



HAL
open science

Genus theory and ϵ -conjectures on p-class groups

Georges Gras

► **To cite this version:**

| Georges Gras. Genus theory and ϵ -conjectures on p-class groups. 2019. hal-02059441v1

HAL Id: hal-02059441

<https://hal.science/hal-02059441v1>

Preprint submitted on 6 Mar 2019 (v1), last revised 25 Jun 2019 (v3)

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.

Genus theory and ε -conjectures on p -class groups

Georges Gras

ABSTRACT. We suspect that the “genus part” of the class number of a number field K is an obstruction for an “easy proof” of a “strong ε -conjecture” for p -class groups: $\#(\mathcal{C}_K \otimes \mathbb{Z}_p) \ll_{d,p,\varepsilon} (\sqrt{D_K})^\varepsilon$ for all K totally real of degree d . We analyse the weight of genus theory in this inequality by means of an infinite family of p -cyclic fields with many ramified primes, then prove the usual p -rank form of the ε -conjecture: $\#(\mathcal{C}_K \otimes \mathbb{F}_p) \ll_{d,p,\varepsilon} (\sqrt{D_K})^\varepsilon$, for $d = p$ and the family of p -cyclic extensions of \mathbb{Q} (Theorem 2.4) then sketch the case of arbitrary base fields. The possible obstruction, for the strong form, is the order of magnitude of the set of “exceptional” p -classes given by a well-known unpredictable algorithm. Then we compare the ε -conjectures with some p -adic conjectures, of Brauer–Siegel type, about the torsion group \mathcal{T}_K of the Galois group of the maximal abelian p -ramified pro- p -extension of totally real number fields K . We give numerical computations with the corresponding PARI/GP programs.

CONTENTS

1. Introduction	2
2. A possible obstruction due to genus theory	3
2.1. Definition of the family $(F_{N,p})_{N \geq 1}$	3
2.2. About the exceptional p -classes	4
2.2.1. The algorithm	4
2.2.2. Exceptional examples	5
2.3. Estimation of $C_{p,p,\varepsilon}$ for the fields $F_{N,p}$	7
2.4. A lower bound for $C_{p,p,\varepsilon}$	9
3. PARI/GP programs computing $\mathcal{C}_{F_{N,p}}$	10
3.1. The p -structure of some $\mathcal{C}_{F_{N,p}}$	10
3.2. Examples of exceptional p -classes	11
4. Genus theory – Abelian p -ramification theory	14
4.1. Reminders on Genus theory	14

Date: March 6, 2019.

2010 Mathematics Subject Classification. 11R29, 11R37, 08-04.

Key words and phrases. class groups; ε -conjecture; class field theory; p -ramification; genus theory.

4.1.1.	Genus field and genus number $g_{K/k}$	14
4.1.2.	Non-genus ε -conjecture	15
4.2.	Reminders on p -ramification theory	16
4.2.1.	Structure of the p -torsion group \mathcal{T}_K	16
4.2.2.	The p -adic Brauer–Siegel conjecture for \mathcal{T}_K	18
4.2.3.	Estimation of $\mathcal{C}_{F_{N,p,p}}$	18
4.3.	p -adic Brauer–Siegel conjecture versus ε -conjectures	21
4.3.1.	Analysis by means of CM-fields	22
4.3.2.	Computation of $\mathcal{C}_{K,p}$ (imaginary quadratic fields)	22
4.3.3.	Conclusion	25
4.4.	Reflection theorem and p -rank ε -conjectures	25
	References	26

1. Introduction

For any number field K , we denote by \mathcal{C}_K the class group of K in the restricted sense and by $\mathcal{C}_K \otimes \mathbb{Z}_p$ its p -class group, for any prime number p ; to avoid any ambiguity, we shall write $\mathcal{C}_K \otimes \mathbb{F}_p$ for the “ p -torsion group”, often denoted $\mathcal{C}_K[p]$ in most papers, only giving the p -rank $\text{rk}_p(\mathcal{C}_K)$ of \mathcal{C}_K . One knows the following classical result (weak form of theorems of Brauer, Brauer–Siegel, Tsfasman–Vladuț–Zykin [34, 37]):

For all $\varepsilon > 0$ there exists a constant $C_{d,\varepsilon}$ such that $\#\mathcal{C}_K \leq C_{d,\varepsilon} \cdot (\sqrt{D_K})^{1+\varepsilon}$, where d is the degree of K and D_K the absolute value of its discriminant.

But it is clear that, arithmetically, the behaviour of the p -Sylow subgroups of \mathcal{C}_K depends, in conflicting manners (regarding p), on many parameters (signature, ramification, prime divisors of d , action of Galois group, etc.).

After the Cohen–Lenstra–Martinet–Adam–Malle heuristics or conjectures on the order and structure of $\mathcal{C}_K \otimes \mathbb{Z}_p$ [3, 4, 1, 24], many authors study and prove inequalities of the form $\#(\mathcal{C}_K \otimes \mathbb{F}_p) \leq C_{d,p,\varepsilon} \cdot (\sqrt{D_K})^{c+\varepsilon}$, with positive constant $c < 1$ as small as possible (e.g., under GRH, the inequality $\#(\mathcal{C}_K \otimes \mathbb{F}_p) \leq C_{d,p,\varepsilon} \cdot (\sqrt{D_K})^{1-\frac{1}{p(d-1)}+\varepsilon}$ [6, Proposition 1]; see also [10, § 1.1], [27, § 1.1] for more examples and comments). The links between this ε -conjecture and the above heuristics are studied in [27, § 1.1, Theorem 1.2].

For a general history upon today about such inequalities, we refer to some recent papers of the bibliography (e.g., [5, 6, 10, 27, 36] in which the reader can have a more complete list of recent contributions).

For short, we shall call “ p -rank ε -conjecture” the case:

$$\#(\mathcal{C}_K \otimes \mathbb{F}_p) \leq C_{d,p,\varepsilon} \cdot (\sqrt{D_K})^\varepsilon,$$

and “strong ε -conjecture” the case:

$$\#(\mathcal{C}_K \otimes \mathbb{Z}_p) \leq C_{d,p,\varepsilon} \cdot (\sqrt{D_K})^\varepsilon.$$

These kind of results do not separate the case of totally real fields, for which we know that the class number is rather small, regarding the case of non totally real fields (see papers by Schoof as [30, 32] and Washington's book [35], among many contributions). Moreover, by nature, they deal with upper bounds of the p -rank $\text{rk}_p(\mathcal{C}_K)$ of \mathcal{C}_K and precisely we shall see that genus theory gives, when it applies, large p -ranks and possibly much large orders, which probably makes harder classical proofs by complex analytic way.

Remark 1.1. Nevertheless many arguments and computations are in favour of the strong ε -conjecture $\#(\mathcal{C}_K \otimes \mathbb{Z}_p) \leq C_{d,p,\varepsilon} \cdot (\sqrt{D_K})^\varepsilon$, for totally real number fields, even if such a conjecture is “a conjecture at infinity” because, as we shall see in numerical calculations, the constants $C_{d,p,\varepsilon}$ are enormous, so that for “usual fields” with small discriminants, the inequalities are trivial up to some huge bound of this discriminant. So it will be difficult to give convincing computations “at infinity”.

In this context, we shall only prove the case of the p -rank ε -conjecture for p -cyclic fields (Theorem 2.4). The case $d = p = 2$ is known from Gauss genera theory, but its generalization is not obvious since for $p = 2$ the p -rank is canonical (given by Chevalley's formula (1)) while for $p > 2$ it depends on the unpredictable algorithm which determines the complete structure of \mathcal{C}_K ; indeed, for $d = p = 2$ and any class γ such that $\gamma^2 = 1$, we can write, with obvious notations, $\gamma^{\sigma-1} = \gamma^{\sigma+1-2} = \mathbb{N}_{K/\mathbb{Q}}(\gamma) \gamma^{-2} = 1$, which does not work for $d = p > 2$. To our knowledge, for $d = p > 2$, only the case of cyclic cubic fields is proved [6, Corollary 1, case (3)] for the 3-rank ε -conjecture.

The question, for p -class groups $\mathcal{C}_K \otimes \mathbb{Z}_p$ of imaginary fields, is very different and we shall try to put it in “duality” with the torsion group \mathcal{T}_K of the Galois group of the maximal abelian p -ramified pro- p -extension of K for which, on the contrary, we shall prove that there is no strong ε -conjecture for \mathcal{T}_K in the case of totally real fields.

2. A possible obstruction due to genus theory

We shall illustrate the above comments with a family of fields with optimal p -ranks, and give numerical illustrations with PARI/GP [26] programs.

2.1. Definition of the family $(F_{N,p})_{N \geq 1}$. We consider a fixed prime $p \geq 2$ and the sequence of all prime numbers ℓ_k , totally split in $\mathbb{Q}(\mu_p)$, whence such that $\ell_k \equiv 1 \pmod{p}$. For $p > 2$, let $F_{N,p}$ be any cyclic extension of degree p , of global conductor $f_{N,p} = \prod_{k=1}^N \ell_k$, for any $N \geq 1$. For $p = 2$ we shall consider $F_{N,2} := \mathbb{Q}(\sqrt{\pm \ell_1 \cdots \ell_N}) = \mathbb{Q}(\sqrt{\pm 3 \cdot 5 \cdots \ell_N})$ with \pm such that 2 be unramified, and consider the restricted sense for class groups, which is more canonical for our purpose.¹ We may consider p -cyclic extensions ramified at p without any modification of the forthcoming reasonings (since

¹In fact, only the real quadratic fields $F_{N,2}$ shall be considered, but the imaginary ones may give interesting comparisons.

this modifies conductors up to the constant factor p^2 , 4 or 8), except an useless complexity of redaction.

The discriminant $D_{N,p}$ of $F_{N,p}$ is the product of the conductors associated to each nontrivial character of $G_{N,p} := \text{Gal}(F_{N,p}/\mathbb{Q})$, thus $D_{N,p} = f_{N,p}^{p-1}$. There are $(p-1)^{N-1}$ such fields, all contained in $\mathbb{Q}(\mu_{\ell_1 \dots \ell_N})$.

The Chevalley formula [2] gives the number of ambiguous classes (i.e., invariant by $G_{N,p}$) which is equal to the genus number for cyclic fields:

$$(1) \quad \#(\mathcal{C}_{F_{N,p}} \otimes \mathbb{Z}_p)^{G_{N,p}} = p^{N-1}.$$

It is obvious that the group of ambiguous classes is p -elementary of p -rank $N-1 \leq \text{rk}_p(\mathcal{C}_{F_{N,p}})$ and generated by the ramified primes $\mathfrak{l}_i \mid \ell_i$, $1 \leq i \leq N$, with a (non-trivial and non-canonical) relation $\prod_{i=1}^N \mathfrak{l}_i^{n_i} = (a)$, $a \in F_{N,p}^\times$, due to the classical Kummer theory over $\mathbb{Q}(\mu_p)$ giving $F_{N,p}(\mu_p) = \mathbb{Q}(\mu_p)(\sqrt[p]{\alpha})$, $\alpha \in \mathbb{Q}(\mu_p)^\times$ depending of canonical Gauss sums.

2.2. About the exceptional p -classes. We know that $\#(\mathcal{C}_{F_{N,p}} \otimes \mathbb{F}_p)$ and $\#(\mathcal{C}_{F_{N,p}} \otimes \mathbb{Z}_p)$, both depend of an unpredictable algorithm that we recall below; this shows that the so-called Brumer–Silverman–Duke–Zhang–Ellenberg–Venkatesh ε -conjecture on the p -ranks is not so different from the strong ε -conjecture, in a logical point of view, except that we shall see that the p -rank is an $O_p(N)$ contrary to $\#(\mathcal{C}_{F_{N,p}} \otimes \mathbb{Z}_p)$ whose order of magnitude is unknown.

Definition 2.1. Let $\delta(N) \geq 0$ be such that $\#(\mathcal{C}_{F_{N,p}} \otimes \mathbb{F}_p) = p^{N-1+\delta(N)}$ and let $\Delta(N) \geq \delta(N)$ be such that $\#(\mathcal{C}_{F_{N,p}} \otimes \mathbb{Z}_p) = p^{N-1+\Delta(N)}$.

In other words, $p^{\Delta(N)}$ measures what we call the “exceptional p -classes” (i.e., non-invariant) obtained via the classical filtration of $\mathcal{C}_{F_{N,p}} \otimes \mathbb{Z}_p$ (a general theoretical and numerical approach was given in [14, 15], after the historical papers of Inaba [20], Redei–Reichardt [29], and many others; for a complete survey, see [13]). Then $N-1+\delta(N)$ is the p -rank.

2.2.1. The algorithm. Recall briefly the computation of $\delta(N)$ and $\Delta(N)$ in the purpose of some probabilistic considerations.

Let F be any p -cyclic extension of \mathbb{Q} with $N \geq 1$ ramified primes, put $M := \mathcal{C}_F \otimes \mathbb{Z}_p$, and let σ be a generator of $G := \text{Gal}(F/\mathbb{Q}) \simeq \mathbb{Z}/p\mathbb{Z}$.

Let I_F be the group of ideals of F , prime to p , and let $M_i := \mathcal{C}_F(\mathcal{I}_i)$, $i \geq 0$, $\mathcal{I}_i \subset I_F$, defined inductively by $M_0 := 1$, and:

$$M_{i+1}/M_i := (M/M_i)^G, \text{ for } 0 \leq i \leq m-1,$$

where $m \geq 1$ is the least integer i such that $M_i = M$ (i.e., such that $M_{i+1} = M_i$). Then $M_i = \{c \in M, c^{(1-\sigma)^i} = 1\}$ for all $i \geq 0$ and $M_1 = M^G$.

