

# PRACTICE OF INCOMPLETE $p$ -RAMIFICATION OVER A NUMBER FIELD

## APPENDIX: HISTORY OF ABELIAN $p$ -RAMIFICATION

GEORGES GRAS

ABSTRACT. The theory of  $p$ -ramification, regarding the Galois group of the maximal pro- $p$ -extension of a number field  $K$ , unramified outside  $p$  and  $\infty$ , is well known including numerical experiments with PARI/GP programs. The case of “incomplete  $p$ -ramification” (i.e., when the set  $S$  of ramified places is a strict subset of the set  $P$  of the  $p$ -places) is, on the contrary, mostly unknown in a theoretical point of view. We give, in a first part, a way to compute, for any  $S \subseteq P$ , the structure of the maximal  $S$ -ramified *abelian* pro- $p$ -extension  $H_{K,S}$  of any field  $K$  given by means of an irreducible polynomial. We publish PARI/GP programs usable without any special prerequisites. Then, in the Appendix, we recall the “story” of abelian  $S$ -ramification restricting ourselves to elementary aspects in order to precise much basic contributions and references, often disregarded, which may be used by specialists of other domains of number theory. Indeed, the torsion  $\mathcal{T}_{K,S}$  of  $\text{Gal}(H_{K,S}/K)$  (even if  $S = P$ ) is a fundamental obstruction in many problems. All relationships involving  $S$ -ramification, as Iwasawa’s theory, Galois cohomology,  $p$ -adic  $L$ -functions, elliptic curves, algebraic geometry, would merit special developments, which is not the purpose of this text.

### CONTENTS

1. Introduction and basic results	3
1.1. Notion of Galois $S$ -ramification	3
1.2. Main cohomological invariants	3
1.3. Class field theory	3
2. General $p$ -adic context of $S$ -ramification	5
2.1. Fundamental exact sequences	5
2.2. Diagram of $S$ -ramification	6
2.3. Local computations	6
2.4. Practical computation of $\tilde{r}_{K,S}$	7

---

*Date:* May 12, 2019.

1991 *Mathematics Subject Classification.* Primary 11R37; Secondary 11F85; 11R34; 11Y40.

*Key words and phrases.* Abelian  $S$ -ramification; class field theory;  $p$ -adic regulators; Leopoldt’s conjecture; class groups, units, pro- $p$ -groups,  $\mathbb{Z}_p$ -extensions.

3. Algorithmic approach of $S$ -ramification	8
3.1. Main program computing $\mathcal{T}_{K,S}$ and $\tilde{r}_{K,S}$	8
3.1.1. The PARI/GP program	8
3.1.2. Instructions for use	8
3.1.3. Example with $p$ totally split in degree 5	12
3.1.4. Example with $p$ totally split in degree 7	13
3.1.5. Example with a field discovered by Jaulent–Sauzet	13
3.1.6. Abelian fields with $\mathcal{T}_{K,S} = 1$ but $\mathcal{T}_{K,P} \neq 1$	14
3.2. Experiments with the fields $K = \mathbb{Q}(\sqrt[p]{N})$	15
3.3. The fields $K = \mathbb{Q}(\sqrt{-\sqrt{-q}})$ associated to elliptic curves	17
3.3.1. Program for various $p$	17
3.3.2. Program for various $q$ and $p = 2$	18
Appendix A. History of abelian $p$ -ramification	20
A.1. Motivations	20
A.2. Prehistory	21
A.2.1. Šafarevič formula	22
A.2.2. Kubota formalism	22
A.3. Main developments after the pioneering works	22
A.3.1. Reflection and rank formulas	22
A.3.2. Regulators and $p$ -adic residues of the $\zeta_p$ -functions	24
A.3.3. Cohomological interpretation	25
A.3.4. Principal Conjectures and Theorems	25
A.4. Basic $p$ -adic properties of $\mathcal{A}_{K,P}$ & $\mathcal{T}_{K,P}$	25
A.4.1. The $p$ -adic $\text{Log}_S$ -functions	25
A.4.2. Fixed point formula	26
A.4.3. $p$ -primitive ramification	27
A.5. New formalisms and use of pro- $p$ -group theory	27
A.5.1. Infinitesimal arithmetic	27
A.5.2. Pro- $p$ -group theory version	28
A.5.3. Synthesis 2003–2005	29
A.6. Present theoretical and algorithmic aspects	29
A.6.1. Absolute abelian Galois group $A_K$ of $K$	29
A.6.2. Greenberg’s conjecture on Iwasawa’s $\lambda, \mu$	30
A.6.3. Galois representations with open image	30
A.6.4. Order of magnitude of $\mathcal{T}_{K,P}$ and conjectures	31
A.6.5. Fermat curves	32
A.7. Computational references and numerical tables	32
A.8. Conclusion and open questions	34
Acknowledgments	35
References	35

## 1. INTRODUCTION AND BASIC RESULTS

**1.1. Notion of Galois  $S$ -ramification.** Let  $p \geq 2$  be a prime number and let  $K$  be a number field; we denote by  $P := \{\mathfrak{p} \text{ prime, } \mathfrak{p} | p\}$  the set of  $p$ -places of  $K$  and by  $S$  an arbitrary set of finite places (later we shall assume  $S \subseteq P$ ).

A main problem in Galois theory above  $K$  is to study the Galois group  $\mathcal{G}_{K,S}$  of the maximal pro- $p$ -extension of  $K$  which is  $S$ -ramified in the ordinary sense (i.e., unramified outside  $S$  and non-complexified (= totally split) at the real infinite places of  $K$  when  $p = 2$ ).

As we will recall it in detail, in Section A.1, the study of  $\mathcal{G}_{K,S}$  goes back to fundamental contributions of Serre [Ser64], Šafarevič [Sha64], Brumer [Bru66], and has been largely extended, from the 1980's, in much works considering  $S$ -ramification (eventually with decomposition of another set  $\Sigma$  of finite and infinite places).

The analogous theory for a local base field has also a long history that we shall not consider in this article.

**1.2. Main cohomological invariants.** For complete current information about the “cohomology of number fields”, see [NSW00, Chapter X].

When  $S = P$ , the  $\mathbb{F}_p$ -dimension of  $H^1(\mathcal{G}_{K,P}, \mathbb{Z}/p\mathbb{Z})$ , which gives the minimal number of generators of  $\mathcal{G}_{K,P}$ , is the  $p$ -rank<sup>1</sup> of the abelianization:

$$\mathcal{A}_{K,P} := \mathcal{G}_{K,P}^{\text{ab}} := \mathcal{G}_{K,P} / [\mathcal{G}_{K,P}, \mathcal{G}_{K,P}].$$

Denote by  $(r_1, r_2)$  the signature of  $K$  (whence  $r_1 + 2r_2 = [K : \mathbb{Q}]$ ); then, the  $\mathbb{F}_p$ -dimension of  $H^2(\mathcal{G}_{K,P}, \mathbb{Z}/p\mathbb{Z})$ , which gives the minimal number of relations between these generators, fulfills the identity:

$$\text{rk}_p(H^1(\mathcal{G}_{K,P}, \mathbb{Z}/p\mathbb{Z})) = \text{rk}_p(H^2(\mathcal{G}_{K,P}, \mathbb{Z}/p\mathbb{Z})) + r_2 + 1,$$

giving, for the torsion group  $\mathcal{T}_{K,P}$  of  $\mathcal{A}_{K,P}$  under Leopoldt's conjecture:

$$\text{rk}_p(\mathcal{T}_{K,P}) = \text{rk}_p(H^2(\mathcal{G}_{K,P}, \mathbb{Z}/p\mathbb{Z})).$$

**1.3. Class field theory.** In the general case for  $S$  (possibly containing tame places and not all the  $p$ -places) we may write:

$$(1.1) \quad \mathcal{A}_{K,S} = \Gamma_{K,S} \oplus \mathcal{T}_{K,S}, \text{ with } \Gamma_{K,S} \simeq \mathbb{Z}_p^{\tilde{r}_{K,S}},$$

where  $\mathcal{T}_{K,S} := \text{tor}_{\mathbb{Z}_p}(\mathcal{A}_{K,S})$  and  $\tilde{r}_{K,S} \geq 0$ .

Without any  $p$ -adic assumption on the group of global units of  $K$ , we still have  $\text{rk}_p(H^1(\mathcal{G}_{K,S}, \mathbb{Z}/p\mathbb{Z})) = \text{rk}_p(\mathcal{A}_{K,S})$ , but  $\tilde{r}_{K,S}$  (called the  $\mathbb{Z}_p$ -rank of  $\mathcal{A}_{K,S}$ ) is more difficult when  $S \subsetneq P$ ; however,  $\text{rk}_p(\mathcal{A}_{K,S}) = \tilde{r}_{K,S} + \text{rk}_p(\mathcal{T}_{K,S})$  is computable in complete generality with the invariants of class field theory for  $K$  as follows (Šafarevič formula):

---

<sup>1</sup> As usual, the  $p$ -rank of an abelian group  $A$  is the  $\mathbb{F}_p$ -dimension of  $A/A^p$ .

