=2}^N \log(j) \right).$$

We have, for $N \geq 1$, $\log(N!) = N \log(N) - N + \frac{1}{2} \log(N) + O(1)$, giving:

$$X(N) = (p-1)(N+2)d_k \log(p) - \varepsilon \cdot \frac{p-1}{2} \left[N \log(N) - N + \frac{1}{2} \log(N) + O(1) \right],$$

whence:

$$X(N) = -\varepsilon \frac{p-1}{2} N \log(N) + N \left[(p-1)d_k \log(p) - \varepsilon O(1) + o(1) \right].$$

The dominant term (for ε fixed):

$$-\varepsilon \frac{p-1}{2} N \log(N)$$

ensures the existence of a bound $c_{k,p,\varepsilon}$ and completes the proof. \square

Remark 3.4. It is easy to verify that $X(N)$, as function of $N \geq 0$, admits, for an $N_0(\varepsilon) \gg 0$, a maximum, roughly speaking of the form $e^{O(1) \cdot \varepsilon^{-1}}$, giving enormous constants $c_{k,p,\varepsilon}$. This is due in part to the method using certain extreme bounds which are not achieved in practice; for example the use of the systematic upper bounds $d_k = [k : \mathbb{Q}]$ at each step of the tower. It would perhaps be interesting to give heuristics for more reasonable constants.

Finally, we may write in the degree p cyclic extension K/k (Formula (3) and Lemma 3.3 giving $p^{(p-1)(N+2)d_k} \leq c_{k,p,\varepsilon} \cdot (\sqrt{D_N^*})^\varepsilon \leq c_{k,p,\varepsilon} \cdot (\sqrt{D_{K/k}})^\varepsilon$):

$$\begin{aligned} p^{\text{rk}_p(\mathcal{A}_K)} &\leq C_{k,p,\varepsilon}^p \left(\sqrt{D_k^p}\right)^\varepsilon \cdot p^{(p-1)(N+2)d_k} \\ &\leq C_{k,p,\varepsilon}^p \left(\sqrt{D_k^p}\right)^\varepsilon \cdot c_{k,p,\varepsilon} \left(\sqrt{D_{K/k}}\right)^\varepsilon \leq C_{k,p,\varepsilon}^p \cdot c_{k,p,\varepsilon} \left(\sqrt{D_k^p \cdot D_{K/k}}\right)^\varepsilon \\ &\leq C_{K,p,\varepsilon} \cdot \left(\sqrt{D_K}\right)^\varepsilon, \end{aligned}$$

with $C_{K,p,\varepsilon} := C_{k,p,\varepsilon}^p \cdot c_{k,p,\varepsilon}$. The degree $[F : \kappa]$ being fixed, the above induction leads to (denoting $C_{F,p,\varepsilon} := C_{\kappa,p^e,\varepsilon}$):

Theorem 3.5. *Let $p \geq 2$ be prime. The p -rank ε -conjecture for p -cyclic-towers F/κ of given degree p^e , on the existence, for all $\varepsilon > 0$, of a constant $C_{\kappa,p^e,\varepsilon}$ such that $\#(\mathcal{A}_F \otimes \mathbb{F}_p) \leq C_{\kappa,p^e,\varepsilon} \cdot (\sqrt{D_F})^\varepsilon$, is fulfilled unconditionally.*

Remark 3.6. If F/κ , of degree p^e , is inside the p -Hilbert tower of a number field κ , we have $D_F = D_\kappa^{p^e}$, whence $\#(\mathcal{A}_F \otimes \mathbb{F}_p) \leq C_{\kappa,p^e,\varepsilon} \cdot (\sqrt{D_\kappa})^{\varepsilon p^e}$; renormalizing ε since p^e is a constant, this may be written: for all $\varepsilon > 0$, there exists a constant $C'_{\kappa,p^e,\varepsilon}$ such that, for all such unramified p -towers:

$$\#(\mathcal{A}_F \otimes \mathbb{F}_p) \leq C'_{\kappa,p^e,\varepsilon} \cdot (\sqrt{D_\kappa})^\varepsilon;$$

this kind of results (with huge constants) is probably necessary because of some results giving large ranks as the degree grows, as it is done by Hajir–Maire in [8].

4. THE p -RANK ε -CONJECTURE IN p -RAMIFICATION THEORY

More precisely, we shall replace, in the p -cyclic-towers F/κ of given degree p^e , the p -class group \mathcal{A}_F by the pro- p -group \mathcal{A}_F which is the Galois group of the maximal p -ramified abelian pro- p -extension $\mathcal{H}_F^{\text{ab}}$ of F . As we know, this pro- p -group is related to the p -class group \mathcal{A}_F , the normalized p -adic regulator \mathcal{R}_F and its \mathbb{Z}_p -rank depends on Leopoldt’s conjecture (see, e.g., [4, IV, §§1,2,3], [7] and the almost exhaustive bibliography of [5] for the story of abelian p -ramification theory, especially the items [3,16,17,18,19,26,40,50,57,58,59,63,65,67,70,72]).