The sequence $\#(M_{i+1}/M_i)$, $0 \leq i \leq m$, decreases to 1 and is bounded by $\#M_1$ due to the injective maps $M_{i+1}/M_i \hookrightarrow M_i/M_{i-1} \hookrightarrow \dots \hookrightarrow M_2/M_1 \hookrightarrow M_1$ defined by the operation of $1-\sigma$.

We have, for p -cyclic fields F , the formulas [13, Corollary 3.7], for all $i \geq 0$:

$$\#(M_{i+1}/M_i) = \frac{p^{N-1}}{(\Lambda_i : \Lambda_i \cap N_{F/\mathbb{Q}}(F^\times))} \ \& \ \Lambda_i := \{x \in \mathbb{Q}^\times, (x) \in N_{F/\mathbb{Q}}(\mathcal{I}_i)\}.$$

The progression of the algorithm depends on the $x \in \Lambda_i$, $(x) = N_{F/\mathbb{Q}}(\mathfrak{A})$, $\mathfrak{A} \in \mathcal{I}_i$, such that $x = N_{F/\mathbb{Q}}(y)$, $y \in F^\times$, giving the equation:

$$(y) = \mathfrak{A} \cdot \mathfrak{B}^{1-\sigma},$$

in which the solutions \mathfrak{B} (unpredictable) become new elements to be added to \mathcal{I}_i to built $\mathcal{I}_{i+1} \supseteq \mathcal{I}_i$, then $\Lambda_{i+1} \supseteq \Lambda_i$, and so on.

Put, for all $i \geq 0$, $\#(M_{i+1}/M_i) := p^{N-1-t_i^N}$, $t_i^N \geq 0$, where $p^{t_i^N} \mid p^{N-1}$ is the index $(\Lambda_i : \Lambda_i \cap N_{F/\mathbb{Q}}(F^\times))$ (since $x \in \Lambda_i$ is norm of an ideal, it is locally a norm everywhere, except perhaps at the N ramified primes, but the product formula for Hasse's normic symbols gives the above divisibility). We have:

$$t_0^N = 0 \leq t_1^N \leq \dots \leq t_m^N = N - 1.$$

Then $\#M = \#(\mathcal{C}_F \otimes \mathbb{Z}_p) = \prod_{i \geq 0} \#(M_{i+1}/M_i) = p^{m(N-1) - \sum_{i=1}^m t_i^N}$.

We have the following result that we shall use to test the ε -conjecture.

Lemma 2.2 ([13, Lemma 4.2]). *Let F/\mathbb{Q} be a p -cyclic extension with $N \geq 1$ ramified primes. Then $\text{rk}_p(\mathcal{C}_F) = (p-1) \cdot (N-1) - \sum_{i=1}^{p-2} t_i^N$. Whence this yields $\delta(N) = (p-2) \cdot (N-1) - \sum_{i=1}^{p-2} t_i^N$.*

We see that the p -rank may vary in the interval $[N-1, (p-1)(N-1)]$ and is always $O_p(N)$ as $N \rightarrow \infty$ which shall be of a great importance; the p -rank is equal to $N-1$, for all F/\mathbb{Q} of degree p , if and only if $p=2$ as we have seen. In the same manner, the p^r -ranks are given by the expressions:

$$\sum_{i=(r-1)(p-1)}^{r(p-1)-1} (N-1-t_i^N) = (p-1) \cdot (N-1) - \sum_{i=(r-1)(p-1)}^{r(p-1)-1} t_i^N.$$

It is clear that the normic indices depend on the \mathbb{F}_p -ranks of $N \times N$ -matrices of suitable Hilbert symbols [15, Ch. VI, §2] generalizing, for instance, Rédei's matrices for the computation of the 4-ranks of a quadratic field.

But we emphasize the fact that if some heuristics on the \mathbb{F}_p -rank of these matrices are natural, *the number of steps of the algorithm* (i.e., m) is not clear, and it is not known in what manner $\Delta(N)$ may be bounded.

2.2.2. Exceptional examples. In fact, for $p > 2$, the maximal rank, equal to $(p-1) \cdot (N-1)$, is very rare. We remembered that in our thesis [15, p. 39], we gave the first example of cyclic cubic field, for which $\text{rk}_3(\mathcal{C}) = 2(N-1)$; this example has conductor $f = 9 \cdot 577 \cdot 757 \cdot 991$ and gives (using the program below showing moreover that the property is fulfilled for the eight fields of conductor f):

```

f=3895721091 N=4 P=x^3-1298573697*x+18010351461592 C1=[9,3,3,3,3,3]
f=3895721091 N=4 P=x^3-1298573697*x-16034355152657 C1=[3,3,3,3,3,3]
f=3895721091 N=4 P=x^3-1298573697*x+15707980296811 C1=[3,3,3,3,3,3]
f=3895721091 N=4 P=x^3-1298573697*x-10132337699792 C1=[3,3,3,3,3,3]
f=3895721091 N=4 P=x^3-1298573697*x-8835062576489 C1=[3,3,3,3,3,3]
f=3895721091 N=4 P=x^3-1298573697*x-7829966535011 C1=[9,3,3,3,3,3]
f=3895721091 N=4 P=x^3-1298573697*x+912031593193 C1=[3,3,3,3,3,3]
f=3895721091 N=4 P=x^3-1298573697*x-221623244288 C1=[9,3,3,3,3,3]

```

We publish for any further example the following program computing all the cubic fields such that there are exceptional classes; so in most cases the 3-rang is N (instead of $N - 1$) and many examples have a non-trivial 9-rank.

```

{p=3;bf=7;Bf=10^6;for(f=bf,Bf,e=valuation(f,3);if(e!=0 & e!=2,next);F=f/3^e;
if(Mod(F,3)!=1||core(F)!=F,next);F=factor(F);Div=component(F,1);
d=component(matsize(F),1);for(j=1,d-1,D=component(Div,j);
if(Mod(D,3)!=1,break));for(b=1,sqrt(4*f/27),if(e==2 & Mod(b,3)==0,next);
A=4*f-27*b^2;if(issquare(A,&a)==1,if(e==0,if(Mod(a,3)==1,a=-a);
P=x^3+x^2+(1-f)/3*x+(f*(a-3)+1)/27);if(e==2,if(Mod(a,9)==3,a=-a);
P=x^3-f/3*x-f*a/27);N=bigomega(f);if(e==2,N=N-1);L=List;
K=bnfinit(P,1);C8=component(K,8);h=component(component(C8,1),1);
C1=component(component(C8,1),2);dim=component(matsize(C1),2);
rho=0;for(i=1,dim,z=component(C1,i);v=valuation(z,3);if(v>=1,rho=rho+1;
listput(L,3^v));if(rho>=N,print(" f=",f," N=",N," P=",P," C1=",L))))}

```

```

f=657 N=2 P=x^3-219*x-1241 C1=[3,3]
f=657 N=2 P=x^3-219*x+730 C1=[3,3]
(...)
f=3913 N=3 P=x^3+x^2-1304*x+17681 C1=[3,3,3]
f=3913 N=3 P=x^3+x^2-1304*x-17536 C1=[3,3,3]
(...)
f=4711 N=2 P=x^3+x^2-1570*x+19193 C1=[9,3]
f=4711 N=2 P=x^3+x^2-1570*x-13784 C1=[9,3]
f=4921 N=3 P=x^3+x^2-1640*x+23876 C1=[3,3,3]
f=4921 N=3 P=x^3+x^2-1640*x-729 C1=[3,3,3]
(...)
f=5383 N=2 P=x^3+x^2-1794*x+17744 C1=[9,3]
f=5383 N=2 P=x^3+x^2-1794*x-9171 C1=[9,3]
(..)
f=15561 N=4 P=x^3-5187*x+141778 C1=[9,3,3,3]

```

Remarks 2.3. (i) As we have explained, we do not consider p -cyclic extensions F/\mathbb{Q} ramified at p . This shall modify the forthcoming computations by some $O(1)$ without any consequence on the statements.

(ii) The Galois action of $G = \text{Gal}(F/\mathbb{Q}) \simeq \mathbb{Z}/p\mathbb{Z}$ on the non- p -part of the class group gives rise, for all prime $q \mid \#\mathcal{C}_F$, to:

$$\mathcal{C}_F \otimes \mathbb{Z}_q \simeq \mathbb{Z}[\mu_p] / \prod_{q \mid p} \mathfrak{q}^{n_q}, \quad n_q \geq 0,$$

whose \mathbb{F}_q -dimension is a multiple of the residue degree of q in $\mathbb{Q}(\mu_p)/\mathbb{Q}$, which explains the rarity of such divisibilities for large residue degrees.

2.3. Estimation of $C_{p,p,\varepsilon}$ for the fields $F_{N,p}$. We need a lower bound of the k th prime number $\ell_k \equiv 1 \pmod{p}$ to get an estimation of $f_{N,p}$.

We thank G erald Tenenbaum for valuable indications for the good formula, from [33, Notes on   4.6], due to a result of Montgomery–Vaughan giving:

$$(2) \quad \ell_k > (p-1) \cdot \frac{k}{2} \cdot \log\left(\frac{k}{2}\right), \text{ for all } k \geq 6,$$

for the k th prime number $\ell_k \equiv 1 \pmod{p}$. For $1 \leq k \leq 5$ we can take $\ell_k > p$ in general formulas.

We intend to test, for the family $(F_{N,p})_{N \geq 1}$ of discriminants $D_{N,p} := D_{F_{N,p}}$, the strong ε -conjecture, that is to say:

$$(3) \quad \#(\mathcal{C}_{F_{N,p}} \otimes \mathbb{Z}_p) =: p^{N-1+\Delta(N)} \leq C_{p,p,\varepsilon} \cdot (\sqrt{D_{N,p}})^\varepsilon,$$

where $\Delta(N) = (m-1) \cdot (N-1) - \sum_{i=1}^{m-1} t_i^N \geq 0$, related to the set of exceptional classes, has only a probabilistic value depending on m and the t_i^N .

It will be easy, from the forthcoming calculations, to test the p -rank ε -conjecture, $\#(\mathcal{C}_{F_{N,p}} \otimes \mathbb{F}_p) \leq C_{p,p,\varepsilon} \cdot (\sqrt{D_{N,p}})^\varepsilon$, but considering the weaker inequality:

$$p^{N-1+\delta(N)} = p^{(p-1)(N-1) - \sum_{i=1}^{p-2} t_i^N} \leq C_{p,p,\varepsilon} \cdot (\sqrt{D_{N,p}})^\varepsilon,$$

even in the less favorable case $t_i^N = 0$, for $1 \leq i \leq p-2$ and replacing for all N , $D_{N,p}$ by a lower bound $D'_{N,p}$ (in other words the existence of an inequality $p^{(p-1)(N-1)} \leq C'_{p,p,\varepsilon} \cdot (\sqrt{D'_{N,p}})^\varepsilon$ proves the p -rank ε -conjecture).

We fix p and put $D_{N,p} =: D_N$. The strong form is equivalent to prove that $\frac{p^{N-1+\Delta(N)}}{(\sqrt{D_N})^\varepsilon}$ is bounded as $N \rightarrow \infty$, whence:

$$(N-1+\Delta(N)) \log(p) - \varepsilon \cdot \frac{p-1}{2} \sum_{k=1}^N \log(\ell_k) < \infty, \text{ as } N \rightarrow \infty.$$

We then have, replacing ℓ_k by a lower bound, to compute, using (1), (2), (3), the following quantity:

$$\begin{aligned} X(N) &:= (N-1+\Delta(N)) \log(p) - \varepsilon \cdot \frac{p-1}{2} \left[5 \log(p) + \sum_{k=6}^N \log(\ell_k) \right] \\ &= (N-1+\Delta(N)) \log(p) \\ &\quad - \varepsilon \cdot \frac{p-1}{2} \left[5 \log(p) + \sum_{k=6}^N \left[\log\left(\frac{p-1}{2}\right) + \log(k) + \log_2\left(\frac{k}{2}\right) \right] \right] \end{aligned}$$

Since $\sum_{k=6}^N \log_2\left(\frac{k}{2}\right) > 0$ we shall neglect this sum and consider, instead:

$$\begin{aligned} X(N) &= (N-1+\Delta(N)) \log(p) \\ &\quad - \varepsilon \cdot \frac{p-1}{2} \left[5 \log(p) - 5 \log\left(\frac{p-1}{2}\right) - \log(120) + \sum_{k=1}^N \left[\log\left(\frac{p-1}{2}\right) + \log(k) \right] \right] \\ &= (N-1+\Delta(N)) \log(p) - \varepsilon \cdot \frac{p-1}{2} \cdot \left[\eta_p + N \cdot \log\left(\frac{p-1}{2}\right) + \log(N!) \right] \end{aligned}$$

where $\eta_p := 5 \log(p) - 5 \log(\frac{p-1}{2}) - \log(120) = O_p(1) > 0$.