Let  $K_{(S)}^\times$  be the subgroup of  $K^\times$  of elements prime to  $S$  and for any  $\mathfrak{p} \in S$ , let  $K_{\mathfrak{p}}$  be the completion of  $K$  at  $\mathfrak{p}$ ; then:

$$(1.2) \quad \begin{aligned} \mathrm{rk}_p(\mathcal{A}_{K,S}) &= \mathrm{rk}_p(V_{K,S}/K_{(S)}^{\times p}) \\ &+ \sum_{\mathfrak{p} \in S \cap P} [K_{\mathfrak{p}} : \mathbb{Q}_p] + \sum_{\mathfrak{p} \in S} \delta_{\mathfrak{p}} - \delta_K - (r_1 + r_2 - 1), \end{aligned}$$

where  $V_{K,S} := \{\alpha \in K_{(S)}^\times, (\alpha) = \mathfrak{a}^p \text{ for an ideal } \mathfrak{a} \text{ of } K\}$ ,  $\delta_{\mathfrak{p}} = 1$  or  $0$  according as  $K_{\mathfrak{p}}$  contains  $\mu_p$  or not, and  $\delta_K = 1$  or  $0$  according as  $K$  contains  $\mu_p$  or not. Thus:

$$(1.3) \quad \begin{aligned} \mathrm{rk}_p(\mathcal{T}_{K,S}) &= \mathrm{rk}_p(\mathcal{A}_{K,S}) - \tilde{r}_{K,S} = \mathrm{rk}_p(V_{K,S}/K_{(S)}^{\times p}) \\ &+ \sum_{\mathfrak{p} \in S \cap P} [K_{\mathfrak{p}} : \mathbb{Q}_p] - \tilde{r}_{K,S} + \sum_{\mathfrak{p} \in S} \delta_{\mathfrak{p}} - \delta_K - (r_1 + r_2 - 1), \end{aligned}$$

where  $\tilde{r}_{K,S}$  defined by (1.1) fulfills the following formula:

$$(1.4) \quad \sum_{\mathfrak{p} \in S \cap P} [K_{\mathfrak{p}} : \mathbb{Q}_p] - \tilde{r}_{K,S} = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \log_{S \cap P}(E_K)),$$

where  $E_K$  is the group of global units of  $K$  and  $\log_{S \cap P} := (\log_{\mathfrak{p}})_{\mathfrak{p} \in S \cap P}$  the family of  $p$ -adic logarithms over  $S \cap P$  with values in  $\bigoplus_{\mathfrak{p} \in S \cap P} K_{\mathfrak{p}}$ . Note that for  $S = P$ ,  $r_{K,P} := \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \log_P(E_K))$  is the  $p$ -adic rank of  $E_K$  (i.e., the  $\mathbb{Z}_p$ -rank of the closure of the image  $\iota_P(E_K)$  of  $E_K$  in  $U_{K,P}$ , see § 2.1).

The Šafarevič and reflection formulas, generalized with decomposition, may be obtained via [Gra03, Exercise II.5.4.1] or other classical references.

In general,  $\tilde{r}_{K,S}$  is non-obvious and varies from  $0$  to  $r_2 + 1$  (see [Win89, Win91, Yam93, Mai02, Mai03, Mai05, Lab06, Vog07] for some results and cases where  $\mathcal{G}_{K,S}$  may be free with less than  $r_2 + 1$  generators and our forthcoming numerical results showing that many  $\mathbb{Z}_p$ -ranks can occur).

For  $S = P$  we obtain  $\tilde{r}_{K,P} = r_2 + 1$ , under the Leopoldt conjecture, giving (since  $\sum_{\mathfrak{p} \in P} [K_{\mathfrak{p}} : \mathbb{Q}_p] = r_1 + 2r_2$ ):

$$(1.5) \quad \mathrm{rk}_p(\mathcal{T}_{K,P}) = \mathrm{rk}_p(V_{K,P}/K_P^{\times p}) + \sum_{\mathfrak{p} \in P} \delta_{\mathfrak{p}} - \delta_K.$$

If  $S = \emptyset$  then  $\mathcal{A}_{K,S} = \mathcal{T}_{K,S} =: \mathcal{C}_K$ , the  $p$ -class group of  $K$  (ordinary sense).

**Remark 1.1.** We shall not consider  $S$ -ramification with  $S = P \cup T$ , when  $T$  is a finite set of tame places, because of the following exact sequence, *under the Leopoldt conjecture* ([Neu75], [Nqd86, Corollary 4.3], [Gra03, Theorem III.4.1.5]), where the  $F_t$  are the residue fields:

$$1 \longrightarrow \bigoplus_{t \in T} (F_t^\times \otimes \mathbb{Z}_p) \longrightarrow \mathcal{T}_{K,P \cup T} \longrightarrow \mathcal{T}_{K,P} \longrightarrow 1.$$

For some specialized applications (about number fields, elliptic curves, representation theory, Galois cohomology, Iwasawa's theory,  $p$ -adic  $L$ -functions) and some recent conjectures, one needs to study and compute the above  $S$ -invariants when  $S$  is a subset of  $P$  and  $K/\mathbb{Q}$  not necessarily Galois.

So the most tricky invariants of “incomplete  $P$ -ramification” are  $\mathcal{T}_{K,S}$  and  $\tilde{r}_{K,S} = \text{rk}_p(\mathcal{A}_{K,S}) - \text{rk}_p(\mathcal{T}_{K,S}) = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \log_S(E_K))$ . Of course, they highly depend on the decomposition of the prime  $p$  in the Galois closure of  $K$ .

## 2. GENERAL $p$ -ADIC CONTEXT OF $S$ -RAMIFICATION

Consider a number field  $K$  and a given prime  $p \geq 2$ . Let  $S$  be a subset of the set  $P$  of the  $p$ -places of  $K$  and let  $H_{K,S}$  be the maximal *abelian*  $S$ -ramified pro- $p$ -extension of  $K$ ; this field contains a (maximal) compositum  $\widetilde{K}^S$  of  $\mathbb{Z}_p$ -extensions of  $K$  and always the  $p$ -Hilbert class field  $H_K := H_{K,\emptyset}$  of  $K$ . These definitions are given in the ordinary sense when  $p = 2$  (so that the real infinite places of  $K$  are not complexified in the class fields considered; in other words they are totally split).

**2.1. Fundamental exact sequences.** Let  $U_{K,S} := \bigoplus_{\mathfrak{p} \in S} U_{\mathfrak{p}}$ , be the product of the groups of principal local units of  $K_{\mathfrak{p}}$ ,  $\mathfrak{p} \in S$ , and let  $\overline{E}_K^S$  be the closure of the image  $\iota_S(E_K)$  of  $E_K$  in  $U_{K,S}$ . We denote by  $W_{K,S} = \bigoplus_{\mathfrak{p} \in S} \mu_{K_{\mathfrak{p}}}$  the torsion group of the  $\mathbb{Z}_p$ -module  $U_{K,S}$ .

If  $K/\mathbb{Q}$  is Galois and  $S \subsetneq P$ ,  $U_{K,S}$  is not necessarily a Galois module.

The following  $p$ -adic result is valid without any assumption on  $K$  and  $S \subseteq P$ :

**Lemma 2.1.** *We have the exact sequence:*

$$1 \rightarrow W_{K,S}/\text{tor}_{\mathbb{Z}_p}(\overline{E}_K^S) \longrightarrow \text{tor}_{\mathbb{Z}_p}(U_{K,S}/\overline{E}_K^S) \\ \xrightarrow{\log_S} \text{tor}_{\mathbb{Z}_p}(\log_S(U_{K,S})/\log_S(\overline{E}_K^S)) \rightarrow 0.$$

*Proof.* Put  $\log := \log_S$ . The surjectivity comes from the fact that if  $u \in U_{K,S}$  is such that  $p^n \log(u) = \log(\bar{\varepsilon})$ ,  $\bar{\varepsilon} \in \overline{E}_K^S$ , then  $u^{p^n} = \bar{\varepsilon} \cdot \xi$  for  $\xi \in W_{K,S}$ , hence there exists  $m \geq n$  such that  $u^{p^m} \in \overline{E}_K^S$ , whence  $u$  gives a preimage in  $\text{tor}_{\mathbb{Z}_p}(U_{K,S}/\overline{E}_K^S)$ . If  $u \in U_{K,S}$  is such that  $\log(u) \in \log(\overline{E}_K^S)$ , then  $u = \bar{\varepsilon} \cdot \xi$  as above, giving the kernel equal to  $\overline{E}_K^S \cdot W_{K,S}/\overline{E}_K^S = W_{K,S}/\text{tor}_{\mathbb{Z}_p}(\overline{E}_K^S)$ .  $\square$

Put  $\mathcal{W}_{K,S} := W_{K,S}/\text{tor}_{\mathbb{Z}_p}(\overline{E}_K^S)$  and  $\mathcal{R}_{K,S} := \text{tor}_{\mathbb{Z}_p}(\log_S(U_{K,S})/\log_S(\overline{E}_K^S))$ . Then the exact sequence of Lemma 2.1 becomes:

$$(2.1) \quad 1 \longrightarrow \mathcal{W}_{K,S} \longrightarrow \text{tor}_{\mathbb{Z}_p}(U_{K,S}/\overline{E}_K^S) \xrightarrow{\log_S} \mathcal{R}_{K,S} \longrightarrow 0.$$

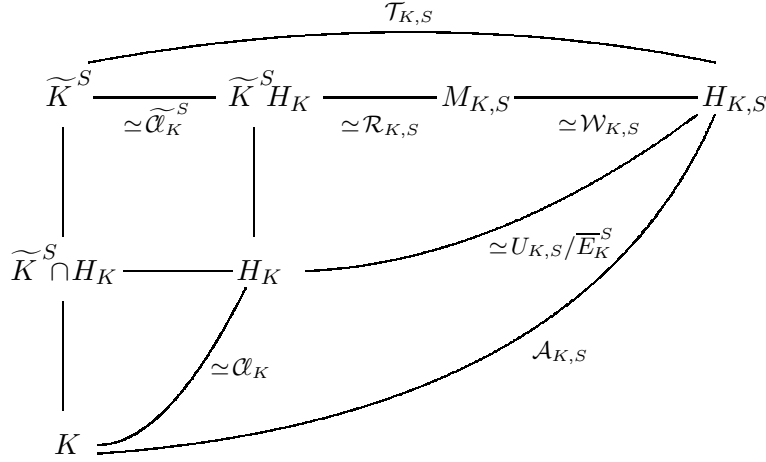
**Lemma 2.2.** *Let  $\mu_K$  be the group of roots of unity of  $p$ -power order of  $K$ . Under the Leopoldt conjecture for  $p$  in  $K$  we have  $\text{tor}_{\mathbb{Z}_p}(\overline{E}_K^P) = \iota_P(\mu_K)$ ; thus, in that case,  $\mathcal{W}_{K,P} = W_{K,P}/\iota_P(\mu_K)$ .*

*Proof.* From [Jau98, Définition 2.11, Proposition 2.12] or [Gra03, Theorem III.3.6.2 (vi)].  $\square$

Note that for  $S \subsetneq P$ , we do not know if  $\text{tor}_{\mathbb{Z}_p}(\overline{E}_K^S)$  may be larger than  $\iota_S(\mu_K)$  (as subgroups of  $W_{K,S}$ ), even under the Leopoldt conjecture.