4.1. Recalls about \mathcal{A}_F . We assume the Leopoldt conjecture for p in all the fields considered. Let \mathcal{G}_F be the Galois group of the maximal pro- p -extension \mathcal{H}_F of F , p -ramified in the ordinary sense (i.e., unramified outside p and non-complexified (= totally split) at the real infinite places of F when $p = 2$). We know that $\mathcal{A}_F = \text{Gal}(\mathcal{H}_F^{\text{ab}}/F)$ is a \mathbb{Z}_p -module of finite type for which $\mathcal{T}_F := \text{tor}_{\mathbb{Z}_p}(\mathcal{A}_F)$ is isomorphic to the dual of the cohomology group $H^2(\mathcal{G}_F, \mathbb{Z}_p)$. Under Leopoldt’s conjecture, we have

$$(4) \quad \mathcal{A}_F \simeq \mathbb{Z}_p^{r_2(F)+1} \oplus \mathcal{T}_F,$$

where $[F : \mathbb{Q}] =: r_1(F) + 2r_2(F)$ and where \mathcal{T}_F fixes the compositum \widetilde{F} of the \mathbb{Z}_p -extensions of F . Let $U_F := \bigoplus_{\mathfrak{p}|p} U_{\mathfrak{p}}$, be the product of the principal local units of the completions $F_{\mathfrak{p}}$ of F , let \overline{E}_F be the closure of the image of E_F in U_F and let $\mathcal{W}_F = \text{tor}_{\mathbb{Z}_p}(U_F)/\mu_p(F)$. Then U_F/\overline{E}_F fixes the p -Hilbert class field H_F and \mathcal{W}_F fixes the Bertrandias–Payan field $\mathcal{H}_F^{\text{bp}}$:

$$\begin{array}{ccccc}
 & & \mathcal{T}_F \simeq \mathrm{H}^2(\mathcal{G}_F, \mathbb{Z}_p)^* & & \\
 & \text{---} & \text{---} & \text{---} & \text{---} \\
 \tilde{F} & \text{---} & \tilde{F}H_F & \xrightarrow[\simeq \mathcal{R}_F]{\mathcal{H}_F^{\mathrm{bp}}} & \mathcal{H}_F^{\mathrm{ab}} \\
 | & & | & & | \\
 \tilde{F} \cap H_F & \text{---} & H_F & \xrightarrow[\simeq \mathcal{A}_F]{\simeq U_F/\overline{E}_F} & \mathcal{H}_F^{\mathrm{ab}} \\
 | & & | & & | \\
 F & & & &
 \end{array}$$

4.2. Fixed point formula. Let K/k be any finite Galois extension of Galois group G ; then from [4, Theorem IV.2.1] the transfer $J : \mathcal{A}_k \rightarrow \mathcal{A}_K$ is always injective under Leopoldt's conjecture. This will be applied to the degree p cyclic sub-extensions of a tower F/κ . Then the analogue of the exact sequence for class groups, used in the proof of Proposition 2.3, is given by the following result:

Theorem 4.1. *We have the exact sequence [4, Proposition IV.3.2.1]:*

$$1 \longrightarrow J(\mathcal{A}_k) \longrightarrow \mathcal{A}_K^G \longrightarrow \bigoplus_{\substack{\mathfrak{l}_k \uparrow p}} \mathbb{Z}_p / e_{\mathfrak{l}_k} \mathbb{Z}_p \longrightarrow 1,$$

where $e_{\mathfrak{l}_k}$ is the ramification index of the tame prime ideals of k ramified in K/k .

Corollary 4.2. *We have $\mathrm{rk}_p(\mathcal{A}_K^G) \leq \mathrm{rk}_p(\mathcal{A}_k) + t'_k$, where t'_k is the number of tame prime ideals of k ramified in K/k .*

4.3. Induction process in a p -cyclic tower F/κ . We consider the framework of the previous sections with degree p cyclic extensions K/k . Let $\mathcal{A}_K^* = \mathrm{Ker}(\nu)$; we get $\mathrm{rk}_p(\mathcal{A}_K) \leq \mathrm{rk}_p(\mathcal{A}_k) + \mathrm{rk}_p(\mathcal{A}_K^*)$. Then considering Proposition 2.1 (valid for the \mathbb{Z}_p -modules of finite type $M = \mathcal{A}_K$ since the M_{h+1}^*/M_h^* are elementary finite p -groups), one obtains from Corollary 4.2 in K/k :