The expression of $N!$ leads to $\log(N!) = N \log(N) - N + \frac{1}{2} \log(N) + O_N(1)$, whence:

$$X(N) = (N - 1 + \Delta(N)) \log(p) - \varepsilon \cdot \frac{p-1}{2} [N \log(N) + N \cdot \gamma_p + \frac{1}{2} \log(N) + O_{N,p}(1)],$$

with $\gamma_p = \log(\frac{p-1}{2}) - 1$. Now we write $X(N)$ under the form:

$$\begin{aligned} X(N) &= N \log(p) + \Delta(N) \log(p) - \varepsilon \cdot \frac{p-1}{2} N \log(N) \\ &\quad - \log(p) - \varepsilon \cdot \frac{p-1}{2} N \cdot \gamma_p - \varepsilon \cdot \frac{p-1}{4} \log(N) - \varepsilon \cdot O_{N,p}(1) \\ &= N \cdot \left[-\varepsilon \cdot \frac{p-1}{2} \log(N) + \frac{\Delta(N)}{N} \log(p) \right. \\ (4) \quad &\quad \left. + \log(p) - \frac{\log(p)}{N} - \varepsilon \cdot O_{N,p}(1) \right] \\ &= N \cdot \left[-\varepsilon \cdot \frac{p-1}{2} \log(N) + \frac{\Delta(N)}{N} \log(p) \right. \\ &\quad \left. + (1 - N^{-1}) \log(p) - \varepsilon \cdot O_{N,p}(1) \right]. \end{aligned}$$

Replacing $\Delta(N)$ by the maximal p -rank $(p-2)(N-1)$, the dominant term $-\varepsilon \cdot \frac{p-1}{2} \log(N)$ ensures the existence of a positive constant C_ε since $\frac{(p-1)(N-1)}{N} \log(p) = O_p(1)$. It is easy to verify that $X(N)$, as function of N , admits, for an $N_0 \gg 0$, a computable maximum, only depending on p and ε (e.g., for $p = 7$, $\varepsilon = 0.1$, $N_0 \approx 2935394 \cdot 10^{10}$, $X(N_0) \approx 88 \cdot 10^{14}$).

This proves the p -rank ε -conjecture for the family $(F_N)_{N \geq 1}$, even assuming always a maximal p -rank $(p-1)(N-1)$. Whence we can state:

Theorem 2.4. *Let $p \geq 2$ be a given prime number. For any cyclic extension F/\mathbb{Q} of degree p , let $\Delta(N) \geq 0$ defined by $\#(\mathcal{C}_F \otimes \mathbb{Z}_p) = p^{N-1+\Delta(N)}$ where N is the number of ramified primes.*

(i) *The p -rank ε -conjecture on the existence, for all $\varepsilon > 0$, of a constant $C_{d,p,\varepsilon}$ such that $\#(\mathcal{C}_K \otimes \mathbb{F}_p) \leq C_{d,p,\varepsilon} \cdot (\sqrt{D_K})^\varepsilon$ for all K , is true for the subfamily of all cyclic extension F/\mathbb{Q} of degree $d = p$.*

(ii) *The corresponding strong ε -conjecture, $\#(\mathcal{C}_K \otimes \mathbb{Z}_p) \leq C_{d,p,\varepsilon} \cdot (\sqrt{D_K})^\varepsilon$, is true for the extensions F/\mathbb{Q} under the condition that $\Delta(N)$ be of a much less order than $N \log(N)$ for $N \rightarrow \infty$.*

Proof. Consider arbitrary prime numbers $\ell_{n_i} \equiv 1 \pmod{p}$, $1 \leq i \leq N$, and a field K of conductor $\prod_{i=1}^N \ell_{n_i}$. Thus $D_K \geq D_{F_N}$, but the maximal p -rank of \mathcal{C}_K is still $(p-1)(N-1)$. We have seen that if we put $\delta(N) = (p-2)(N-1)$ in (4), the main term ensures the existence of the constant $C_{p,p,\varepsilon}$. We omit the details when p^2 (or 4 or 8) divides the conductor. \square

If the strong ε -conjecture is true for such families, it implies some limitation of the order of magnitude of the filtration computing $\Delta(N)$, which may be interesting for other problems and conjectures for totally real number fields.

Very probably, $\Delta(N)$ is of order much less than $N \log(N)$ for $N \rightarrow \infty$ since p^r -ranks are in practice very rare for $r \geq 2$ as well as a maximal p -rank equal to $(p-1)(N-1)$ (see § 2.2.2); but the dominant term in (4) being $\Delta(N) \log(p) - \varepsilon \cdot \frac{p-1}{2} N \log(N)$, this may give some trouble for the proof of an universal strong ε -conjecture assuming for instance $\Delta(N) = O(1) \log(N)$ for infinitely many N .

2.4. A lower bound for $C_{p,p,\varepsilon}$. This part is not essential for our purpose, but it will show that a lower bound of $C_{p,p,\varepsilon}$ is of the same order of magnitude as for the upper bound given by (4). We shall use the following property which may be justified from results given in [25]. For all $k \geq 1$, the k th prime $\ell_k \equiv 1 \pmod{p}$ fulfills, for some constants c_p only depending on p , the inequality $\ell_k < c_p ((p-1)k) \cdot \log((p-1)k) < c_p ((p-1)k)^2$. Then:

$$\begin{aligned} (N-1 + \Delta(N)) \log(p) &\leq \log(C_\varepsilon) + \varepsilon \frac{p-1}{2} \sum_{k=1}^N \log(\ell_k) \\ &\leq \log(C_\varepsilon) + \varepsilon \frac{p-1}{2} \sum_{k=1}^N [\log(c_p) + 2 \log(p-1) + 2 \log(k)], \\ &\leq \log(C_\varepsilon) + \varepsilon \frac{p-1}{2} \cdot [N \gamma'_p + 2 \log(N!)] \end{aligned}$$

where $\gamma'_p := \log(c_p) + 2 \log(p-1) > 0$. Whence, from the value of $\log(N!)$:

$$(N-1 + \Delta(N)) \log(p) \leq \log(C_\varepsilon) + \varepsilon \frac{p-1}{2} [2N \log(N) + N \gamma''_p + \log(N) + O_N(1)],$$

with $\gamma''_p = \gamma'_p - 2 > 0$. Thus:

$$\begin{aligned} \log(C_\varepsilon) &\geq (N-1 + \Delta(N)) \log(p) - \varepsilon (p-1) N \log(N) \\ &\quad - \varepsilon \frac{p-1}{2} N \gamma''_p - \varepsilon \frac{p-1}{2} \log(N) - \varepsilon O_{N,p}(1) \\ &\geq N \cdot \left[-\varepsilon (p-1) \log(N) + \frac{\Delta(N)}{N} \log(p) + O_{N,p}(1) \right]; \end{aligned}$$

thus, for N_0 , this yields an interval containing $\log(C_\varepsilon)$.

Remarks 2.5. (i) As soon as, in $(\sqrt{D_K})^\varepsilon$, we replace ε by $c + \varepsilon$, $0 < c < 1$, as it is done in much papers giving proofs for $\#(\mathcal{C}_K \otimes \mathbb{F}_p) \leq C_{d,p,c,\varepsilon} \cdot (\sqrt{D_K})^{c+\varepsilon}$, the above computations, with that of $X(N)$ in (4), becomes, for the family of fields $F_{N,p}$:

$$\begin{aligned} \log(C_{p,p,c,\varepsilon}) &\leq N \cdot \left[-(c + \varepsilon) \cdot \frac{p-1}{2} \log(N) + \frac{\Delta(N)}{N} \log(p) + O_{N,p}(1) \right] \\ \log(C_{p,p,c,\varepsilon}) &\geq N \cdot \left[-(c + \varepsilon) \cdot (p-1) \log(N) + \frac{\Delta(N)}{N} \log(p) + O_{N,p}(1) \right]. \end{aligned}$$

For the maximal p -rank $\delta(N) = (p-2)(N-1)$, the above inequalities give a computable value $C_{p,c}$ independent of ε . The general case depends on the conjectural property of $\Delta(N)$ regarding $N \log(N)$, but if we consider known results with suitable c (as for instance in [5, 6, 27, 36]) we can deduce $\Delta(N) < \frac{c(p-1)}{\log(p)} N \log(N)$ for the family of p -cyclic extensions $F_{N,p}$.

(ii) If we replace \mathbb{Q} by a number field k and the fields $F_{N,p}$ by the p -cyclic extensions $F_{k,N,p}$ of k with N ramified prime ideals of k , the details of computations are more complicate, but the results and comments are similar

since the p -rank of $\mathcal{C}_{F_{k,N,p}}$ is still equivalent to $O_p(N)$ because of the exact sequence of genus theory and the inequalities [11, Theorem IV.4.5.1]:

$$N - c_{k,p} \leq \text{rk}_p(\mathcal{C}_{F_{k,N,p}}^G) \leq N + c'_{k,p},$$

where the constants $c_{k,p}$, $c'_{k,p}$ depend on the p -classes and units of k . Then, the general algorithm computing the p -rank via the filtration $(M_i)_{i \geq 0}$ is identical up to similar modifications (see [13, §4.4]) and shall give the p -rank ε -conjecture for the relative p -cyclic case without too much difficulties. The case of abelian p -extensions may be accessible from the p^n -cyclic cases, with some effort... So the proof of the strong ε -conjecture, for the family of p -cyclic extensions of k , remains open, but is clearly not a folk conjecture for such very particular real fields. Meanwhile a particular study of the algorithm giving $\Delta(N)$ should be a crucial step.

3. PARI/GP programs computing $\mathcal{C}_{F_{N,p}}$

3.1. The p -structure of some $\mathcal{C}_{F_{N,p}}$. The following numerical results show that exceptional p -classes (indicated by *) are not excessively frequent for these fields. We examine the cases $p = 3, 5, 7$, then $p = 2$ (one must precise p and the conductor $f = \ell_1 \cdots \ell_N$ in the following program giving all the $(p-1)^{N-1}$ fields of conductor f):

```
{p=3;f=7*13*19*31*37;V=polsubcyclo(f,p);d=matsize(V);d=component(d,2);
for(k=1,d,P=component(V,k);if(nfdisc(P)!=f^(p-1),next);K=bnfinit(P,1);
C8=component(K,8);h=component(component(C8,1),1);
C1=component(component(C8,1),2);print("p=",p," f=",f," P=",P," C1=",C1)}
```

```
p=3 f=1983163=7*13*19*31*37
P=x^3+x^2-661054*x+ 49725976 C1=[6,6,3,3]
P=x^3+x^2-661054*x+198463201 C1=[3,3,3,3]
P=x^3+x^2-661054*x+97321888 C1=[39,3,3,3,3]*
P=x^3+x^2-661054*x-186270421 C1=[3,3,3,3]
P=x^3+x^2-661054*x-79179619 C1=[6,6,3,3]
P=x^3+x^2-661054*x-188253584 C1=[3,3,3,3,3]*
P=x^3+x^2-661054*x+138968311 C1=[3,3,3,3]
P=x^3+x^2-661054*x-146607161 C1=[3,3,3,3,3]*
P=x^3+x^2-661054*x-158506139 C1=[3,3,3,3]
P=x^3+x^2-661054*x-140657672 C1=[6,6,3,3]
P=x^3+x^2-661054*x+186564223 C1=[3,3,3,3]
P=x^3+x^2-661054*x+81456584 C1=[3,3,3,3]
P=x^3+x^2-661054*x+206395853 C1=[3,3,3,3]
P=x^3+x^2-661054*x-206102051 C1=[12,12,3,3]
P=x^3+x^2-661054*x+2130064 C1=[3,3,3,3,3]*
P=x^3+x^2-661054*x+27911183 C1=[3,3,3,3,3]*
```

```
p=3 f=85276009=7*13*19*31*37*43
P=x^3-x^2-28425336*x+58104545836 C1=[3,3,3,3,3]
P=x^3-x^2-28425336*x+56995957719 C1=[3,3,3,3,3]
P=x^3-x^2-28425336*x-7472705085 C1=[3,3,3,3,3]
P=x^3-x^2-28425336*x+10264704787 C1=[3,3,3,3,3]
```

$P=x^3-x^2-28425336*x+51623569152$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x+30901498965$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x-50622365639$	$C1=[6,6,3,3,3]$
$P=x^3-x^2-28425336*x-29132811371$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x-46614393216$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x-33226059803$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x-56506410260$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x-12248161589$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x+23994142236$	$C1=[6,6,3,3,3]$
$P=x^3-x^2-28425336*x+52220501215$	$C1=[3,3,3,3,3,3]*$
$P=x^3-x^2-28425336*x+11799672949$	$C1=[6,6,3,3,3]$
$P=x^3-x^2-28425336*x-57529722368$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x-21287418543$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x-47040773261$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x+36273887532$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x-53436473936$	$C1=[6,6,3,3,3,3]*$
$P=x^3-x^2-28425336*x+40964068027$	$C1=[21,3,3,3,3]$
$P=x^3-x^2-28425336*x+45824800540$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x+56313749647$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x+13078813084$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x+39940755919$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x-37830964289$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x+57848717809$	$C1=[6,6,3,3,3]$
$P=x^3-x^2-28425336*x-9775157328$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x-2526696563$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x-58126654431$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x+28428494704$	$C1=[3,3,3,3,3]$
$P=x^3-x^2-28425336*x-51986781783$	$C1=[3,3,3,3,3]$