**2.2. Diagram of  $S$ -ramification.** Consider the following diagram under the Leopoldt conjecture for  $p$  in  $K$ . By definition,  $\mathcal{T}_{K,S} = \text{tor}_{\mathbb{Z}_p}(\mathcal{A}_{K,S})$  is the Galois group  $\text{Gal}(H_{K,S}/\widetilde{K}^S)$ ; let  $\widetilde{\mathcal{C}}_K^S$  be the subgroup of  $\mathcal{C}_K$  corresponding to  $\text{Gal}(H_K/\widetilde{K}^S \cap H_K)$  by class field theory. Then from the schema we get:

$$(2.2) \quad \begin{aligned} \#\mathcal{T}_{K,S} &= [H_K:\widetilde{K}^S \cap H_K] \cdot \#\text{tor}_{\mathbb{Z}_p}(U_{K,S}/\overline{E}_K^S) \\ &= \#\widetilde{\mathcal{C}}_K^S \cdot \#\mathcal{R}_{K,S} \cdot \#\mathcal{W}_{K,S}. \end{aligned}$$



Of course, for  $p \geq p_0$  (explicit),  $\#\mathcal{W}_{K,S} = \widetilde{\mathcal{C}}_K^S = 1$ , whence  $\mathcal{T}_{K,S} = \mathcal{R}_{K,S}$ .

**Remark 2.3.** When  $S = P$ , we have  $\text{Gal}(H_{K,P}/H_K) \simeq U_{K,P}/\overline{E}_K^P$ , in which the image of  $\mathcal{W}_{K,P}$  fixes  $M_{K,P} =: H_K^{\text{bp}}$ , the Bertrandias–Payan field,  $\text{Gal}(H_K^{\text{bp}}/\widetilde{K}^P)$  being the Bertrandias–Payan module as named by Nguyen Quang Do from the results of [BP72] on the  $p$ -cyclic embedding problem. Then  $\mathcal{R}_{K,P} \simeq \text{Gal}(H_K^{\text{bp}}/\widetilde{K}^P H_K)$ . This “normalized regulator”  $\mathcal{R}_{K,P}$  (as  $p$ -group or as a  $p$ -power) is closely related to the classical  $p$ -adic regulator of  $K$  (see [Gra18a, Proposition 5.2]).

**2.3. Local computations.** Recall the following local computation:

**Theorem 2.4.** [Gra03, Theorem I.4.5 & Corollary I.4.5.4, ordinary sense]. For  $\mathfrak{p} \mid p$  in  $K$  and  $j \geq 1$ , let  $U_{\mathfrak{p}}^j$  be the group of local units  $1 + \overline{\mathfrak{p}}^j$ , where  $\overline{\mathfrak{p}}$  is the maximal ideal of the ring of integers of  $K_{\mathfrak{p}}$ . For  $S \subseteq P$ , denote by  $\mathfrak{m}(S)$  the modulus  $\prod_{\mathfrak{p} \in S} \mathfrak{p}$ . Let  $e_{\mathfrak{p}}$  be the ramification index of  $\mathfrak{p}$  in  $K/\mathbb{Q}$ .

For a modulus of the form  $\mathfrak{m}(S)^n$ ,  $n \geq 0$ , let  $\mathcal{C}_K(\mathfrak{m}(S)^n)$  be the corresponding ray class group (ordinary sense). Then for  $m \geq n \geq 0$ , we have:

$$0 \leq \text{rk}_p(\mathcal{C}_K(\mathfrak{m}(S)^m)) - \text{rk}_p(\mathcal{C}_K(\mathfrak{m}(S)^n)) \leq \sum_{\mathfrak{p} \in S} \text{rk}_p((U_{\mathfrak{p}}^1)^p U_{\mathfrak{p}}^{n \cdot e_{\mathfrak{p}}}/(U_{\mathfrak{p}}^1)^p U_{\mathfrak{p}}^{m \cdot e_{\mathfrak{p}}}).$$

**Corollary 2.5.** [Gra17c, Theorem 2.1 & Corollary 2.2] *We have:*

$\mathrm{rk}_p(\mathcal{C}_K(\mathfrak{m}(S)^m)) = \mathrm{rk}_p(\mathcal{C}_K(\mathfrak{m}(S)^n)) = \mathrm{rk}_p(\mathcal{A}_{K,S})$ , for all  $m \geq n \geq n_0$ ,  
 where  $n_0 = 3$  for  $p = 2$  and  $n_0 = 2$  for  $p > 2$ .  
 Thus  $\mathcal{T}_{K,S} = 1$  if and only if  $\mathrm{rk}_p(\mathcal{C}_K(\mathfrak{m}(S)^{n_0})) = \tilde{r}_{K,S}$  ( $\mathbb{Z}_p$ -rank of  $\mathcal{A}_{K,S}$ ).

*Proof.* It is sufficient to get, for some fixed  $n \geq 0$ :

$$(U_{\mathfrak{p}}^1)^p U_{\mathfrak{p}}^{n \cdot e_{\mathfrak{p}}} = (U_{\mathfrak{p}}^1)^p, \text{ for all } \mathfrak{p} \in S,$$

hence  $U_{\mathfrak{p}}^{n \cdot e_{\mathfrak{p}}} \subseteq (U_{\mathfrak{p}}^1)^p$  for all  $\mathfrak{p} \in S$ ; indeed, we then have:

$$\mathrm{rk}_p(\mathcal{C}_K(\mathfrak{m}(S)^n)) = \mathrm{rk}_p(\mathcal{C}_K(\mathfrak{m}(S)^m)) = \tilde{r}_{K,S} + \mathrm{rk}_p(\mathcal{T}_{K,S}) \text{ as } m \rightarrow \infty,$$

giving  $\mathrm{rk}_p(\mathcal{C}_K(\mathfrak{m}(S)^n)) = \tilde{r}_{K,S} + \mathrm{rk}_p(\mathcal{T}_{K,S})$  for such  $n$ .

The condition  $U_{\mathfrak{p}}^{n \cdot e_{\mathfrak{p}}} \subseteq (U_{\mathfrak{p}}^1)^p$  is fulfilled as soon as  $n \cdot e_{\mathfrak{p}} > \frac{p \cdot e_{\mathfrak{p}}}{p-1}$ , whence  $n > \frac{p}{p-1}$  [FV02, Chapter I, § 5.8, Corollary 2] giving the value of  $n_0$ ; furthermore,  $\mathcal{C}_K(\mathfrak{m}(S)^{n_0})$  gives the  $p$ -rank of  $\mathcal{T}_{K,S}$  as soon as the  $\mathbb{Z}_p$ -rank  $\tilde{r}_{K,S}$  is known.  $\square$

**2.4. Practical computation of  $\tilde{r}_{K,S}$ .** Let  $S \subseteq P$ . From (1.4), we have:

$$\tilde{r}_{K,S} = \sum_{\mathfrak{p} \in S} [K_{\mathfrak{p}} : \mathbb{Q}_p] - r_{K,S}, \text{ where } r_{K,S} := \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \log_S(E_K)).$$

(i) In [Mai02, Mai03] Maire has given, in the relative Galois case, some results about  $r_{K,S}$  depending on Schanuel's conjecture and the use of the representation  $\mathbb{Q}_p \log_S(E_K)$  from the results of Jaulent [Jau85].

(ii) In the Galois case, this rank has been studied by Nelson [Nel13] giving formulas (or lower bounds) under the  $p$ -adic Schanuel conjecture.

(iii) We have proposed, in [Gra03, III, § 4 (f)], a conjecture and a calculation process in the general non-Galois case using a Galois descent from the Galois closure  $N$  of  $K$  and the family of decomposition groups of the places of  $N$  above  $p$  and  $\infty$ . If  $K/\mathbb{Q}$  is Galois then (with  $\Sigma := P \setminus S$ ):

$$\mathrm{rk}_{\mathbb{Z}_p}(\mathrm{Gal}(\tilde{K}^P / \tilde{K}^S)) = \sum_{\mathfrak{p} \in \Sigma} [K_{\mathfrak{p}} : \mathbb{Q}_p] - \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \log_P(\mathcal{E}_{K,S})),$$

where  $\mathcal{E}_{K,S} := \{\varepsilon \in E_K \otimes \mathbb{Z}_p, \iota_{\mathfrak{p}}(\varepsilon) = 1, \forall \mathfrak{p} \in S\}$  and  $\iota_{\mathfrak{p}} : E_K \otimes \mathbb{Z}_p \rightarrow U_{\mathfrak{p}}^1$ .

But all these similar approaches are difficult for programming and not so obvious for random  $K$  and  $S$  because of conjectural aspects; so we shall preferably give extensive computations via PARI/GP [Pari16] since ray class fields are well computed. But it remains the problem of justification of the "computing" of  $\tilde{r}_{K,S}$ , when no theoretical value is known (see another explicit numerical method in [Gra03, § III.5, Theorem 5.2]).