$$\mathrm{rk}_p(\mathcal{A}_K^*) \leq (p-1) \mathrm{rk}_p(\mathcal{A}_K^{G*}) = (p-1) \mathrm{rk}_p(\mathcal{A}_K^G) \leq (p-1) (\mathrm{rk}_p(\mathcal{A}_k) + t'_k),$$

whence $\mathrm{rk}_p(\mathcal{A}_K) \leq p \mathrm{rk}_p(\mathcal{A}_k) + (p-1) t'_k$. Let N be the number of tame prime numbers ℓ_j ramified in K/k ; using the same upper bound $d_k := [k : \mathbb{Q}]$, we obtain:

$$(5) \quad \mathrm{rk}_p(\mathcal{A}_K) \leq p \mathrm{rk}_p(\mathcal{A}_k) + (p-1) N d_k.$$

Assume for instance that the real infinite places of k split in K/k (which is the case for $p \neq 2$), we get easily from relations (4) and (5):

$$\mathrm{rk}_p(\mathcal{T}_K) \leq p \mathrm{rk}_p(\mathcal{T}_k) + (p-1) (1 + N d_k).$$

Seeing that, whatever p and F/κ , the inequalities are similar to that obtained for the p -ranks of usual class groups, we can state about the Galois cohomology groups $\mathrm{H}^2(\mathcal{G}_F, \mathbb{Z}_p)$, since $\mathrm{rk}_p(\mathrm{H}^2(\mathcal{G}_F, \mathbb{Z}_p)) = \mathrm{rk}_p(\mathcal{T}_F)$:

Theorem 4.3. *Let $p \geq 2$ be prime. The p -rank ε -conjecture for p -cyclic-towers F/κ of given degree p^e , on the existence, for all $\varepsilon > 0$, of a constant $C'_{\kappa, p^e, \varepsilon}$ such that $\#(\mathrm{H}^2(\mathcal{G}_F, \mathbb{Z}_p) \otimes \mathbb{F}_p) \leq C'_{\kappa, p^e, \varepsilon} \cdot (\sqrt{D_F})^\varepsilon$, is fulfilled unconditionally.*

REFERENCES

- [1] G. Cornell, Relative genus theory and the class group of ℓ -extensions, *Trans. Amer. Math. Soc.*, **277**(1) (1983), 421–429. <https://doi.org/10.1090/S0002-9947-1983-0690061-1>
- [2] J.S. Ellenberg, A. Venkatesh, Reflection principles and bounds for class group torsion, *Int. Math. Res. Not.* **2007**(1) (2007). <https://doi.org/10.1093/imrn/rnm002>
- [3] G. Gras, Genus theory and ε -conjectures on p -class groups, *Jour. Number Theory* **207** (2020), 423–459. <https://doi.org/10.1016/j.jnt.2019.07.008>
- [4] G. Gras, *Class Field Theory: from theory to practice*, corr. 2nd ed., Springer Monographs in Mathematics, Springer (2005), xiii+507 pages. <https://doi.org/10.1007/978-3-662-11323-3>
- [5] 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://dergipark.org.tr/en/download/article-file/906434>
- [6] G. Gras, Invariant generalized ideal classes–Structure theorems for p -class groups in p -extensions, *Proc. Indian Acad. Sci. (Math. Sci.)*, **127**(1) (2017), 1–34. <https://www.ias.ac.in/article/fulltext/pmsc/127/01/0001-0034>
- [7] G. Gras, The p -adic Kummer-Leopoldt Constant: Normalized p -adic Regulator, *Int. J. Number Theory*, **14**(2) (2018), 329–337. <https://doi.org/10.1142/S1793042118500203>
- [8] F. Hajir, C. Maire, On the invariant factors of class groups in towers of number fields, *Canadian Journal of Mathematics* **70**(1) (2018), 142–172. <https://doi.org/10.4153/CJM-2017-032-9>
- [9] P. Koymans, C. Pagano, On the distribution of $\mathcal{C}(K)[\ell^\infty]$ for degree ℓ cyclic fields, preprint (2018) <https://arxiv.org/pdf/1812.06884>
- [10] J. Klüners, J. Wang, ℓ -torsion bounds of the class group for number fields with an ℓ -group as Galois group (July 9, 2019), personal communication.
- [11] J-P. Serre, *Corps Locaux*, *Actualités Scientifiques et Industrielles* **1296**, Hermann, quatrième édition revue et corrigée 2004.
- [12] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 4^e édition, Coll. Échelles, Belin 2015, 592 pages.
- [13] J. Wang, Pointwise Bounds for ℓ -torsion in Class groups: Elementary Abelian Extensions. <https://arxiv.org/abs/2001.03077>

VILLA LA GARDETTE, 4 CHEMIN CHÂTEAU GAGNIÈRE, F-38520 LE BOURG D'OISANS
E-mail address: g.mn.gras@wanadoo.fr