$p=5$ $f=13981=11*31*41$

$P=x^5+x^4-5592*x^3+46417*x^2+4301003*x-26664769$	$C1=[5,5]$
$P=x^5+x^4-5592*x^3+46417*x^2+2623283*x-26664769$	$C1=[5,5]$
$P=x^5+x^4-5592*x^3-261165*x^2-4479065*x-26832541$	$C1=[55,5,5]*$
$P=x^5+x^4-5592*x^3+32436*x^2+1518784*x+1814528$	$C1=[5,5]$
$P=x^5+x^4-5592*x^3-205241*x^2-2074333*x-6028813$	$C1=[5,5,5]*$
$P=x^5+x^4-5592*x^3-135336*x^2+847696*x+1143440$	$C1=[5,5]$
$P=x^5+x^4-5592*x^3-205241*x^2-1878599*x+234675$	$C1=[5,5]$
$P=x^5+x^4-5592*x^3+74379*x^2+3993421*x-7035445$	$C1=[5,5]$
$P=x^5+x^4-5592*x^3+158265*x^2-424575*x-12851541$	$C1=[5,5]$
$P=x^5+x^4-5592*x^3+130303*x^2+442247*x+346523$	$C1=[5,5]$
$P=x^5+x^4-5592*x^3+46417*x^2+1644613*x-16878069$	$C1=[5,5]$
$P=x^5+x^4-5592*x^3+214189*x^2-2493763*x+5715227$	$C1=[5,5]$
$P=x^5+x^4-5592*x^3+74379*x^2+3238447*x-28174717$	$C1=[5,5]$
$P=x^5+x^4-5592*x^3+32436*x^2+5992704*x-2659392$	$C1=[5,5,5]*$
$P=x^5+x^4-5592*x^3-37469*x^2+4384889*x-11397517$	$C1=[5,5]$
$P=x^5+x^4-5592*x^3-9507*x^2+7432747*x+1185383$	$C1=[5,5]$

3.2. Examples of exceptional p -classes. As we can see, if one drops the ambiguous classes from the class group, this gives a very small component (often equal to 1); for instance we list some fields of the above tables with exceptional p -classes and/or nontrivial non- p -parts of the class group (for $p = 3, 5, 7, 11$):

p=3

$$f=1983163 \quad P=x^3+x^2-661054*x+97321888$$

$$C1=[39, 3, 3, 3, 3]=[13]x[3, 3, 3, 3, 3]*$$

$$f=1983163 \quad P=x^3+x^2-661054*x-206102051$$

$$C1=[12, 12, 3, 3]=[4, 4]x[3, 3, 3, 3]$$

$$f=85276009 \quad P=x^3-x^2-28425336*x-53436473936$$

$$C1=[6, 6, 3, 3, 3, 3]=[2, 2]x[3, 3, 3, 3, 3, 3]*$$

p=5

$$f=13981 \quad P=x^5+x^4-5592*x^3-261165*x^2-4479065*x-26832541$$

$$C1=[55, 5, 5]=[11]x[5, 5, 5]*$$

p=7

$$f=88537 \quad P=x^7+x^6-37944*x^5-1134719*x^4+324123632*x^3+13095064100*x^2-393352790753*x-8536744545007$$

$$C1=[301, 7]=[43]x[7, 7]$$

$$f=10004681 \quad P=x^7-x^6-4287720*x^5-1266715121*x^4+5127549957760*x^3+2650344024068794*x^2-951078919604894529*x-488606218944681147667$$

$$C1=[791, 7, 7]=[113]x[7, 7, 7]$$

$$f=10004681 \quad P=x^7-x^6-4287720*x^5+3455494311*x^4+176273349584*x^3-471685834336278*x^2-36087798097778993*x+6487901368894795147$$

$$C1=[7, 7, 7, 7]*$$

$$f=10004681 \quad P=x^7-x^6-4287720*x^5+2985274304*x^4+1830007100160*x^3-1788009977372784*x^2+233770322355404864*x-5599630780142239232$$

$$C1=[14, 14, 14]=[2, 2, 2]x[7, 7, 7]$$

$$f=10004681 \quad P=x^7-x^6-4287720*x^5+6276814353*x^4-4047542893720*x^3+1360785664233294*x^2-232635292693132049*x+15953699891990750023$$

$$C1=[7, 7, 7, 7]*$$

$$f=10004681 \quad P=x^7-x^6-4287720*x^5-6169008811*x^4-3865457699520*x^3-1247559831026016*x^2-202130636944756129*x-12969698603184144677$$

$$C1=[7, 7, 7, 7]*$$

$$f=10004681 \quad P=x^7-x^6-4287720*x^5+1224450448*x^4+5079527488960*x^3-2161274540764336*x^2-1677161713287529664*x+812143879436422435328$$

$$C1=[7, 7, 7, 7]*$$

$$f=10004681 \quad P=x^7-x^6-4287720*x^5-1306733845*x^4+4849019638720*x^3+2420349994235592*x^2-659732951886568641*x-207964718993797238079$$

$$C1=[7, 7, 7, 7]*$$

$$f=10004681 \quad P=x^7-x^6-4287720*x^5+5756570941*x^4-3107102879720*x^3+760318637129246*x^2-74394888056758073*x+1594979915105904419$$

$$C1=[7, 7, 7, 7]$$

$$f=10004681 \quad P=x^7-x^6-4287720*x^5-1746939809*x^4+2392910471944*x^3+1648023037138232*x^2+241022177190387487*x-9669121620934915453$$

$$C1=[7, 7, 7, 7]*$$

$$f=10004681 \quad P=x^7-x^6-4287720*x^5-4188081973*x^4-284662313448*x^3+706702291060440*x^2+90226184532822239*x-3998693323498243787$$

$$C1=[7, 7, 7, 7]*$$

$$f=10004681 \quad P=x^7-x^6-4287720*x^5-2227164497*x^4+1569805356712*x^3+369664737597974*x^2-166416491455189217*x+3813962316737479895$$

$$C1=[7, 7, 7, 7]*$$

$$f=10004681 \quad P=x^7-x^6-4287720*x^5-3307670045*x^4+1296557509240*x^3+1587033521303494*x^2+232482552302284071*x-10617355312468435915$$

$$C1=[203, 7, 7]=[203]x[7, 7, 7]$$

$$f=10004681 \quad P=x^7-x^6-4287720*x^5+1654651731*x^4+4187910318240*x^3-1965195178959414*x^2-1012216801097102473*x+451605062388713519719$$

```

                                C1=[14,14,14]=[2,2,2]x[7,7,7]
f=10004681  P=x^7-x^6-4287720*x^5+1544600240*x^4+4818925558272*x^3
-2343209264562096*x^2-1609606088655340480*x+886992887186768275456
                                C1=[203,7,7]=[203]x[7,7,7]
f=10004681  P=x^7-x^6-4287720*x^5-1306733845*x^4+4427622475000*x^3
+1798213808544282*x^2-1313378138040048441*x-613859706212867719587
                                C1=[301,7,7]=[301]x[7,7,7]

p=11
f=137149  P=x^11+x^10-62340*x^9-2099173*x^8+998038116*x^7+30321726924*x^6
-5078707527329*x^5+3275334221180*x^4+8066546096404148*x^3
-214723422858644515*x^2+1902599837479513519*x-4121588229203611219
                                C1=[253,11]=[23]x[11,11]
f=137149  P=x^11+x^10-62340*x^9-727683*x^8+1217887963*x^7+33409088063*x^6
-7760886906947*x^5-350751766601032*x^4+3398347545513222*x^3
+236507399684756272*x^2+2593585988882665302*x+8529384350363670191
                                C1=[979,11]=[89]x[11,11]
f=137149  P=x^11+x^10-62340*x^9-1550577*x^8+1265615815*x^7+66889353347*x^6
-7866931610939*x^5-712972865698216*x^4-12900860936489076*x^3
+143276981594922336*x^2+1596818122984871186*x+3178173588229813309
                                C1=[737,11]=[67]x[11,11]
f=137149  P=x^11+x^10-62340*x^9-7310835*x^8+70636578*x^7+43296296622*x^6
+1378934348258*x^5-28471672310749*x^4-944763467217249*x^3
+12433374265353417*x^2+31266667418235948*x-324164722946199831
                                C1=[253,11]=[23]x[11,11]
f=137149  P=x^11+x^10-62340*x^9-727683*x^8+1153290784*x^7+18055120364*x^6
-7130815486262*x^5-134781314432095*x^4+13777568483843493*x^3
+310799275320778321*x^2+883774494827373474*x-5728549445587601897
                                C1=[253,11]=[23]x[11,11]

```

For $p = 2$, we choose odd discriminants for which $F_{N,2}$ may be real or complex; as we know, the 2-rank is always $N - 1$ and any exceptional classes give non-trivial 4-ranks. The PARI/GP instruction `bnfnarrow` allows the 2-structure in the restricted sense:

```

{m=1;for(N=2,100,e1=prime(N);m=(-1)^((e1-1)/2)*e1*m;P=x^2-m;
K=bnfinit(P,1);L=bnfnarrow(K);C1=component(L,2);print("m=",m," C1=",C1))}

```

```

m=-3  C1=[]
m=-15 C1=[2]
m=+105 C1=[2,2]
m=-1155 C1=[2,2,2]
m=-15015 C1=[12,2,2,2]
m=-255255 C1=[16,2,2,2,2]*
m=+4849845 C1=[4,2,2,2,2,2]*
m=-111546435 C1=[42,2,2,2,2,2,2]
m=-3234846615 C1=[308,2,2,2,2,2,2,2]*
m=+100280245065 C1=[2,2,2,2,2,2,2,2,2]
m=+3710369067405 C1=[34,2,2,2,2,2,2,2,2,2]
m=+152125131763605 C1=[2,2,2,2,2,2,2,2,2,2,2]
m=-6541380665835015 C1=[28284,2,2,2,2,2,2,2,2,2,2,2]*
m=+307444891294245705 C1=[14,2,2,2,2,2,2,2,2,2,2,2,2]
m=+16294579238595022365 C1=[2,2,2,2,2,2,2,2,2,2,2,2,2,2,2]
m=-961380175077106319535 C1=[1210734,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2]

```

```

m=-58644190679703485491635  C1=[1622526,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2]
m=+3929160775540133527939545  C1=[2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2]
m=-278970415063349480483707695
      C1=[83911452,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2]*
m=-20364840299624512075310661735
      C1=[362626834,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2]
m=+1608822383670336453949542277065
      C1=[4,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2]*
m=-133532257844637925677812008996395
      C1=[2322692420,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2]*

```

For $m = -58644190679703485491635$ and $\#\mathcal{C}_K = 2^{16} \cdot 3 \cdot 270421$, one may compute a lower bound for $\log(C_\varepsilon)$ as a function of ε :

```

{for (e=1,20, eps=10^-e; X=log(53166931968)-
eps*log(58644190679703485491635); print("eps=10^", -e, " log(C_eps)=", X))}

```

```

eps=10^-1   log(C_eps)=19.454124913242064862076764295884513437
eps=10^-2   log(C_eps)=24.172444705760239527345923333230826283
(...)
eps=10^-19  log(C_eps)=24.696702460484481151577696790138000305
eps=10^-20  log(C_eps)=24.696702460484481156296016582656174970

```

Clearly, the lower bound of C_ε , for $\varepsilon = 10^{-20}$, seems to be:

$$53166931967.999999972126823620879814694 \approx 53166931968.$$

4. Genus theory – Abelian p -ramification theory

4.1. Reminders on Genus theory. For wide information on genus theory, see for example [7, 8, 9, 11, 22, 23, 28].

4.1.1. Genus field and genus number $g_{K/k}$. Introduce the genus field according to an extension K/k (we shall take $k = \mathbb{Q}$ in the sequel) which is the maximal subextension $H_{K/k}$ of H_K (in the restricted sense) equal to the compositum of K with an abelian extension of k :

$$\begin{array}{ccccccc}
 K & \text{---} & KH_k & \text{---} & H_{K/k} & \text{---} & H_K \\
 | & & | & & | & & \\
 K^{\text{ab}} & \text{---} & K^{\text{ab}}H_k & \text{---} & H_K^{\text{ab}} & & \\
 | & & | & & & & \\
 K \cap H_k & \text{---} & H_k & & & & \\
 | & & & & & & \\
 k & & & & & &
 \end{array}$$

Thus $H_{K/k}$ is for instance equal to the compositum of K with H_K^{ab} (the maximal abelian subextension of H_K/k), according to the diagram above, where K^{ab} is the maximal abelian subextension of K/k . The genus number is $g_{K/k} := [H_{K/k} : KH_k]$. When K/k is cyclic, the genus number $g_{K/k}$ is equal to the number of invariant classes by $\text{Gal}(K/k)$ given by Chevalley's

formula (1). In the general Galois case, we have the similar expression $g_{K/k} = \frac{\#\mathcal{C}_k \cdot \prod_{\mathfrak{l}} e_{\mathfrak{l}}^{\text{ab}}}{[K^{\text{ab}} : k] \cdot (E_k^{\text{pos}} : E_k^{\text{pos}} \cap \mathcal{N}_{K/k})}$, where E_k^{pos} is the group of *totally positive* units of k , $e_{\mathfrak{l}}^{\text{ab}}$ the index of ramification of \mathfrak{l} in K^{ab}/k and $\mathcal{N}_{K/k}$ the group of local norms in K/k . A general formula does exist for non-Galois fields (e.g., [11, Theorem IV.4.2 & Corollaries]).