We conclude by the following comments:

**Remark 2.6.** If  $\mathcal{T}_{K,P} = 1$  (i.e., the field  $K$  is called  $p$ -rational as proposed by Movahhedi in [Mov88, Mov90]), this does not imply  $\mathcal{T}_{K,S} = 1$  for  $S \subsetneq P$  (the numerical examples will show many cases). In the opposite situation, we may have  $\mathcal{T}_{K,P} \neq 1$ , but often  $\mathcal{T}_{K,S} = 1$  for  $S \subsetneq P$ .

This intricate aspects have been studied by Maire [Mai05, Section 3] in which he introduces the “ $S$ -cohomological condition”  $H^2(\mathcal{G}_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$  (knowing that  $\mathcal{G}_{K,S}$  is a free pro- $p$ -group if and only if  $H^2(\mathcal{G}_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p)$  and  $\mathcal{T}_{K,S}$  are trivial) and that of “ $S$ -arithmetical condition” ( $E_K \otimes \mathbb{Z}_p \rightarrow U_{K,S}$  injective), and compare them, which of course coincide for  $S = P$ ; we know that the  $S$ -arithmetical condition implies the  $S$ -cohomological one.

We shall speak of  $S$ -rationality, when  $\mathcal{T}_{K,S} = 1$  for  $S \subseteq P$ , even if this may be rather ambiguous when  $S \subsetneq P$  because of the above observations; one must understand this as a “free  $S$ -ramification” over  $K$  (i.e., giving a free abelian  $S$ -ramified pro- $p$ -extension  $H_{K,S}/K$ ). This is also justified by the fact that many variants of the definition have been given, as those of Jaulent–Sauzet [JS97, JS00], Bourbon–Jaulent [BJ13], where are defined and studied the case of singleton  $S = \{\mathfrak{p}\}$  or that of the “2-birationality” of quadratic extensions of totally real fields when  $S = \{\mathfrak{p}, \mathfrak{p}'\}$ .

### 3. ALGORITHMIC APPROACH OF $S$ -RAMIFICATION

The principle is to consider a modulus  $\mathfrak{m}_S := \prod_{\mathfrak{p} \in S} \mathfrak{p}^{\lambda_{\mathfrak{p}}}$ ,  $S \subseteq P$ , with  $\lambda_{\mathfrak{p}} \gg 0$  for all  $\mathfrak{p} \in S$  to “read” the structure of  $\mathcal{A}_{K,S}$  on the ray class group  $\mathcal{C}_K(\mathfrak{m}_S)$ . The practice shows that the more convenient modulus is of the form:

$$\left( \prod_{\mathfrak{p} \in S} \mathfrak{p}^{e_{\mathfrak{p}}} \right)^n,$$

where  $e_{\mathfrak{p}}$  is the ramification index of  $\mathfrak{p}$  in  $K/\mathbb{Q}$  and  $n \gg 0$ . Of course, this modulus is  $(p^n)$  only for  $S = P$ ; so we must use the ideal decomposition of  $p$  in  $K$ , given by PARI/GP, and compute everywhere with ideals.

#### 3.1. Main program computing $\mathcal{T}_{K,S}$ and $\tilde{r}_{K,S}$ .

##### 3.1.1. The PARI/GP program.

```

=====
{P=x^3+197*x^2+718*x+508;if(polisirreducible(P)==0,break);print(P);
bp=2;Bp=5000;n0=6;K=bnfinit(P,1);forprime(p=bp,Bp,n=n0+floor(30/p));
print();print("p=",p);F=idealfactor(K,p);d=component(matsize(F),1);
F1=component(F,1);for(j=1,d,print(component(F1,j)));
for(z=2^d,2^(d+1)-1,bin=binary(z);mod=List;
for(j=1,d,listput(mod,component(bin,j+1),j));M=1;
for(j=1,d,ch=component(mod,j);if(ch==1,F1j=component(F1,j);
ej=component(F1j,3);F1j=idealpow(K,F1j,ej);
M=idealmul(K,M,F1j));Idn=idealpow(K,M,n);
Kpn=bnrinit(K,Idn);Hpn=component(component(Kpn,5),2);L=List;
e=component(matsize(Hpn),2);R=0;for(k=1,e,c=component(Hpn,e-k+1);
w=valuation(c,p);if(w>0,R=R+1;listinsert(L,p^w,1));
print("S=",mod," rk(A_S)=",R," A_S=",L))}
=====

```

3.1.2. *Instructions for use.* The reader has only to copy and past the verbatim of the program and to use a “terminal session via Sage”, on his or her computer, or a cell in the page <http://pari.math.u-bordeaux.fr/gp.html>



It is assumed that the irreducible monic polynomial  $P$  defining  $K$  is given and that the interval  $[\mathbf{bp}, \mathbf{Bp}]$  of tested primes  $p$  is also given by the user.

(i) The program computes the decomposition of  $p$  into  $\mathbf{d}$  prime ideals; for instance, the following data gives, for  $P = x^3 + 197 * x^2 + 718 * x + 508$  and  $p = 2$ , the decomposition  $(p) = \mathbf{pp}'$  in  $\mathbb{Q}(x)$ , using `idealfactor(K, p)`:

```
[2, [-65, 0, 1]~, 1, 1, [0, 0, -1]~]
[2, [0, 0, 1]~, 1, 2, [0, 1, 0]~]
```

Recall that for an ideal as  $[2, [0, 0, 1]~, 1, 2, [0, 1, 0]~]$ , the 3th component is its ramification index, the 4th component is its residue degree. For the computation of the modulus  $\mathbf{m}_S$  (to be considered at the power  $n$ ), we replace each prime ideal  $\mathbf{p} \in S$  by  $\mathbf{p}^{e_p}$  using the function `idealpov`.

(ii) For each modulus  $\mathbf{m}_S = \prod_{\mathbf{p} \in S} \mathbf{p}^{e_p \cdot n}$ , the program gives  $\text{rk}_p(\mathcal{A}_{K,S})$  and the  $\mathbb{Z}$ -structure of  $\mathcal{A}_{K,S}/\mathcal{A}_{K,S}^{p^N}$ , for  $N$  of the order of  $n$ , under the form:

$$\mathcal{A}_{K,S} = [a_1, \dots, a_r; b_1, \dots, b_t],$$

where the coefficients  $a_1, \dots, a_r$  increase (resp. the coefficients  $b_1, \dots, b_t$  stabilize) as the exponent  $n$  increases, so in the non-ambiguous cases,  $b_1, \dots, b_t$  give the group-invariants of  $\mathcal{T}_{K,S}$  and  $r$  is the  $p$ -rank  $\tilde{r}_{K,S}$  of  $\text{Gal}(\widehat{K}^S/K)$ .

Of course, if the rank  $\tilde{r}_{K,S}$  is not certain, we can not, in a mathematical point of view, deduce the structure of  $\mathcal{T}_{K,S}$ ; but in practice the information is correct since one can always verify, with the program, the stabilization of the invariants  $b_j$  whereas the  $a_i$  increase linearly to infinity.

(iii) The symbolic data  $S = [\delta_1, \dots, \delta_d]$ ,  $\delta_i \in \{0, 1\}$ , indicates that the  $S$ -modulus considered is:

$$\mathbf{m}_S = \left( \prod_{i=1}^d \mathbf{p}_i^{e_{\mathbf{p}_i} \cdot \delta_i} \right)^n.$$

We have chosen  $n = n_0 + \frac{30}{p}$  to get small values when  $p \gg 0$  but larger ones for small  $p$  (especially  $p = 2$  giving possibly huge  $\#\mathcal{T}_{K,S}$ ). The parameter  $n_0$  may be increased at will (here  $n_0 = 6$ ).

There are  $2^{\#S}$  distinct sets  $S$  parametrized with the binary writing of the integers  $z \in [0, 2^d - 1]$ .

For  $S = [0, \dots, 0]$  one obtains the structure of the  $p$ -class group  $\mathcal{C}_K$ .

(iv) We illustrate the program with an example where  $K$  (a totally real cubic field) is not  $S$ -rational for some small  $p$  and some  $S \subseteq P$ ; but in almost all cases,  $K$  is  $S$ -rational.

**Remark 3.1.** We do not compute the Galois group associated to the given polynomial, nor the discriminant or the fundamental units; otherwise, the reader has only to add if necessary the instructions:

```
print("Galois :", polgalois(P));
print("Discriminant: ", factor(component(component(K,7), 3)));
print("Fundamental system of units: ", component(component(K,8), 5));
```

giving, for the Galois group and the discriminant:

Galoisgroup =  $[6, -1, 1, "S3"]$  in the PARI/GP notation<sup>2</sup> and  
 Discriminant =  $[769, 1; 1390573, 1]$ .

```

P=x^3 + 197*x^2 + 718*x + 508
p=2
[2, [-65, 0, 1]~, 1, 1, [0, 0, -1]~]
[2, [0, 0, 1]~, 1, 2, [0, 1, 0]~]
S=[0, 0] rk(A_S)=0 A_S=[]
S=[0, 1] rk(A_S)=1 A_S=[4]
S=[1, 0] rk(A_S)=0 A_S=[]
S=[1, 1] rk(A_S)=3 A_S=[274877906944, 4, 2]
p=3
[3, [3, 0, 0]~, 1, 3, 1]
S=[0] rk(A_S)=0 A_S=[]
S=[1] rk(A_S)=2 A_S=[22876792454961, 3]
p=5
[5, [-68, 0, 1]~, 1, 1, [-1, 2, -1]~]
[5, [12589, 2, -196]~, 1, 2, [2, 0, 1]~]
S=[0, 0] rk(A_S)=0 A_S=[]
S=[0, 1] rk(A_S)=1 A_S=[390625]
S=[1, 0] rk(A_S)=0 A_S=[]
S=[1, 1] rk(A_S)=2 A_S=[19073486328125, 390625]
p=7
[7, [-65, 0, 1]~, 1, 1, [3, 2, 1]~]
[7, [12519, 2, -195]~, 1, 2, [-2, 0, 1]~]
S=[0, 0] rk(A_S)=0 A_S=[]
S=[0, 1] rk(A_S)=1 A_S=[7]
S=[1, 0] rk(A_S)=0 A_S=[]
S=[1, 1] rk(A_S)=2 A_S=[33232930569601, 7]
p=11
[11, [11, 0, 0]~, 1, 3, 1]
S=[0] rk(A_S)=0 A_S=[]
S=[1] rk(A_S)=2 A_S=[3138428376721, 11]
p=13
[13, [13, 0, 0]~, 1, 3, 1]
S=[0] rk(A_S)=0 A_S=[]
S=[1] rk(A_S)=1 A_S=[1792160394037]
(...)
p=127
[127, [-66, 0, 1]~, 1, 1, [-16, 2, 2]~]
[127, [16240, 2, -252]~, 1, 2, [61, 0, 1]~]
S=[0, 0] rk(A_S)=0 A_S=[]
S=[0, 1] rk(A_S)=1 A_S=[127]
S=[1, 0] rk(A_S)=0 A_S=[]
S=[1, 1] rk(A_S)=2 A_S=[532875860165503, 127]
p=1571
[1571, [275, 0, 1]~, 1, 1, [-418, 2, -339]~]
[1571, [21576, 2, -339]~, 1, 2, [275, 0, 1]~]
S=[0, 0] rk(A_S)=0 A_S=[]
S=[0, 1] rk(A_S)=1 A_S=[1571]

```

<sup>2</sup>See <http://galoisdb.math.upb.de/home>

```

S=[1, 0] rk(A_S)=0 A_S=[]
S=[1, 1] rk(A_S)=2 A_S=[23617465807865561078891, 1571]
p=1759
[1759, [1759, 0, 0]~, 1, 3, 1]
S=[0, 0] rk(A_S)=0 A_S=[]
S=[1] rk(A_S)=2 A_S=[52102777604679963122719, 1759]
p=3371
[3371, [-295, 0, 1]~, 1, 1, [-1597, 2, 231]~]
[3371, [-121, 0, 1]~, 1, 1, [355, 2, 57]~]
[3371, [415, 0, 1]~, 1, 1, [38, 2, -479]~]
S=[0, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 1] rk(A_S)=0 A_S=[]
S=[0, 1, 0] rk(A_S)=0 A_S=[]
S=[0, 1, 1] rk(A_S)=1 A_S=[3371]
S=[1, 0, 0] rk(A_S)=0 A_S=[]
S=[1, 0, 1] rk(A_S)=1 A_S=[3371]
S=[1, 1, 0] rk(A_S)=1 A_S=[3371]
S=[1, 1, 1] rk(A_S)=2 A_S=[4946650964538063853923491, 3371]

```

If, for the remarkable case  $p = 5$ , one has some doubt, one increases  $n$ , which gives (for  $n = 50$ ):

```

[5, [-68, 0, 1]~, 1, 1, [-1, 2, -1]~]
[5, [12589, 2, -196]~, 1, 2, [2, 0, 1]~]
S=[0, 0] rk(A_S)=0 A_S=[]
S=[0, 1] rk(A_S)=1 A_S=[390625]
S=[1, 0] rk(A_S)=0 A_S=[]
S=[1, 1] rk(A_S)=2 A_S=[17763568394002504646778106689453125, 390625]

```

Whence  $\mathcal{T}_{K,S} \simeq \mathbb{Z}/5^8\mathbb{Z}$  for  $S_1 = \{\mathfrak{p}\}$  (for the prime of residue degree 2) and  $S_2 = P$ . Note that once the substantial computation of  $K = \text{bnfinit}(P, 1)$  (giving all the basic information about the field) is done, very large values of  $n$  do not increase much the execution time; so any skeptical user can make  $n \rightarrow \infty$  to see that only the data 390625 remains constant.

(v) In [Gra19a, § 9.1] we have used some special families of polynomials (e.g., Lecacheux–Washington ones) in which we can force the  $p$ -adic regulator to be  $p$ -adically close to 0 at will; but we must take the parameter  $n$  in proportion, even if here the  $\mathbb{Z}_p$ -ranks of the  $\mathcal{A}_{K,S}$  are obvious, since  $K$  is totally real, giving finite groups except for  $S = P$  where  $\text{rk}_{\mathbb{Z}_p}(\mathcal{A}_{K,P}) = 1$ :

```

P=x^3-134480895*x^2-263169*x-1
p=2
[2, [0, 0, 1]~, 1, 1, [1, 0, 1]~]
[2, [0, 1, 0]~, 1, 1, [1, 1, 0]~]
[2, [2, 1, 1]~, 1, 1, [1, 1, 1]~]
S=[0, 0, 0] rk(A_S)=6 A_S=[16, 16, 2, 2, 2, 2]
S=[0, 0, 1] rk(A_S)=6 A_S=[512, 16, 8, 2, 2, 2]
S=[0, 1, 0] rk(A_S)=6 A_S=[512, 16, 8, 2, 2, 2]
S=[0, 1, 1] rk(A_S)=6 A_S=[1024, 512, 8, 8, 2, 2]
S=[1, 0, 0] rk(A_S)=6 A_S=[512, 16, 8, 2, 2, 2]
S=[1, 0, 1] rk(A_S)=6 A_S=[1024, 512, 8, 8, 2, 2]
S=[1, 1, 0] rk(A_S)=6 A_S=[1024, 512, 8, 8, 2, 2]
S=[1, 1, 1] rk(A_S)=7 A_S=[9444732965739290427392, 1024, 1024, 8, 8, 2, 2]

```

```

x^3-7625984944841*x^2-387459856*x-1
p=3
[3, [1, -1, -1]~, 1, 1, [0, 1, 1]~]
[3, [2, 1, 0]~, 1, 1, [1, 1, 0]~]
[3, [2541994975055, -19683, 1]~, 1, 1, [-1, 0, -1]~]
S=[0, 0, 0] rk(A_S)=4 A_S=[27, 9, 3, 3]
S=[0, 0, 1] rk(A_S)=4 A_S=[177147, 9, 3, 3]
S=[0, 1, 0] rk(A_S)=4 A_S=[177147, 9, 3, 3]
S=[0, 1, 1] rk(A_S)=4 A_S=[177147, 59049, 3, 3]
S=[1, 0, 0] rk(A_S)=4 A_S=[177147, 9, 3, 3]
S=[1, 0, 1] rk(A_S)=4 A_S=[177147, 59049, 3, 3]
S=[1, 1, 0] rk(A_S)=4 A_S=[177147, 59049, 3, 3]
S=[1, 1, 1] rk(A_S)=5 A_S=[834385168331080533771857328695283,
177147, 59049, 3, 3]

P=x^3-1628427439432947*x^2-13841522500*x-1
p=7
[7, [1, -3, -3]~, 1, 1, [0, 1, 1]~]
[7, [4, 3, 0]~, 1, 1, [1, 1, 0]~]
[7, [542809146438439, -117649, 1]~, 1, 1, [2, 0, 2]~]
S=[0, 0, 0] rk(A_S)=2 A_S=[7, 7]
S=[0, 0, 1] rk(A_S)=2 A_S=[117649, 7]
S=[0, 1, 0] rk(A_S)=2 A_S=[117649, 7]
S=[0, 1, 1] rk(A_S)=3 A_S=[117649, 16807, 7]
S=[1, 0, 0] rk(A_S)=2 A_S=[117649, 7]
S=[1, 0, 1] rk(A_S)=3 A_S=[117649, 16807, 7]
S=[1, 1, 0] rk(A_S)=3 A_S=[117649, 16807, 7]
S=[1, 1, 1] rk(A_S)=4 A_S=[3219905755813179726837607, 117649, 16807, 7]

```

3.1.3. *Example with  $p$  totally split in degree 5.* For  $P = x^5 - 5$ ,  $n_0 = 8$ , and  $p = 31$  (totally split) one finds one case of non  $S$ -rationality:

$S = [1, 0, 0, 0, 1]$   $\text{rk}(A_S) = 1$   $A_S = [961]$ , i.e.,  $\tilde{r}_{K,S} = 0$ ,  $\mathcal{T}_{K,S} \simeq \mathbb{Z}/31^2\mathbb{Z}$ :

```

[31, [-14, 1, 0, 0, 0]~, 1, 1, [7, -15, 10, 14, 1]~]
[31, [-7, 1, 0, 0, 0]~, 1, 1, [14, 2, -13, 7, 1]~]
[31, [3, 1, 0, 0, 0]~, 1, 1, [-12, 4, 9, -3, 1]~]
[31, [6, 1, 0, 0, 0]~, 1, 1, [-6, 1, 5, -6, 1]~]
[31, [12, 1, 0, 0, 0]~, 1, 1, [-3, 8, -11, -12, 1]~]
S=[0, 0, 0, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 0, 0, 1] rk(A_S)=0 A_S=[]
S=[0, 0, 0, 1, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 0, 1, 1] rk(A_S)=0 A_S=[]
S=[0, 0, 1, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 1, 0, 1] rk(A_S)=0 A_S=[]
S=[0, 0, 1, 1, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 1, 1, 1] rk(A_S)=1 A_S=[27512614111]
S=[0, 1, 0, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 1, 0, 0, 1] rk(A_S)=0 A_S=[]
S=[0, 1, 0, 1, 0] rk(A_S)=0 A_S=[]
S=[0, 1, 0, 1, 1] rk(A_S)=1 A_S=[27512614111]
S=[0, 1, 1, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 1, 1, 0, 1] rk(A_S)=1 A_S=[27512614111]
S=[0, 1, 1, 1, 0] rk(A_S)=1 A_S=[27512614111]