4.1.2. Non-genus ε -conjecture. Considering that the genus group of K may be an obstruction to an easy proof of the strong ε -conjecture for the totally real number fields, we may consider the number $\frac{1}{g_{K/\mathbb{Q}}} \cdot \#\mathcal{C}_K$ (giving the number of exceptional classes and of “ordinary” classes instead of the whole class group) and propose the following global form of the ε -conjecture for totally real fields K :

Conjecture 4.1. *For all $\varepsilon > 0$ there exists a constant $C'_{d,\varepsilon}$ such that the inequality $g_{K/\mathbb{Q}}^{-1} \cdot \#\mathcal{C}_K \leq C'_{d,\varepsilon} \cdot (\sqrt{D_K})^\varepsilon$ is fulfilled for all totally real number field K , where $g_{K/\mathbb{Q}}$ is the genus number of K/\mathbb{Q} .*

The following program, for imaginary quadratic fields, allows a study of the analogous question in the non-real case by computing the successive local maxima of $C'_{d,\varepsilon}$ given in C, the discriminant and the class number obtained for each local maximum of C are given in D and h:

```
{eps=0.05; Cm=0; bD=2; BD=10^9; for (D=bD, BD, e=valuation(D, 2); M=D/2^e;
if (core(M) != M, next); if ((e==1 || e>3) || (e==0 & Mod(M, 4) != -1) || (e==2 & Mod(M, 4) != 1),
next); h=qfbclassno(-D); N=bigomega(D); if (e==2, N=N-1); if (e==3, N=N-2);
C=h/(2^(N-1)*(sqrt(D)^eps)); if (C>Cm, Cm=C; print("D=", -D, " h=", h, " C=", C))}
```

As far as the program has run, it slows down between $C = 6 \cdot 10^4$ and $C = 7 \cdot 10^4$, but no conclusion is possible. But the most spectacular fact, that we have discover, is that, for each local maximum of C, the corresponding discriminant is prime (whence h odd) whatever ε , as shown by this short excerpt:

D	h	C
-3	1	0.972908434869468710702241668941166407
-23	3	2.773818617890694606606085132125197163
-47	5	4.541167885124564220325740509229014479
-71	7	6.292403751297605635733619062872115785
-167	11	9.678872599268429560299054329160821597
-191	13	11.400332501352005304200415816510168367
-239	15	13.080709822134822456679612679136456819
-311	19	16.460180420909375330798097085967676763
-431	21	18.045019802162182082161592477498679286
-479	25	21.425532320359474690178248184779886979
(...)		
-1118314391	77395	45972.572539103313552220923397893022055
-1130984399	77697	46138.963607764612827282941613333974355
-1139075159	78141	46394.356488699687700451681236043961611
-1184068679	81267	48203.636807716833174323833829210758624

-1229647319 81419 48248.214898940545998582986401841694028
 -1237871879 82171 48685.729279564354497202266261569081321
 -1250370239 83503 49462.505651262222727040029721940389296

We have no counterexample in the selected interval $D \leq 2 \cdot 10^9$ and no serious explanation, but if we test the local maxima of $\frac{\#\mathcal{O}_K}{(\sqrt{D_K})^\varepsilon}$ instead of $2^{-(N-1)} \frac{\#\mathcal{O}_K}{(\sqrt{D_K})^\varepsilon}$, we have for instance the following normal behaviour:

D=[3, 1; 5, 1]	h=2	C2=1.8690792417830016333288729232969402612
D=Mat([23, 1])	h=3	C2=2.7738186178906946066060851321251971632
D=[3, 1; 13, 1]	h=4	C2=3.6499202570298105632113852382187054319
D=Mat([47, 1])	h=5	C2=4.5411678851245642203257405092290144795
D=Mat([71, 1])	h=7	C2=6.2924037512976056357336190628721157852
D=[5, 1; 19, 1]	h=8	C2=7.1391564091327201771370767959908455517
D=[7, 1; 17, 1]	h=10	C2=8.8738345254872857598506328581670649858
(...)		
D=Mat([63839, 1])	h=423	C2=320.78438186581184951419633278279394585
D=[23, 1; 2833, 1]	h=424	C2=321.37826092893978747476207092089453868
D=[113, 1; 607, 1]	h=434	C2=328.53606501556853121813362584226004750
D=[19, 1; 23, 1; 163, 1]	h=440	C2=332.76370450428389891215784283045533831
D=[41, 1; 1831, 1]	h=454	C2=342.90123385517606193005461615124054801
D=[19, 1; 37, 1; 113, 1]	h=468	C2=352.97586311634473415004028909597003881
D=[43, 1; 1973, 1]	h=480	C2=361.43179021472306392157190052394995551
D=Mat([88079, 1])	h=487	C2=366.35924203761999218970143789845358049

4.2. Reminders on p -ramification theory. We intend to give now some analogies with the torsion group \mathcal{T}_K of the Galois group of the maximal abelian p -ramified (i.e., unramified outside p and ∞) pro- p -extension of K ; this extension contains the p -Hilbert class field of K (in the ordinary sense) and the compositum of the \mathbb{Z}_p -extensions of K . This Galois group introduces the “normalized” p -adic regulator of K defined in [16, § 5]. Since in this section the non- p -part of the class group does not intervene, unless otherwise stated, we shall put, by abuse of notation, $\mathcal{O}_K := \mathcal{O}_K \otimes \mathbb{Z}_p$.

4.2.1. Structure of the p -torsion group \mathcal{T}_K . Let K be any number field and let $p \geq 2$ be a prime number; we denote by $\mathfrak{p} \mid p$ the prime ideals of K dividing p . Consider the group E_K of p -principal global units of K (i.e., units $\varepsilon \equiv 1 \pmod{\prod_{\mathfrak{p} \mid p} \mathfrak{p}}$). For each $\mathfrak{p} \mid p$, let $K_{\mathfrak{p}}$ be the \mathfrak{p} -completion of K and $\bar{\mathfrak{p}}$ the corresponding prime ideal of the ring of integers of $K_{\mathfrak{p}}$; then let:

$$U_K := \left\{ u \in \bigoplus_{\mathfrak{p} \mid p} K_{\mathfrak{p}}^\times, u = 1 + x, x \in \bigoplus_{\mathfrak{p} \mid p} \bar{\mathfrak{p}} \right\} \quad \& \quad W_K := \text{tor}_{\mathbb{Z}_p}(U_K),$$

the \mathbb{Z}_p -module of principal local units at p and its torsion subgroup.

We consider the diagonal embedding $E_K \otimes \mathbb{Z}_{\bar{p}} \rightarrow U_K$ whose image is \bar{E}_K , the topological closure of E_K in U_K .

We assume in this paper that K satisfies the Leopoldt conjecture at p . Whence the following p -adic result ([16, Lemma 3.1, Corollary 3.2], [11, Lemma 4.2.4], [21, Définition 2.11, Proposition 2.12]):

Lemma 4.2. *Let μ_K be the group of global roots of unity of p -power order of K . Under the Leopoldt conjecture for p in K , we have $\mathrm{tor}_{\mathbb{Z}_p}(\overline{E}_K) = \mu_K$ and the exact sequence (where \log is the p -adic logarithm):*

$$1 \rightarrow W_K/\mu_K \longrightarrow \mathrm{tor}_{\mathbb{Z}_p}(U_K/\overline{E}_K) \xrightarrow{\log} \mathrm{tor}_{\mathbb{Z}_p}(\log(U_K)/\log(\overline{E}_K)) \rightarrow 0.$$

Put $\mathcal{W}_K := W_K/\mu_K$ & $\mathcal{R}_K := \mathrm{tor}_{\mathbb{Z}_p}(\log(U_K)/\log(\overline{E}_K))$. Then the above exact sequence becomes:

$$1 \rightarrow \mathcal{W}_K \longrightarrow \mathrm{tor}_{\mathbb{Z}_p}(U_K/\overline{E}_K) \xrightarrow{\log} \mathcal{R}_K \rightarrow 0.$$

Let \tilde{K} be the compositum of the \mathbb{Z}_p -extensions, H_K the p -Hilbert class field and H_K^{pr} the maximal Abelian p -ramified pro- p -extension, of K . Then let H_K^{bp} be the Bertrandias–Payan field (compositum of the p -cyclic extensions of K embeddable in p -cyclic extensions of arbitrary large degree). In the following diagram, class field theory yields $\mathrm{Gal}(H_K^{\mathrm{pr}}/H_K) \simeq U_K/\overline{E}_K$:

$$\begin{array}{ccccc}
 & & \mathcal{T}_K & & \\
 & \tilde{K} & \xrightarrow{\quad} & \tilde{K}H_K & \xrightarrow{\quad} & H_K^{\mathrm{bp}} & \xrightarrow{\quad} & H_K^{\mathrm{pr}} \\
 & \downarrow & \simeq \tilde{\mathcal{C}}_K & \downarrow & \simeq \mathcal{R}_K & \downarrow & \simeq \mathcal{W}_K & \downarrow \\
 & \tilde{K} \cap H_K & \xrightarrow{\quad} & H_K & \xrightarrow{\quad} & H_K^{\mathrm{pr}} & \xrightarrow{\quad} & H_K^{\mathrm{pr}} \\
 & \downarrow & & \downarrow & \simeq U_K/\overline{E}_K & & & \downarrow \\
 & K & & K & & & & K \\
 & & & \simeq \mathcal{C}_K & & & &
 \end{array}$$

We denote by $\tilde{\mathcal{C}}_K$ the subgroup of the p -class group \mathcal{C}_K corresponding to $\mathrm{Gal}(H_K/\tilde{K} \cap H_K)$ by class field theory. The group \mathcal{R}_K is then isomorphic to $\mathrm{Gal}(H_K^{\mathrm{bp}}/\tilde{K}H_K)$ and \mathcal{W}_K isomorphic to $\mathrm{Gal}(H_K^{\mathrm{pr}}/H_K^{\mathrm{bp}})$.

We have $\#\mathcal{T}_K = \#\tilde{\mathcal{C}}_K \cdot \#\mathcal{R}_K \cdot \#\mathcal{W}_K$ and the following inequalities:

$$\begin{aligned}
 (5) \quad \mathrm{rk}_p(\mathcal{T}_K) &\leq \mathrm{rk}_p(\tilde{\mathcal{C}}_K) + \mathrm{rk}_p(\mathcal{R}_K) + \mathrm{rk}_p(\mathcal{W}_K) \\
 &\leq \mathrm{rk}_p(\mathcal{C}_K) + r_1 + r_2 - 1 + \#S_K,
 \end{aligned}$$

where (r_1, r_2) is the signature of K and S_K the set of p -places of K . So, for a constant degree d , the p -rank ε -conjecture for the p -class groups implies the p -rank ε -conjecture for the torsion groups \mathcal{T}_K and conversely since we have the other inequality:

$$\begin{aligned}
 (6) \quad \mathrm{rk}_p(\mathcal{C}_K) &\leq \mathrm{rk}_p(\tilde{\mathcal{C}}_K) + \mathrm{rk}_p(\mathrm{Gal}(\tilde{K} \cap H_K/K)) \\
 &\leq \mathrm{rk}_p(\tilde{\mathcal{C}}_K) + r_2 + 1 \leq \mathrm{rk}_p(\mathcal{T}_K) + r_2 + 1.
 \end{aligned}$$

For more precise rank formulas for \mathcal{T}_K , see [11, Corollary III.4.2.3] and the reflection theorem in §4.4.

4.2.2. The p -adic Brauer–Siegel conjecture for \mathcal{T}_K . We have proposed in [12] for the totally real case, after extensive numerical computations, the following conjecture:

Conjecture 4.3. *Let $p \geq 2$ be prime and let d be a given degree. For any number field K , let \mathcal{T}_K be the torsion group of the Galois group of the maximal abelian p -ramified pro- p -extension of K (under Leopoldt’s conjecture). There exists a constant $\mathcal{C}_{d,p}$ such that:*

$$\#\mathcal{T}_K \leq (\sqrt{D_K})^{\mathcal{C}_{d,p}}, \text{ for all } K, \text{ totally real of degree } d.$$

We put, for p fixed and for any totally real number field K :

$$\mathcal{C}_{K,p} := \frac{\log(\#\mathcal{T}_K)}{\log(\sqrt{D_K})}.$$

In practice, $\mathcal{C}_{K,p}$ may be much smaller than 1, except very sparse cases as that of $K = \mathbb{Q}(\sqrt{19})$ and $p = 13599893$, for which $\mathcal{T}_K = \mathcal{R}_K \simeq \mathbb{Z}/p\mathbb{Z}$, whence $\mathcal{C}_{K,p} = \frac{\log(\#\mathcal{T}_K)}{\log(\sqrt{4 \times 19})} = \frac{\log(13599893)}{\log(\sqrt{4 \times 19})} = 7.5855$. But $\mathcal{C}_K = 1$.

4.2.3. Estimation of $\mathcal{C}_{F_{N,p},p}$. Put $F = F_{N,p}$ and $\mathcal{C}_{N,p} := \mathcal{C}_{F_{N,p},p}$. Then, from the computations in Subsection 2.3, using for the group \mathcal{T}_F the analog of Chevalley’s formula given in [11, Theorem IV.3.3], we can put similarly $\#\mathcal{T}_F =: p^{N-r+\tilde{\Delta}(N)}$, $\tilde{\Delta}(N) \geq 0$, where $r \geq 0$ depends on p -adic properties of the ramified primes $\ell \neq p$, and estimate that, as $N \rightarrow \infty$:

$$\mathcal{C}_{N,p} \approx \frac{(N - r + \tilde{\Delta}(N)) \log(p)}{\frac{p-1}{2} [N \log(N) + N \gamma_p + \frac{1}{2} \log(N) + O_{N,p}(1)]} \sim c_p \cdot \frac{1 + o_{N,p}(1)}{\log(N)},$$

where $c_p = \frac{2 \log(p)}{p-1}$ and assuming a small order of magnitude of $\tilde{\Delta}(N)$.

Give now a program computing $\mathcal{C}_{N,2}$ (in $\mathbb{C}p$); in the imaginary quadratic case for $p = 2$, the conjectural inequality becomes $\#(\tilde{\mathcal{C}}_F) \leq (\sqrt{D_F})^{\mathcal{C}_{d,p}}$ (indeed, $\#\mathcal{R}_F = 1$ and $\#\mathcal{T}_F = \#\tilde{\mathcal{C}}_F \cdot \mathcal{W}_F$, where $\mathcal{W}_F = 2$ (resp. 1) if $m \equiv \pm 1 \pmod{8}$ (resp. if not)). So \mathcal{C}_F (in Clres) may be larger than $\#\mathcal{T}_F$ (in Tor):

```
{p=2;n=12;m=1;for(N=2,100,e1=prime(N);m=(-1)^(e1-1)/2*e1*m;P=x^2-m;
K=bnfinit(P,1);D=abs(m);Kpn=bnrinit(K,p^n);r=1;if(m<0,r=2);L=List;
Hpn=component(component(Kpn,5),2);e=component(matsize(Hpn),2);T=1;
for(k=1,e-r,c=component(Hpn,e-k+1);if(Mod(c,p)==0,q=p^valuation(c,p);
T=T*q;listinsert(L,q,1));C8=component(K,8);h=component(component(C8,1),1);
Clord=component(component(C8,1),2);K=bnfnarrow(K);Cl=component(K,2);
print("m=",m," Clres=",Clres," Clord =",Clord);
print("Structure of T=",L);print("#Tor=",T," Cp=",log(T)/log(sqrt(D))));}
```

```
m=-3 Clres=[]
Structure of Tor=[]
#Tor=1 Cp=0.E-38
m=-15 Clres=[2]
Structure of Tor=[2]
```

```

#Tor=2          Cp=0.51191604961963097877535535772960454081
m=105   Clres=[2,2]=[2]xClord
Structure of Tor=[2,2]
#Tor=4          Cp=0.59574824743531323067786608868687642325
m=-1155   Clres=[2,2,2]
Structure of Tor=[2,2,2]
#Tor=8          Cp=0.58975726471501581115878339498474155345
m=-15015   Clres=[12,2,2,2]
Structure of Tor=[2,2,2,2]
#Tor=16         Cp=0.57661327808675875001115538902772596330
m=-255255   Clres=[16,2,2,2,2]
Structure of Tor=[2,2,2,2,2]
#Tor=32         Cp=0.55674390390043840097934284424073618196
m=4849845   Clres=[4,2,2,2,2,2]=[2]xClord
Structure of Tor=[4,2,2,2,2,2]
#Tor=128        Cp=0.63036067699149527703810495075838580918
m=-111546435   Clres=[42,2,2,2,2,2,2]
Structure of Tor=[2,2,2,2,2,2,2]
#Tor=128        Cp=0.52369594802182316940823598390366865409
m=-3234846615   Clres=[308,2,2,2,2,2,2,2]
Structure of Tor=[4,2,2,2,2,2,2,2]
#Tor=512        Cp=0.56978162829823280646049502887398109011
m=100280245065   Clres=[2,2,2,2,2,2,2,2,2]=[2]xClord
Structure of Tor=[2,2,2,2,2,2,2,2,2]
#Tor=512        Cp=0.49254011775311327297187105815891979776
m=3710369067405   Clres=[34,2,2,2,2,2,2,2,2,2]=[2]xClord
Structure of Tor=[2,2,2,2,2,2,2,2,2,2]
#Tor=1024       Cp=0.47898799604336105240349464751069989167
m=152125131763605   Clres=[2,2,2,2,2,2,2,2,2,2,2]=[2]xClord
Structure of Tor=[4,2,2,2,2,2,2,2,2,2,2]
#Tor=4096       Cp=0.50942162732997733185991268818214459006
m=-6541380665835015   Clres=[28284,2,2,2,2,2,2,2,2,2,2,2]
Structure of Tor=[2,2,2,2,2,2,2,2,2,2,2,2]
#Tor=4096       Cp=0.45680772041407406738242757697825579415
m=307444891294245705   Clres=[14,2,2,2,2,2,2,2,2,2,2,2,2]=[2]xClord
Structure of Tor=[2,2,2,2,2,2,2,2,2,2,2,2,2]
#Tor=8192       Cp=0.44755741322126195443312989366082458089
m=16294579238595022365   Clres=[2,2,2,2,2,2,2,2,2,2,2,2,2,2]=[2]xClord
Structure of Tor=[32,2,2,2,2,2,2,2,2,2,2,2,2,2]
#Tor=262144    Cp=0.56407742575833976013164891102271736655
m=-961380175077106319535   Clres=[1210734,2,2,2,2,2,2,2,2,2,2,2,2,2,2]
Structure of Tor=[2,2,2,2,2,2,2,2,2,2,2,2,2,2,2]
#Tor=32768     Cp=0.43039341330765014032907101774855577316
m=-58644190679703485491635   Clres=[1622526,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2]
Structure of Tor=[2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2]
#Tor=65536     Cp=0.42308787191112227068703992014107942867

```

We do not know an algorithm computing the “exceptional elements” of \mathcal{T}_F as for p -class groups.

The case $p = 3$ is similar and gives for instance for the 16 cyclic cubic fields of conductor $f = 7 \cdot 13 \cdot 19 \cdot 31 \cdot 37$:

```

P=x^3+x^2-661054*x+49725976      Cl=[3,3,3,3,3]

```

```

Structure of Tor=[9,3,3,3,3]
#Tor=729 Cp=0.45459180523024141673723101157712338880
P=x^3+x^2-661054*x+198463201 Cl=[6,6,3,3]
Structure of Tor=[9,3,3,3,3]
#Tor=729 Cp=0.45459180523024141673723101157712338880
P=x^3+x^2-661054*x+97321888 Cl=[3,3,3,3]
Structure of Tor=[3,3,3,3,3]
#Tor=243 Cp=0.37882650435853451394769250964760282400
P=x^3+x^2-661054*x-186270421 Cl=[39,3,3,3,3]
Structure of Tor=[9,3,3,3,3]
#Tor=729 Cp=0.45459180523024141673723101157712338880
P=x^3+x^2-661054*x-79179619 Cl=[3,3,3,3]
Structure of Tor=[3,3,3,3,3]
#Tor=81 Cp=0.30306120348682761115815400771808225920
P=x^3+x^2-661054*x-188253584 Cl=[6,6,3,3]
Structure of Tor=[9,3,3,3,3]
#Tor=729 Cp=0.45459180523024141673723101157712338880
P=x^3+x^2-661054*x+138968311 Cl=[3,3,3,3,3]
Structure of Tor=[3,3,3,3,3]
#Tor=81 Cp=0.30306120348682761115815400771808225920
P=x^3+x^2-661054*x-146607161 Cl=[3,3,3,3]
Structure of Tor=[3,3,3,3,3]
#Tor=243 Cp=0.37882650435853451394769250964760282400
P=x^3+x^2-661054*x-158506139 Cl=[3,3,3,3,3]
Structure of Tor=[3,3,3,3,3]
#Tor=243 Cp=0.37882650435853451394769250964760282400
P=x^3+x^2-661054*x-140657672 Cl=[3,3,3,3]
Structure of Tor=[3,3,3,3,3]
#Tor=243 Cp=0.37882650435853451394769250964760282400
P=x^3+x^2-661054*x+186564223 Cl=[6,6,3,3]
Structure of Tor=[3,3,3,3,3]
#Tor=81 Cp=0.30306120348682761115815400771808225920
P=x^3+x^2-661054*x+81456584 Cl=[3,3,3,3]
Structure of Tor=[3,3,3,3,3]
#Tor=243 Cp=0.37882650435853451394769250964760282400
P=x^3+x^2-661054*x+206395853 Cl=[3,3,3,3]
Structure of Tor=[3,3,3,3,3]
#Tor=81 Cp=0.30306120348682761115815400771808225920
P=x^3+x^2-661054*x-206102051 Cl=[3,3,3,3]
Structure of Tor=[3,3,3,3,3]
#Tor=81 Cp=0.30306120348682761115815400771808225920
P=x^3+x^2-661054*x+2130064 Cl=[12,12,3,3]
Structure of Tor=[3,3,3,3,3,3]
#Tor=729 Cp=0.45459180523024141673723101157712338880
P=x^3+x^2-661054*x+27911183 Cl=[3,3,3,3,3]
Structure of Tor=[3,3,3,3,3,3]
#Tor=243 Cp=0.37882650435853451394769250964760282400

```

Now we give some examples for $p = 2$ and $p = 3$ where the constant $\mathcal{C}_{N,p}$ is rather large; the cyclic extensions F are not necessary of the form F_N .

(i) $p = 2$, m divides $5 \cdot 7 \cdot \dots \cdot 41 \cdot 43$.

$m=5005$ Clres=[2,2,2] Clord =[2,2]

```

Structure of Tor=[4,2,2]
#Tor=16      Cp=0.65098051255057821664489247470558390764
m=1078282205 Clres=[4,2,2,2,2,2,2] Clord =[4,2,2,2,2,2,2]
Structure of Tor=[32,4,2,2,2,2,2]
#Tor=4096    Cp=0.79983769534579979852611700457236749058
m=215656441 Clres=[2,2,2,2,2,2] Clord =[2,2,2,2,2,2]
Structure of Tor=[8,2,2,2,2,2]
#Tor=256     Cp=0.57794783195778051534152523962133180636
m=436092044389001 Clres=[2,2,2,2,2,2,2,2,2,2] Clord =[2,2,2,2,2,2,2,2,2,2]
Structure of Tor=[32,2,2,2,2,2,2,2,2,2]
#Tor=16384   Cp=0.57575701869336876560350400103707496594
m=46189 Clres=[2,2,2] Clord =[2,2]
Structure of Tor=[16,2,2]
#Tor=64      Cp=0.77443028965455279095387556052161745644
m=221 Clres=[4] Clord =[2]
Structure of Tor=[16]
#Tor=16      Cp=1.0272342185833848333397010211662592994
m=435656388001 Clres=[2,2,2,2,2,2,2,2] Clord =[2,2,2,2,2,2,2,2]
Structure of Tor=[8,2,2,2,2,2,2]
#Tor=512     Cp=0.46554453503678235229309396294036417544

```

We note the case of $m = 221$ for which $\mathcal{C}_F^{\text{res}} \simeq \mathbb{Z}/4\mathbb{Z}$, $\mathcal{C}_F^{\text{ord}} \simeq \mathbb{Z}/2\mathbb{Z}$, but $\mathcal{T}_F \simeq \mathbb{Z}/16\mathbb{Z}$ due to the 2-adic regulator. This gives the exceptional value $\mathcal{C}_{F,2} \approx 1.02723422$.

(ii) $p = 3$, f divides $13 \cdot 19 \cdot 31 \cdot 37 \cdot 43$.

```

f=10621 P=x^3+x^2-3540*x-60579      C1=[3,3]
Structure of Tor=[9,9,3]
#Tor=243    Cp=0.33667761382504192691963484073748684274
P=x^3+x^2-4060762*x-3150249179      C1=[3,3,3,3]
Structure of Tor=[27,27,3,3,3]
#Tor=19683  Cp=0.60601970488507546845534271332747631693
f=12182287 P=x^3+x^2-4060762*x+187697459      C1=[9,9,3,3,3]
Structure of Tor=[9,9,3,3,3]
#Tor=2187   Cp=0.47134865935505869768748877703248157983
f=12182287 P=x^3+x^2-4060762*x+2380509119      C1=[3,3,3,3,3]
Structure of Tor=[9,3,3,3,3]
#Tor=729    Cp=0.40401313659005031230356180888498421129
f=12182287 P=x^3+x^2-4060762*x-2309671376      C1=[3,3,3,3,3]
Structure of Tor=[9,9,3,3,3]
#Tor=2187   Cp=0.47134865935505869768748877703248157983
f=641173 P=x^3-x^2-213724*x-29968901      C1=[6,6,3]
Structure of Tor=[9,3,3,3]
#Tor=243    Cp=0.33667761382504192691963484073748684274
f=392977 P=x^3-x^2-130992*x+6826156      C1=[3,3,3]
Structure of Tor=[9,3,3,3]
#Tor=243    Cp=0.33667761382504192691963484073748684274
f=7657 P=x^3+x^2-2552*x+47360      C1=[9,3,3]
Structure of Tor=[9,9,3]
#Tor=243    Cp=0.33667761382504192691963484073748684274

```

4.3. p -adic Brauer–Siegel conjecture versus ε -conjectures. The p -adic Brauer–Siegel Conjecture 4.3 concerns more essentially the totally real

case for the following reasons which are yet given by the rank inequalities (5) and (6).