```

```

S=[0, 1, 1, 1, 1] rk(A_S)=2 A_S=[27512614111, 27512614111]
S=[1, 0, 0, 0, 0] rk(A_S)=0 A_S=[]
S=[1, 0, 0, 0, 1] rk(A_S)=1 A_S=[961]
S=[1, 0, 0, 1, 0] rk(A_S)=0 A_S=[]
S=[1, 0, 0, 1, 1] rk(A_S)=1 A_S=[27512614111]
S=[1, 0, 1, 0, 0] rk(A_S)=0 A_S=[]
S=[1, 0, 1, 0, 1] rk(A_S)=1 A_S=[27512614111]
S=[1, 0, 1, 1, 0] rk(A_S)=1 A_S=[27512614111]
S=[1, 0, 1, 1, 1] rk(A_S)=2 A_S=[27512614111, 27512614111]
S=[1, 1, 0, 0, 0] rk(A_S)=0 A_S=[]
S=[1, 1, 0, 0, 1] rk(A_S)=1 A_S=[27512614111]
S=[1, 1, 0, 1, 0] rk(A_S)=1 A_S=[27512614111]
S=[1, 1, 0, 1, 1] rk(A_S)=2 A_S=[27512614111, 27512614111]
S=[1, 1, 1, 0, 0] rk(A_S)=1 A_S=[27512614111]
S=[1, 1, 1, 0, 1] rk(A_S)=2 A_S=[27512614111, 27512614111]
S=[1, 1, 1, 1, 0] rk(A_S)=2 A_S=[27512614111, 27512614111]
S=[1, 1, 1, 1, 1] rk(A_S)=3 A_S=[27512614111, 27512614111, 27512614111]

```

3.1.4. *Example with  $p$  totally split in degree 7.* For the polynomial  $P = x^7 - 7$  and  $p = 43$ , one finds two cases:

```

[43, [-18, 1, 0, 0, 0, 0, 0]~, 1, 1, [-2, 19, 13, -16, -20, 18, 1]~]
[43, [-7, 1, 0, 0, 0, 0, 0]~, 1, 1, [1, -6, -7, -1, 6, 7, 1]~]
[43, [9, 1, 0, 0, 0, 0, 0]~, 1, 1, [4, -10, -18, 2, -5, -9, 1]~]
[43, [13, 1, 0, 0, 0, 0, 0]~, 1, 1, [16, 12, 9, -4, -3, -13, 1]~]
[43, [14, 1, 0, 0, 0, 0, 0]~, 1, 1, [21, 20, 17, 8, -19, -14, 1]~]
[43, [15, 1, 0, 0, 0, 0, 0]~, 1, 1, [11, 5, 14, -21, 10, -15, 1]~]
[43, [17, 1, 0, 0, 0, 0, 0]~, 1, 1, [-8, 3, 15, -11, -12, -17, 1]~]
(...)
S=[0, 1, 0, 1, 0, 0, 1] rk(A_S)=1 A_S=[43]
S=[1, 1, 0, 0, 1, 0, 0] rk(A_S)=1 A_S=[43]

```

i.e.,  $\tilde{r}_{K,S} = 0$  and  $\mathcal{T}_{K,S} \simeq \mathbb{Z}/43\mathbb{Z}$  for the two above cases. For the other modulus,  $\mathcal{T}_{K,S} = 1$ .

3.1.5. *Example with a field discovered by Jaulent–Sauzet.* In [JS97], some numerical examples of  $\{\mathfrak{l}\} (= \{\mathfrak{p}\})$ -rational fields, which are not  $p$ -rational, are given; of course this corresponds to a suitable choice of  $S = \{\mathfrak{p}\}$  and we give the case of the field defined by the polynomial:

$$P = x^{10} + 19x^8 + 8x^7 + 130x^6 + 16x^5 + 166x^4 - 888x^3 - 15x^2 + 432x + 243$$

for  $p = 3$ :

```

[3, [-1, 1, 0, 0, 1, 1, -1, 0, 0, -1]~, 2, 1,
                                     [2, 0, 2, 1, 2, 0, 1, 1, 2, 1]~]
[3, [-1, 1, 0, 1, 1, 0, -1, 0, 0, -1]~, 2, 1,
                                     [2, 0, 1, 2, 1, 2, 1, 1, 2, 1]~]
[3, [-5, 14, -4, -2, 5, 5, 13, -13, 2, 6]~, 2, 3,
                                     [0, 1, 1, 1, -1, -1, -1, -1, -1, 1]~]

S=[0, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 1] rk(A_S)=2 A_S=[14348907,14348907]
S=[0, 1, 0] rk(A_S)=0 A_S=[]
S=[0, 1, 1] rk(A_S)=5 A_S=[14348907,14348907,14348907,14348907, 3]
S=[1, 0, 0] rk(A_S)=0 A_S=[]

```

```
S=[1, 0, 1] rk(A_S)=5 A_S=[14348907,14348907,14348907,14348907, 3]
S=[1, 1, 0] rk(A_S)=1 A_S=[27]
S=[1, 1, 1] rk(A_S)=8 A_S=[14348907,14348907,14348907,14348907,
14348907,14348907, 3, 3]
```

which is indeed  $\{\mathfrak{p}\}$ -rational for each prime ideal  $\mathfrak{p}$ , but the field is not 3-rational since  $\mathcal{T}_{K,P} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ . Note the case  $\mathcal{A}_{K,S} = \mathcal{T}_{K,S} \simeq \mathbb{Z}/27\mathbb{Z}$ . Many other numerical examples are available in [JS97, § 3.c].

3.1.6. *Abelian fields with  $\mathcal{T}_{K,S} = 1$  but  $\mathcal{T}_{K,P} \neq 1$ .* We consider for this the cyclotomic field  $\mathbb{Q}(\mu_{24})$ . The following program may be used for any abelian field given by `polcyclo(N)` or `polsubcyclo(N, d)` giving the suitable polynomials of degree  $d$  dividing  $\varphi(N)$ :

```
{P=polcyclo(24);bp=2;Bp=500;n0=8;K=bnfinit(P,1);forprime(p=bp,Bp,
n=n0+floor(30/p);print();print("p=",p);F=idealfactor(K,p);
d=component(matsize(F),1);F1=component(F,1);for(j=1,d,
print(component(F1,j)));for(z=2^d,2*2^d-1,bin=binary(z);mod=List;
for(j=1,d,listput(mod,component(bin,j+1),j));M=1;for(j=1,d,
ch=component(mod,j);if(ch==1,F1j=component(F1,j);ej=component(F1j,3);
FF1j=idealp(K,F1j,ej);M=idealmul(K,M,FF1j));Idn=idealp(K,M,n);
Kpn=bnrinit(K,Idn);Hpn=component(component(Kpn,5),2);L=List;
e=component(matsize(Hpn),2);R=0;for(k=1,e,c=component(Hpn,e-k+1);
w=valuation(c,p);if(w>0,R=R+1;listinsert(L,p^w,1)));
print("S=",mod," rk(A_S)=",R," A_S=",L)}}

p=3
[3, [-1, 0, -1, 0, 1, 0, 0, 0]~, 2, 2, [-1, -1, 1, 1, 1, 1, 0, 0]~]
[3, [-1, 0, 1, 0, 1, 0, 0, 0]~, 2, 2, [-1, -1, -1, -1, 1, 1, 0, 0]~]
S=[0, 0] rk(A_S)=0 A_S=[]
S=[0, 1] rk(A_S)=1 A_S=[22876792454961]
S=[1, 0] rk(A_S)=1 A_S=[22876792454961]
S=[1, 1] rk(A_S)=6 A_S=[68630377364883, 22876792454961, 22876792454961,
22876792454961, 22876792454961, 3]

p=7
[7, [-3, 0, -1, 0, 1, 0, 0, 0]~, 1, 2, [2, -3, -3, 1, -3, 1, 0, 0]~]
[7, [-3, 0, 1, 0, 1, 0, 0, 0]~, 1, 2, [2, -3, 3, -1, -3, 1, 0, 0]~]
[7, [2, 0, -2, 0, 1, 0, 0, 0]~, 1, 2, [-3, 2, -3, 2, 2, 1, 0, 0]~]
[7, [2, 0, 2, 0, 1, 0, 0, 0]~, 1, 2, [-3, 2, 3, -2, 2, 1, 0, 0]~]
S=[0, 0, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 0, 1] rk(A_S)=0 A_S=[]
S=[0, 0, 1, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 1, 1] rk(A_S)=2 A_S=[4747561509943, 7]
S=[0, 1, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 1, 0, 1] rk(A_S)=2 A_S=[4747561509943,4747561509943]
S=[0, 1, 1, 0] rk(A_S)=2 A_S=[4747561509943, 7]
S=[0, 1, 1, 1] rk(A_S)=4 A_S=[4747561509943,4747561509943,4747561509943, 7]
S=[1, 0, 0, 0] rk(A_S)=0 A_S=[]
S=[1, 0, 0, 1] rk(A_S)=2 A_S=[4747561509943, 7]
S=[1, 0, 1, 0] rk(A_S)=2 A_S=[4747561509943,4747561509943]
S=[1, 0, 1, 1] rk(A_S)=4 A_S=[4747561509943,4747561509943,4747561509943, 7]
S=[1, 1, 0, 0] rk(A_S)=2 A_S=[4747561509943, 7]
S=[1, 1, 0, 1] rk(A_S)=4 A_S=[4747561509943,4747561509943,4747561509943, 7]
```

```

S=[1, 1, 1, 0] rk(A_S)=4 A_S=[4747561509943,4747561509943,4747561509943, 7]
S=[1, 1, 1, 1] rk(A_S)=6 A_S=[4747561509943,4747561509943,4747561509943,
                                4747561509943,4747561509943, 7]

p=13
[13, [-6, 0, 0, 0, 1, 0, 0, 0]~, 1, 2, [2, 6, 0, 0, -4, 1, 0, 0]~]
[13, [-2, 0, 0, 0, 1, 0, 0, 0]~, 1, 2, [6, 2, 0, 0, 3, 1, 0, 0]~]
[13, [2, 0, 0, 0, 1, 0, 0, 0]~, 1, 2, [-6, -2, 0, 0, 3, 1, 0, 0]~]
[13, [6, 0, 0, 0, 1, 0, 0, 0]~, 1, 2, [-2, -6, 0, 0, -4, 1, 0, 0]~]
S=[0, 0, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 0, 1] rk(A_S)=0 A_S=[]
S=[0, 0, 1, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 1, 1] rk(A_S)=2 A_S=[1792160394037,13]
S=[0, 1, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 1, 0, 1] rk(A_S)=2 A_S=[1792160394037,1792160394037]
S=[0, 1, 1, 0] rk(A_S)=2 A_S=[1792160394037,13]
S=[0, 1, 1, 1] rk(A_S)=4 A_S=[1792160394037,1792160394037,1792160394037,13]
S=[1, 0, 0, 0] rk(A_S)=0 A_S=[]
S=[1, 0, 0, 1] rk(A_S)=2 A_S=[1792160394037,13]
S=[1, 0, 1, 0] rk(A_S)=2 A_S=[1792160394037,1792160394037]
S=[1, 0, 1, 1] rk(A_S)=4 A_S=[1792160394037,1792160394037,1792160394037,13]
S=[1, 1, 0, 0] rk(A_S)=2 A_S=[1792160394037,13]
S=[1, 1, 0, 1] rk(A_S)=4 A_S=[1792160394037,1792160394037,1792160394037,13]
S=[1, 1, 1, 0] rk(A_S)=4 A_S=[1792160394037,1792160394037,1792160394037,13]
S=[1, 1, 1, 1] rk(A_S)=6 A_S=[1792160394037,1792160394037,1792160394037,
                                1792160394037,1792160394037,13]