4.3.1. Analysis by means of CM-fields. We have, with obvious notations and $p \neq 2$:

$$\begin{aligned}\mathcal{C}_K &= \mathcal{C}_K^- \oplus \mathcal{C}_K^+, & \mathcal{T}_K &= \mathcal{T}_K^- \oplus \mathcal{T}_K^+, \\ \mathcal{R}_K &= \mathcal{R}_K^- \oplus \mathcal{R}_K^+, & \mathcal{W}_K &= \mathcal{W}_K^- \oplus \mathcal{W}_K^+;\end{aligned}$$

but we have the following properties which explain the differences between real fields and non real ones (under the Leopoldt conjecture):

- (i) $\#\mathcal{R}_K^- = 1$ since all the units of infinite order of K are real;
- (ii) $\#\mathcal{C}_K^- = \#\tilde{\mathcal{C}}_K^- \cdot \#\text{Gal}(\tilde{K} \cap H_K/K)^-$ where $\text{Gal}(\tilde{K} \cap H_K/K)^- \simeq \mathcal{C}_K^-/\tilde{\mathcal{C}}_K^-$ may be large (with bounded rank), then $\tilde{\mathcal{C}}_K^-$ small since $\text{Gal}(\tilde{K}/K)^- \simeq \mathbb{Z}_p^{\frac{d}{2}}$ contrary to $\text{Gal}(\tilde{K}/K)^+ \simeq \mathbb{Z}_p$;
- (iii) $\#\mathcal{T}_K^- = \#\tilde{\mathcal{C}}_K^- \cdot \#\mathcal{W}_K^-$ is essentially equal to $\#\tilde{\mathcal{C}}_K^-$ since \mathcal{W}_K^- is most often trivial and does not intervene in estimations of class groups for d fixed;
- (iv) $\#\mathcal{R}_K^+$ is the main p -adic invariant which may be nontrivial for much primes p , even if we have conjectured in [19] that it is trivial for all p large enough;
- (v) $\#\mathcal{C}_K^+$ is essentially equal to $\#\tilde{\mathcal{C}}_K^+$ since the part of the Hilbert class field, contained in the cyclotomic \mathbb{Z}_p -extension, is very limited;
- (vi) $\#\mathcal{T}_K^+ = \#\tilde{\mathcal{C}}_K^+ \cdot \#\mathcal{R}_K^+ \cdot \#\mathcal{W}_K^+$ is essentially the product $\#\mathcal{C}_K^+ \cdot \#\mathcal{R}_K^+$.

So if we assume that $\#\mathcal{T}_K^+$ is controled, we may consider that $\#\mathcal{C}_K^+$ is much less than $\#\mathcal{T}_K^+$ because of the regulator; then, since $\#\mathcal{T}_K^-$ is independent of any regulator, it is mesured by a divisor of $\#\mathcal{C}_K^-$ (equal to $\#\tilde{\mathcal{C}}_K^-$) and by $\#\mathcal{W}_K^-$ controled, which explains (from $[\tilde{K} \cap H_K : K]$) a bigger order of magnitude of $\#\mathcal{C}_K^-$ regarding $\#\mathcal{T}_K^-$ than $\#\mathcal{C}_K^+$ regarding $\#\mathcal{T}_K^+$.

4.3.2. Computation of $\mathcal{C}_{K,p}$ (imaginary quadratic fields). We illustrate the cases $p = 2$, then $p = 3$, in various intervals of negative discriminants to observe the local decreasing of the variable $\mathcal{C}_{K,p}$.

Note that for $p > 3$, the group \mathcal{W}_K is trivial contrary to the cases $p = 2$ and 3 where \mathcal{W}_K may be $\mathbb{Z}/p\mathbb{Z}$, which must probably be discarded in our considerations.

(b) Case $p = 2$. The case $p = 2$ is interesting because of the influence of exceptional classes and gives:

```
{p=2; bD=10^8; BD=2*10^8; Lp=log(p); vp=0; n=18;
for(D=bD, BD, e=valuation(D, 2); M=D/2^e; if(core(M) != M, next);
if((e==1 || e>3) || (e==0 & Mod(M, 4) != -1) || (e==2 & Mod(M, 4) == -1), next);
m=D; if(e != 0, m=D/4); P=x^2+m; K=bnfinit(P, 1); Kpn=bnrinit(K, p^n);
C5=component(Kpn, 5); Hpn0=component(C5, 1); Hpn=component(C5, 2);
Hpn1=component(Hpn, 1); vptor=valuation(Hpn0/Hpn1, p)-(n-1);
```

```
if (vptor > vp, vp = vptor); if (vptor >= vp, Cp = vptor * Lp / log(sqrt(D));
print("D=", -D, " m=", -m, " vptor=", vptor, " Cp=", Cp))}]
```

```
p=2, Interval [10^6, 2*10^6]
```

```
D=-1000011 m=-1000011 vptor=3 Cp=0.301029755983435929933445793
D=-1000020 m=-250005 vptor=3 Cp=0.3010295598834164958938994188
D=-1000036 m=-250009 vptor=4 Cp=0.4013722816881976053812061427
D=-1000132 m=-250033 vptor=5 Cp=0.5017118661610285687682449315
(...)
D=-1003620 m=-250905 vptor=5 Cp=0.5015854691511746133432777519
D=-1003940 m=-250985 vptor=6 Cp=0.6018886779424325532238667109
D=-1005843 m=-1005843 vptor=7 Cp=0.702107244840955486811297669
D=-1007492 m=-251873 vptor=8 Cp=0.8023131911871206028276870051
(...)
D=-1327972 m=-331993 vptor=8 Cp=0.7865966565831969109249007496
D=-1345476 m=-336369 vptor=9 Cp=0.8841001125437591214944446738
D=-1347524 m=-336881 vptor=10 Cp=0.982227596578129040877631145
```

```
p=2, Interval [10^7, 2*10^7]
```

```
D=-10000004 m=-2500001 vptor=3 Cp=0.25802570416574861895099915
(...)
D=-10000136 m=-2500034 vptor=3 Cp=0.25802549285588586651933610
D=-10000212 m=-2500053 vptor=4 Cp=0.34403382825873844184039068
D=-10000228 m=-2500057 vptor=5 Cp=0.43004224263528166242354902
(...)
D=-10001220 m=-2500305 vptor=5 Cp=0.43003959612044524303603555
D=-10001355 m=-10001355 vptor=7 Cp=0.6020549303754533561270683
(...)
D=-10028164 m=-2507041 vptor=10 Cp=0.8599356519990630566433445
D=-11423624 m=-2855906 vptor=10 Cp=0.8530415407428446759627785
D=-11434244 m=-2858561 vptor=11 Cp=0.9382920445879771130663980
D=-19227908 m=-4806977 vptor=11 Cp=0.9092149504336010969244116
```

```
p=2, Interval [10^8, 2*10^8]
```

```
D=-100000011 m=-100000011 vptor=2 Cp=0.15051499693318294862950
D=-100000020 m=-25000005 vptor=3 Cp=0.225772494296692430574969
(...)
D=-100000072 m=-25000018 vptor=3 Cp=0.225772487923331962924891
D=-100000120 m=-25000030 vptor=4 Cp=0.301029976053644338278634
(...)
D=-100000228 m=-25000057 vptor=4 Cp=0.301029958404363471726365
D=-100000324 m=-25000081 vptor=6 Cp=0.451544914074197327895496
(...)
D=-100009811 m=-100009811 vptor=6 Cp=0.45154258866246136591601
D=-100009988 m=-25002497 vptor=7 Cp=0.526799636159210448373252
(...)
D=-100042692 m=-25010673 vptor=9 Cp=0.677301796362621931199437
D=-100120215 m=-100120215 vptor=11 Cp=0.8277784989602807429303
D=-100703939 m=-100703939 vptor=11 Cp=0.8275173634473368234393
D=-101091716 m=-25272929 vptor=13 Cp=0.97777114254342282551717
D=-196241540 m=-49060385 vptor=13 Cp=0.94380528108729550144090
```


One sees some influence of genus theory since, for $D = -101091716$, we have $\mathcal{C}_{K,2} \approx 0.977771$ because of $\#\mathcal{T}_K = 2^{13}$, but to be put in relation with $\mathcal{C}_{K,2} \approx 0.982227$ for $D = -1347524$, of the first interval, with $\#\mathcal{T}_K = 2^{10}$.

The structure of the class group given by PARI/GP is $[1024, 2, 2, 2]$.

Then consider the program computing the structure of \mathcal{T}_K [18, Programme I, §3.2] that we recall for the convenience of the reader (choose p , nt such that p^{nt} be a multiple of the exponent of \mathcal{T}_K , then the polynomial P):

```
{p=3;nt=32;P=x^2+101091716;K=bnfinit(P,1);Kpn=bnrinit(K,p^nt);
S=component(component(Kpn,1),7);r=component(component(S,2),2)+1;
Hpn=component(component(Kpn,5),2);L=List;e=component(matsize(Hpn),2);
R=0;for(k=1,e-r,c=component(Hpn,e-k+1);if(Mod(c,p)==0,R=R+1;
listinsert(L,p^valuation(c,p),1));print("Structure of T: ",L)}
```

Then we obtain for \mathcal{T}_K the structure $[1024, 4, 2]$. The difference may be easily explained because $\mathcal{W}_K \simeq \mathbb{Z}/2\mathbb{Z}$ (indeed, $-101091716 \equiv -1 \pmod{16}$) and $[\tilde{K} \cap H_K : K] = 2$.

(a) Case $p = 3$.

```
{p=3;bd=10^6;BD=2*10^6;Lp=log(p);vp=0;n=8;
for(D=bD,BD,e=valuation(D,2);M=D/2^e;if(core(M)!=M,next);
if((e==1 || e>3)||(e==0 & Mod(M,4)!=-1)||(e==2 & Mod(M,4)==-1),next);
m=D;if(e!=0,m=D/4);P=x^2+m;K=bnfinit(P,1);Kpn=bnrinit(K,p^n);
C5=component(Kpn,5);Hpn0=component(C5,1);Hpn=component(C5,2);
Hpn1=component(Hpn,1);vptor=valuation(Hpn0/Hpn1,p)-(n-1);
if(vptor>vp,vp=vptor);if(vptor>vp,Cp=vptor*Lp/log(sqrt(D));
print("D=",D," m=",m," vptor=",vptor," Cp=",Cp))}
```

```
p=3, Interval [10^6, 2*10^6]
D=-1000011 m=-1000011 vptor=1 Cp=0.1590402916116620131420348520
D=-1000020 m=-250005 vptor=1 Cp=0.1590401880079362819278196125
D=-1000043 m=-1000043 vptor=1 Cp=0.1590399232477087416304663599
(...)
D=-1020548 m=-255137 vptor=3 Cp=0.4764198506806243371783107010
D=-1021332 m=-255333 vptor=4 Cp=0.6351912130796763789096457580
D=-1022687 m=-1022687 vptor=5 Cp=0.7939129439088033794338891302
(...)
D=-1898859 m=-1898859 vptor=5 Cp=0.7599296140003213455753306574

p=3, Interval [10^7, 10^7+10^6]
D=-10002927 m=-10002927 vptor=3 Cp=0.40895365007950900178024254

D=-10003224 m=-2500806 vptor=4 Cp=0.54527052902405852884991426
(...)
D=-10065279 m=-10065279 vptor=4 Cp=0.54506139909286008239956811
D=-10066440 m=-2516610 vptor=5 Cp=0.68132187532448910070906763
(...)
D=-14316744 m=-3579186 vptor=5 Cp=0.66675746065456780942779488
D=-14547531 m=-14547531 vptor=6 Cp=0.79933316809564910995167969
(...)
D=-19767512 m=-4941878 vptor=6 Cp=0.78474406738375920976115602
```

```

p=3, Interval [10^8, 10^8+10^7]
D=-100075971 m=-100075971 vptor=4 Cp=0.477101585455621088296257
D=-100080003 m=-100080003 vptor=5 Cp=0.596375677517090310811391
(...)
D=-100787315 m=-100787315 vptor=5 Cp=0.596147767754605081482216
D=-100867844 m=-25216961 vptor=6 Cp=0.715346318656502973478053
(...)
D=-117344127 m=-117344127 vptor=6 Cp=0.709521342553855083402930
D=-119846559 m=-119846559 vptor=7 Cp=0.826835890443221508331985
(...)
D=-135140024 m=-33785006 vptor=7 Cp=0.821531794828164970116186
D=-136159455 m=-136159455 vptor=8 Cp=0.938516745792290367614873

```

For $D_K = -136159455$, we get:

$$\mathcal{W}_K \simeq \mathbb{Z}/3\mathbb{Z}, \mathcal{T}_K \simeq \mathbb{Z}/3^7\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \text{ and } \mathcal{C}_K \simeq \mathbb{Z}/3^6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

(using the PARI/GP instruction `quadclassunit(-136159455)`).

4.3.3. Conclusion. Consider a prime p and a fixed degree d . Assume, tentatively, a strong ε -conjecture for the groups \mathcal{T}_K in the case of totally real number fields K of degree d , which implies a strong ε -conjecture for the p -class groups.

We then have:

$$\log(\#\mathcal{T}_K) \leq \log(\tilde{\mathcal{C}}_\varepsilon) + \varepsilon \cdot \log(\sqrt{D_K});$$

then introduce the variable $\mathcal{C}_{K,p}$:

$$(7) \quad \mathcal{C}_{K,p} := \frac{\log(\#\mathcal{T}_K)}{\log(\sqrt{D_K})} \leq \frac{\log(\tilde{\mathcal{C}}_\varepsilon)}{\log(\sqrt{D_K})} + \varepsilon.$$

So, when $D_K \rightarrow \infty$, we get $\mathcal{C}_{K,p} = \varepsilon + o(1)$. But in [12, § 5.3], we have proved that there exist explicit infinite families of real quadratic fields for which $\mathcal{C}_{K,p} \approx 1$ (contradiction). We obtain the following heuristic:

There is no strong ε -conjectures for the \mathcal{T}_K of totally real number fields K .