```

**3.2. Experiments with the fields  $K = \mathbb{Q}(\sqrt[p]{N})$ .** These fields are studied in great detail by Lecouturier in [Lec18, § 5] for their  $p$ -class groups and these fields have some remarkable properties. For instance if  $\log$  is the discrete logarithm for  $(\mathbb{Z}/p\mathbb{Z})^\times$  provided with a primitive root  $g$ , the expression  $T = \sum_{k=1}^{(N-1)/2} k \cdot \log(k) \pmod{p}$  governs, under some conditions, the  $p$ -rank of  $\mathcal{C}_K$  (from a result of Calegari–Emerton, after other similar results of Iimura, proved again in [Lec18, Theorem 1.1]).

So we shall give the general calculations, for all  $S \subseteq P$ , with that of  $T$ . We assume  $N$  prime congruent to 1 modulo  $p$ , but the reader may suppress this conditions. It seems that many interesting heuristics can be elaborated from the numerical results; we only give some examples (recall that the structure of the class group is given by the first data  $S = \emptyset$ ):

```

{p=3;print("p=",p);n=8+floor(30/p);g=znprimroot(p);forprime(N=1,10^3,
if(Mod(N,p)!=1,next);P=x^p-N;print();print("P=",P);T=Mod(0,p);
for(k=1,(N-1)/2,if(Mod(k,p)==0,next);T=T+k*znlog(k,g));K=bnfinit(P,1);
F=idealfactor(K,p);d=component(matsize(F),1);F1=component(F,1);for(j=1,d,
print(component(F1,j)));for(z=2^d,2*2^d-1,bin=binary(z);mod=List;for(j=1,d,
listput(mod,component(bin,j+1),j));M=1;for(j=1,d,ch=component(mod,j);
if(ch==1,F1j=component(F1,j);ej=component(F1j,3);F1j=idealpow(K,F1j,ej);
M=idealmul(K,M,F1j));Idn=idealpow(K,M,n);Kpn=bnrinit(K,Idn);
Hpn=component(component(Kpn,5),2);L=List;e=component(matsize(Hpn),2);R=0;
for(k=1,e,c=component(Hpn,e-k+1);w=valuation(c,p);if(w>0,R=R+1;
listinsert(L,p^w,1));print("S=",mod," rk(A_S)=",R," A_S=",L))}

```

```

p=3
P=x^3 - 7
[3, [-1, 1, 0]~, 3, 1, [1, 1, 1]~]
T=Mod(2,3) S=[0] rk(A_S)=1 A_S=[3]
T=Mod(2,3) S=[1] rk(A_S)=2 A_S=[387420489, 387420489]
P=x^3 - 271
[3, [-2, 0, -1]~, 1, 1, [0, 0, 1]~]
[3, [-1, 1, 1]~, 2, 1, [2, 1, 0]~]
T=Mod(0,3) S=[0,0] rk(A_S)=1 A_S=[9]
T=Mod(0,3) S=[0,1] rk(A_S)=3 A_S=[129140163, 27, 3]
T=Mod(0,3) S=[1,0] rk(A_S)=2 A_S=[9, 3]
T=Mod(0,3) S=[1,1] rk(A_S)=4 A_S=[129140163, 129140163, 27, 3]
P=x^3 - 523
[3, [0, 0, 1]~, 2, 1, [2, 1, 0]~]
[3, [1, 0, -1]~, 1, 1, [2, 1, 1]~]
T=Mod(0,3) S=[0,0] rk(A_S)=1 A_S=[9]
T=Mod(0,3) S=[0,1] rk(A_S)=2 A_S=[9, 3]
T=Mod(0,3) S=[1,0] rk(A_S)=3 A_S=[387420489, 9, 3]
T=Mod(0,3) S=[1,1] rk(A_S)=4 A_S=[387420489, 129140163, 9, 3]

p=5
P=x^5 - 11
[5, [-1, 1, 0, 0, 0]~, 5, 1, [1, 1, 1, 1, 1]~]
T=Mod(4,5) S=[0] rk(A_S)=1 A_S=[5]
T=Mod(4,5) S=[1] rk(A_S)=3 A_S=[30517578125, 6103515625, 6103515625]
P=x^5 - 211
[5, [-1, 1, 0, 0, 0]~, 5, 1, [1, 1, 1, 1, 1]~]
T=Mod(4,5) S=[0] rk(A_S)=3 A_S=[5, 5, 5]
T=Mod(4,5) S=[1] rk(A_S)=5 A_S=[6103515625, 6103515625, 6103515625, 5, 5]
P=x^5 - 401
[5, [-1, 1, 0, 1, 0]~, 4, 1, [4, 3, 2, 0, 1]~]
[5, [1, 0, 0, -1, 0]~, 1, 1, [4, 3, 2, 1, 1]~]
T=Mod(0,5) S=[0,0] rk(A_S)=2 A_S=[5, 5]
T=Mod(0,5) S=[0,1] rk(A_S)=2 A_S=[25, 5]
T=Mod(0,5) S=[1,0] rk(A_S)=3 A_S=[6103515625, 6103515625, 25]
T=Mod(0,5) S=[1,1] rk(A_S)=4 A_S=[6103515625, 6103515625, 1220703125, 25]

p=7
P=x^7 - 29
[7, [-1, 1, 0, 0, 0, 0, 0]~, 7, 1, [1, 1, 1, 1, 1, 1, 1]~]
T=Mod(6,7) S=[0] rk(A_S)=1 A_S=[7]
T=Mod(6,7) S=[1] rk(A_S)=4 A_S=[96889010407, 13841287201, 13841287201,
13841287201]
P=x^7 - 197
[7, [0, 0, 0, 0, 0, 0, 1]~, 1, 1, [6, 5, 4, 3, 3, 2, 1]~]
[7, [1, 0, 0, 0, 0, 0, -1]~, 6, 1, [6, 5, 4, 3, 1, 2, 1]~]
T=Mod(0,7) S=[0,0] rk(A_S)=1 A_S=[7]
T=Mod(0,7) S=[0,1] rk(A_S)=4 A_S=[96889010407, 13841287201, 1977326743, 49]
T=Mod(0,7) S=[1,0] rk(A_S)=1 A_S=[7]
T=Mod(0,7) S=[1,1] rk(A_S)=5 A_S=[96889010407, 13841287201, 1977326743,
1977326743, 49]
P=x^7 - 337
[7, [-1, 1, 0, 0, 0, 0, 0]~, 7, 1, [1, 1, 1, 1, 1, 1, 1]~]

```



```

T=Mod(2,7) S=[0] rk(A_S)=2 A_S=[7, 7]
T=Mod(2,7) S=[1] rk(A_S)=5 A_S=[13841287201,13841287201,13841287201,
                                     13841287201, 7]

p=11
P=x^11 - 67
[11, [-1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0]~, 11, 1,
                                     [1, 1, 1, 1, 1, 1, 1, 1, 1, 1]~]
T=Mod(8,11) S=[0] rk(A_S)=2 A_S=[11, 11]
T=Mod(8,11) S=[1] rk(A_S)=7 A_S=[285311670611,285311670611,25937424601,
                                     25937424601,25937424601, 11]

P=x^11 - 727
[11, [-5, 0, 0, 0, 0, 0, 0, 0, 0, 0, -5]~, 1, 1,
                                     [10, 9, 8, 7, 6, 5, 4, 6, 3, 2, 1]~]
[11, [-5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 5]~, 10, 1,
                                     [10, 9, 8, 7, 6, 5, 4, 4, 3, 2, 1]~]
T=Mod(0,11) S=[0,0] rk(A_S)=1 A_S=[11]
T=Mod(0,11) S=[0,1] rk(A_S)=6 A_S=[25937424601,25937424601,25937424601,
                                     25937424601,2357947691, 121]

T=Mod(0,11) S=[1,0] rk(A_S)=1 A_S=[11]
T=Mod(0,11) S=[1,1] rk(A_S)=7 A_S=[25937424601,25937424601,25937424601,
                                     25937424601,2357947691,2357947691,121]

p=13
P=x^13 - 53
[13, [-1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]~, 13, 1,
                                     [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]~]
T=Mod(11,13) S=[0] rk(A_S)=1 A_S=[13]
T=Mod(11,13) S=[1] rk(A_S)=7 A_S=[1792160394037,137858491849,137858491849,
                                     137858491849,137858491849,137858491849]

P=x^13 - 677
[13, [-4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 4]~, 12, 1,
                                     [12, 11, 10, 9, 8, 7, 6, 5, 5, 4, 3, 2, 1]~]
[13, [5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4]~, 1, 1,
                                     [12, 11, 10, 9, 8, 7, 6, 5, 2, 4, 3, 2, 1]~]
T=Mod(0,13) S=[0,0] rk(A_S)=1 A_S=[13]
T=Mod(0,13) S=[0,1] rk(A_S)=1 A_S=[13]
T=Mod(0,13) S=[1,0] rk(A_S)=7 A_S=[137858491849,137858491849,137858491849,
                                     137858491849,137858491849,10604499373, 169]
T=Mod(0,13) S=[1,1] rk(A_S)=8 A_S=[137858491849,137858491849,137858491849,
                                     137858491849,10604499373,10604499373, 169]