One can say that, in the totally real case, \mathcal{T}_K is essentially governed by the normalized p -adic regulator \mathcal{R}_K , which leaves the possibility of the existence of a strong ε -conjecture for the p -class groups. Recall that, from (5) and (6), the p -rank ε -conjecture for the \mathcal{T}_K does exist if and only if the p -rank ε -conjecture does exist for the p -class groups \mathcal{C}_K .

This is to be compared with the opposite case of the global class groups of imaginary quadratic fields for which $\#\mathcal{C}_K \sim \sqrt{D_K}$ for infinitely many fields.

4.4. Reflection theorem and p -rank ε -conjectures. Another justification of the above comments is to recall the reflection theorem [17] which exchanges, roughly speaking, p -class groups \mathcal{C} for “imaginary components” with p -torsion groups \mathcal{T} for “real components” and conversely, subject to consider fields K containing the group μ_p of p th roots of unity.

In full generality, the following result precises (5) and (6) when $\mu_p \subset K$:

Proposition 4.4 ([11, Theorem III.4.2.2]). *Let K be a number field containing μ_p and fulfilling Leopoldt's conjecture at p . Then we have the rank formula (reflection theorem)² $\mathrm{rk}_p(\mathcal{T}_K^{\mathrm{ord}}) = \mathrm{rk}_p(\mathcal{C}_K^{S,\mathrm{res}}) + \#S - 1$, where S is the set of p -places of K and $\mathcal{C}_K^{S,\mathrm{res}}$ the S -class group $\mathcal{C}_K^{\mathrm{res}}/\mathcal{c}^{\mathrm{res}}(S)$.*

So, $\mathrm{rk}_p(\mathcal{C}_K^{S,\mathrm{res}}) = \mathrm{rk}_p(\mathcal{T}_K^{\mathrm{ord}}) - (\#S - 1)$ yields, because of a relation in $\mathcal{c}^{\mathrm{res}}(S)$ due to the principality of the unique prime ideal of $\mathbb{Q}(\mu_p)$ dividing p :

$$\begin{aligned} \mathrm{rk}_p(\mathcal{C}_K^{\mathrm{res}}) &\leq \mathrm{rk}_p(\mathcal{C}_K^{S,\mathrm{res}}) + \mathrm{rk}_p(\mathcal{c}^{\mathrm{res}}(S)) \\ &\leq \mathrm{rk}_p(\mathcal{T}_K^{\mathrm{ord}}) - [(\#S - 1) - \mathrm{rk}_p(\mathcal{c}^{\mathrm{res}}(S))] \leq \mathrm{rk}_p(\mathcal{T}_K^{\mathrm{ord}}), \end{aligned}$$

giving:

$$\begin{aligned} \mathrm{rk}_p(\mathcal{T}_K^{\mathrm{ord}}) - (\#S - 1) &\leq \mathrm{rk}_p(\mathcal{C}_K^{\mathrm{res}}) \leq \mathrm{rk}_p(\mathcal{T}_K^{\mathrm{ord}}), \\ \mathrm{rk}_p(\mathcal{C}_K^{\mathrm{res}}) &\leq \mathrm{rk}_p(\mathcal{T}_K^{\mathrm{ord}}) \leq \mathrm{rk}_p(\mathcal{C}_K^{\mathrm{res}}) + (\#S - 1), \end{aligned}$$

since $\#S - 1$ is fortunately bounded for the family of number fields, of fixed degree d , containing μ_p , these relations shows that any p -rank ε -conjecture, true for an invariant, is fulfilled by the other. When $\mu_p \not\subset K$, one must use the field $K(\mu_p)$ and the general reflection theorem with p -adic characters ([11, Theorem II.5.4.5], [17]).

The reflection theorem has been used in [6], in a different manner, using many split primes in $K(\mu_p)$, the notion of Arakelov class group (see e.g., [31]) and the following analytic explanation by the authors:

Roughly, the point is that small non-inert primes in a number field represent elements of the class group which tend not to satisfy any relation with small coefficients. Thus the existence of many such primes contributes significantly to the quotient of the class group by its ℓ -torsion, yielding the desired upper bounds.

It would be interesting to deepen these approaches that have connections through class field theory, complex and p -adic analytic methods.

References

- [1] ADAM, M.; MALLE, G. A class group heuristic based on the distribution of 1-eigenspaces in matrix groups, *J. Number Theory* **149** (2015), 225–235. [MR3296009](#) [Zbl 1371.11145](#)
- [2] CHEVALLEY, C. Sur la théorie du corps de classes dans les corps finis et les corps locaux, *Jour. of the Fac. of Sc., Tokyo, Sec. I*, **2** (1933), 365–476. [Zbl 0008.05301](#)
- [3] COHEN, H.; LENSTRA JR., H.W. Heuristics on class groups of number fields, *In Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, 33–62, Lecture Notes in Math. **1068**, Springer, Berlin, 1984. [MR0756082](#) [Zbl 0558.12002](#)
- [4] COHEN, H.; MARTINET, J. Étude heuristique des groupes de classes des corps de nombres, *Journal für die Reine und Angewandte Mathematik* **404** (1990), 39–76. [MR1037430](#) [Zbl 0699.12016](#) <https://eudml.org/doc/153196>

²The mentions “ord”, “res” are related to the case $p = 2$; for $p > 2$, since $\mu_p \subset K$, the two notions coincide.

- [5] ELLENBERG, J.S.; PIERCE, L.B.; WOOD, M.M. On ℓ -torsion in class groups of number fields (preprint 2017). <https://arxiv.org/abs/1606.06103v2>
- [6] ELLENBERG, J.S.; VENKATESH, A. Reflection principles and bounds for class group torsion, *Int. Math. Res. Not.* **2007** (2007), no. 1. MR2331900 Zbl 1130.11060 <https://doi.org/10.1093/imrn/rnm002>
- [7] FRÖHLICH, A. The generalization of a theorem of L. Rédei's, *Qart. Jour. of math. Oxford* **2** (1954), no. 5, 13–140. Zbl 0058.26903 <https://doi.org/10.1093/qmath/5.1.130>
- [8] FRÖHLICH, A. The genus field and genus group in finite number fields I, *Mathematika* **6** (1959), 40–46. MR0113868 Zbl 0202.33005 <https://doi.org/10.1112/S0025579300001911>
- [9] FURUTA, Y. The genus field and genus number in algebraic number fields, *Nagoya Math. J.* **29** (1967), 281–285. MR0209260 Zbl 0166.05901 <https://doi.org/10.1017/S0027763000024387>.
- [10] FREI, C.; WIDMER, M. Average bounds for the p -torsion in class groups of cyclic extensions (2018). <https://arxiv.org/abs/1709.09934>.
- [11] GRAS, G. Class Field Theory: from theory to practice, corr. 2nd ed., *Springer Monographs in Mathematics*, Springer (2005), xiii+507 pages. MR1941965 Zbl 1019.11032 <https://doi.org/10.1007/978-3-662-11323-3>
- [12] GRAS, G. Heuristics and conjectures in direction of a p -adic Brauer–Siegel theorem, *Math. Comp.* (2018). <https://doi.org/10.1090/mcom/3395>
- [13] GRAS, G. Invariant generalized ideal classes – structure theorems for p -class groups in p -extensions, *Proc. Indian Acad. Sci. Math. Sci.* **127** (2017), no. 1, 1–34. MR3605238 Zbl 06731203 <https://doi.org/10.1007/s12044-016-0324-1>
- [14] GRAS, G. Sur les p -classes d'idéaux dans les extensions cycliques relatives de degré premier p , I, *Annales de l'Institut Fourier* **23** (1973), no. 3, 1–48. MR360519 Zbl 0276.12013 <https://doi.org/10.5802/aif.471>
- [15] GRAS, G. Sur les p -classes d'idéaux dans les extensions cycliques relatives de degré premier p , II, *Annales de l'Institut Fourier* **23** (1973), no. 4, 1–44. MR360519 Zbl 0276.12013 <https://doi.org/10.5802/aif.480>
- [16] GRAS, G. The p -adic Kummer-Leopoldt Constant: Normalized p -adic Regulator, *Int. J. Number Theory* **14** (2018), no. 2, 329–337. MR3761496 Zbl 1393.11071 <https://doi.org/10.1142/S1793042118500203>
- [17] GRAS, G. Théorèmes de réflexion, *J. Théor. Nombres Bordeaux* **10** (1998), no. 2, 399–499. MR1828251 Zbl 0949.11058 http://www.numdam.org/item/JTNB_1998__10_2_399_0/
- [18] GRAS, G. On p -rationality of number fields. Applications – PARI/GP programs, *Publ. Math. Fac. Sci. Besançon (Théorie des Nombres)*, Années 2017/2018 (to appear). <https://arxiv.org/pdf/1709.06388.pdf>
- [19] GRAS, G. Les θ -régulateurs locaux d'un nombre algébrique : Conjectures p -adiques, *Canadian Journal of Mathematics* **68** (2016), no. 3, 571–624. <http://dx.doi.org/10.4153/CJM-2015-026-3> MR3492629 Zbl 1351.11033
- [20] INABA, E. Über die Struktur der ℓ -klassengruppe zyklischer Zahlkörper von Primzahlgrad ℓ , *J. Fac. Sci. Univ. Tokyo, Sect. I* **4** (1940), 61–115. Zbl 0024.01002
- [21] JAULENT, J.-F. Théorie ℓ -adique globale du corps de classes, *J. Théorie des Nombres de Bordeaux* **10** (1998), no. 2, 355–397. http://www.numdam.org/article/JTNB_1998__10_2_355_0.pdf MR1828250 Zbl 0938.11052
- [22] JAULENT, J.-F. Unités et classes dans les extensions métabéliennes de degré np^s sur un corps de nombres algébriques, *Ann. Inst. Fourier (Grenoble)* **31** (1981), no. 1, ix–x, 39–62. MR0613028 Zbl 0436.12007 http://www.numdam.org/article/AIF_1981__31_1_39_0.pdf/

- [23] MAIRE, C. Genus theory and governing fields, *New York J. Math.* **24** (2018), 1056–1067. Zbl 06982028 <http://nyjm.albany.edu/j/2018/24-50.html>
- [24] MALLE, G. On the distribution of class groups of number fields, *Experiment. Math.* **19** (2010), 465–474. MR2011m:11224 Zbl 1297.11139
- [25] MAYNAR, J. On the Brun–Titchmarsh theorem, *Acta Arithmetica* **157** (2013), No. 3, 249–296. MR3019418 Zbl 1321.11099
- [26] The PARI Group, PARI/GP, version 2.9.0, *Université de Bordeaux* (2016). <http://pari.math.u-bordeaux.fr/>
- [27] PIERCE, L.B.; TURNAGE-BUTTERBAUGH, C.L.; WOOD, M.M. On a conjecture for p -torsion in class groups of number fields: from the perspective of moments (2019). <https://arxiv.org/abs/1902.02008>
- [28] RAZAR, M.J. Central and genus class fields and the Hasse norm theorem, *Compositio Math.* **35** (1977), no. 3, 281–298. MR0466073 Zbl 0376.12006 http://www.numdam.org/item?id=CM_1977__35_3_281_0.1057
- [29] REDEI, L.; REICHARDT, H. Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *J. f.d.r.u.a. Math.* **170** (1933). Zbl 0007.39602
- [30] SCHOOF, R. Class numbers of real cyclotomic fields of prime conductor, *Math. Comp.* **72** (2003), no. 242, 913–937. MR1954975 Zbl 1052.11071 <https://doi.org/10.1090/S0025-5718-02-01432-1>
- [31] SCHOOF, R. Minus class groups of the fields of the ℓ -th roots of unity, *Math. Comp.* **67** (1998), no. 67, 1225–1245. MR1458225 Zbl 0902.11043 <http://www.mat.uniroma2.it/~schoof/minus.pdf>
- [32] SCHOOF, R. Computing Arakelov class groups, Buhler, J.P. (ed.) et al., Algorithmic Number Theory, *Cambridge University Press, MSRI Publications* **44** (2008), 447–495. MR2467554 Zbl 1188.11076 <https://www.mat.uniroma2.it/~schoof/14schoof.pdf>
- [33] TENENBAUM, G. Introduction à la théorie analytique et probabiliste des nombres, 3^e édition revue et augmentée, *Coll. Échelles*, Belin 2008.
- [34] TSFASMAN, M.; VLADUȚ, S. Infinite global fields and the generalized Brauer–Siegel theorem, Dedicated to Yuri I. Manin on the occasion of his 65th birthday, *Moscow Math. J.* **2** (2002), no. 2, 329–402. MR1944510 Zbl 1004.11037 <http://www.ams.org/distribution/mmj/vol2-2-2002/tsfasman-vladuts.pdf>
- [35] WASHINGTON, L.C. Introduction to cyclotomic fields, GTM **83**, *Springer-Verlag, New York* 1997, xiv+487 pp. MR1421575 Zbl 0484.12001
- [36] WIDMER, M. Bounds for the p -torsion in class groups, *Bull. Lond. Math. Soc.* **50** (2018), 124–13. <https://doi.org/10.1112/blms.12113>
- [37] ZYKIN, A.I. Brauer–Siegel and Tsfasman–Vladuț theorems for almost normal extensions of global fields, *Moscow Math. J.* **5** (2005), no. 4, 961–968. MR2267316 Zbl 1125.11062 <http://www.ams.org/distribution/mmj/vol5-4-2005/zykin.pdf>

VILLA LA GARDETTE, 4 CHEMIN CHÂTEAU GAGNIÈRE, F-38520, LE BOURG D’OISANS.
g.mn.gras@wanadoo.fr