```

**3.3. The fields  $K = \mathbb{Q}(\sqrt{-\sqrt{-q}})$  associated to elliptic curves.** These fields, used in [CL18, CL19] to prove non-vanishing theorems for the central values at  $s = 1$  of the complex  $L$ -series of a family of elliptic curves studied by Gross (for any prime  $q \equiv 7 \pmod{8}$  and  $p = 2$ ), are particularly interesting. Note once for all that the signature of  $K$  is  $[0, 2]$ , the Galois closure of  $K$  is of degree 8 with Galois group  $[8, -1, 1, "D(4)"]$  and  $D_K = 2^m q^3$ .

**3.3.1. Program for various  $p$ .** In this part, we fix the prime number  $q$  and compute the structure of  $\mathcal{A}_{K,S}$  for all sets  $S \subseteq P$ . Recall that the parameter  $n$  must be such that  $p^n$  be much larger than the exponent of  $\mathcal{T}_K$ .

For instance, for  $P = x^4 + 23$ , we give the results for  $p = 3$  and  $p = 71$ :

```

{q=23;P=x^4+q;print("P=",P);bp=2;Bp=500;n0=8;K=bnfinit(P,1);
forprime(p=bp,Bp,n=n0+floor(30/p);print();print("p=",p);F=idealfactor(K,p);
d=component(matsize(F),1);F1=component(F,1);for(j=1,d,
print(component(F1,j)));for(z=2^d,2*2^d-1,bin=binary(z);mod=List;for(j=1,d,
listput(mod,component(bin,j+1),j));M=1;for(j=1,d,ch=component(mod,j);
if(ch==1,F1j=component(F1,j);ej=component(F1j,3);FF1j=idealpow(K,F1j,ej);
M=idealmul(K,M,FF1j));Idn=idealpow(K,M,n);Kpn=bnrinit(K,Idn);
Hpn=component(component(Kpn,5),2);L=List;e=component(matsize(Hpn),2);R=0;
for(k=1,e,c=component(Hpn,e-k+1);w=valuation(c,p);if(w>0,R=R+1;
listinsert(L,p^w,1));print("S=",mod," rk(A_S)="R," A_S="(L))}
P=x^4 + 23
p=3
[3, [-1, 1, 0, 0]~, 1, 1, [1, 0, 1, 1]~]
[3, [1, 1, 0, 0]~, 1, 1, [0, 0, 0, 1]~]
[3, [2, 0, 2, 0]~, 1, 2, [0, 0, -1, 0]~]
S=[0, 0, 0] rk(A_S)=1 A_S=[3]
S=[0, 0, 1] rk(A_S)=1 A_S=[68630377364883]
S=[0, 1, 0] rk(A_S)=1 A_S=[3]
S=[0, 1, 1] rk(A_S)=2 A_S=[68630377364883, 22876792454961]
S=[1, 0, 0] rk(A_S)=1 A_S=[3]
S=[1, 0, 1] rk(A_S)=2 A_S=[68630377364883, 22876792454961]
S=[1, 1, 0] rk(A_S)=1 A_S=[68630377364883]
S=[1, 1, 1] rk(A_S)=3 A_S=[68630377364883, 22876792454961, 22876792454961]
p=71
[71, [-32, 1, 0, 0]~, 1, 1, [0, 29, -5, 4]~]
[71, [32, 1, 0, 0]~, 1, 1, [4, 29, 9, 4]~]
[71, [31, 0, 2, 0]~, 1, 2, [-29, 0, 2, 0]~]
S=[0, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 1] rk(A_S)=1 A_S=[9095120158391]
S=[0, 1, 0] rk(A_S)=1 A_S=[71]
S=[0, 1, 1] rk(A_S)=2 A_S=[9095120158391, 9095120158391]
S=[1, 0, 0] rk(A_S)=1 A_S=[71]
S=[1, 0, 1] rk(A_S)=2 A_S=[9095120158391, 9095120158391]
S=[1, 1, 0] rk(A_S)=2 A_S=[9095120158391, 71]
S=[1, 1, 1] rk(A_S)=3 A_S=[9095120158391, 9095120158391, 9095120158391]

```

The user is invited to vary  $n$  at will to certify the numerical results when the  $p$ -rank of  $\mathcal{A}_{K,S}$  is unknown (i.e., when  $S \subsetneq P$ ). In the above examples, some  $\mathcal{T}_{K,S}$  are of order  $p$  and the  $\mathbb{Z}_p$ -rank of  $\mathcal{A}_{K,S}$  is 0 or 1.

3.3.2. *Program for various  $q$  and  $p = 2$ .* The analogous program is the following ( $n = 32$  is large enough):

```

{bq=3;Bq=100;p=2;n=32;forprime(q=bq,Bq,P=x^4+q;print();
print("q=",q," ",Mod(q,16));K=bnfinit(P,1);F=idealfactor(K,p);
d=component(matsize(F),1);F1=component(F,1);for(j=1,d,
print(component(F1,j)));for(z=2^d,2*2^d-1,bin=binary(z);mod=List;for(j=1,d,
listput(mod,component(bin,j+1),j));M=1;for(j=1,d,ch=component(mod,j);
if(ch==1,F1j=component(F1,j);ej=component(F1j,3);F1j=idealpow(K,F1j,ej);
M=idealmul(K,M,F1j));Idn=idealpow(K,M,n);Kpn=bnrinit(K,Idn);
Hpn=component(component(Kpn,5),2);L=List;e=component(matsize(Hpn),2);R=0;
for(k=1,e,c=component(Hpn,e-k+1);w=valuation(c,p);if(w>0,R=R+1;
listinsert(L,p^w,1));print("S=",mod," rk(A_S)="R," A_S="(L))}

```

We give an example of each congruence class  $q \pmod{16}$ ; for  $q \equiv 7 \pmod{16}$ , the decomposition of (2) in  $\mathbb{Q}(\sqrt{-q})$  is  $(2) = \mathfrak{p} \cdot \mathfrak{p}^*$  where  $e_{\mathfrak{p}} = 2$  in  $K/\mathbb{Q}$ :

```
q=17    Mod(1, 16)
[2, [1, 1, 0, 0]~, 4, 1, [1, 1, 1, 1]~]
S=[0] rk(A_S)=2 A_S=[8, 2]
S=[1] rk(A_S)=5 A_S=[4294967296, 2147483648, 2147483648, 8, 2]
```

```
q=3     Mod(3, 16)
[2, [1, 0, -1, 0]~, 2, 2, [1, 0, 1, 0]~]
S=[0] rk(A_S)=0 A_S=[]
S=[1] rk(A_S)=3 A_S=[4294967296, 2147483648, 1073741824]
```

```
q=5     Mod(5, 16)
[2, [1, 1, 0, 0]~, 4, 1, [1, 1, 1, 1]~]
S=[0] rk(A_S)=1 A_S=[4]
S=[1] rk(A_S)=3 A_S=[8589934592, 4294967296, 4294967296]
```

```
q=7     Mod(7, 16)
[2, [0, -1, 0, 1]~, 2, 1, [1, 0, 0, 1]~]
[2, [0, 1, 0, 0]~, 1, 2, [1, 1, 0, 0]~]
S=[0, 0] rk(A_S)=0 A_S=[]
S=[0, 1] rk(A_S)=2 A_S=[1073741824, 4]
S=[1, 0] rk(A_S)=1 A_S=[2147483648]
S=[1, 1] rk(A_S)=4 A_S=[2147483648, 2147483648, 1073741824, 2]
```

```
q=41    Mod(9, 16)
[2, [1, 1, 0, 0]~, 4, 1, [1, 1, 1, 1]~]
S=[0] rk(A_S)=2 A_S=[16, 2]
S=[1] rk(A_S)=4 A_S=[8589934592, 4294967296, 2147483648, 8]
```

```
q=11    Mod(11, 16)
[2, [1, 0, -1, 0]~, 2, 2, [1, 0, 1, 0]~]
S=[0] rk(A_S)=0 A_S=[]
S=[1] rk(A_S)=3 A_S=[4294967296, 2147483648, 1073741824]
```

```
q=13    Mod(13, 16)
[2, [1, 1, 0, 0]~, 4, 1, [1, 1, 1, 1]~]
S=[0] rk(A_S)=1 A_S=[4]
S=[1] rk(A_S)=3 A_S=[8589934592, 4294967296, 4294967296]
```

```
q=31    Mod(15, 16)
[2, [-1, 0, 0, 1]~, 1, 1, [0, 0, 0, 1]~]
[2, [0, 1, -1, 0]~, 2, 1, [1, 1, 0, 0]~]
[2, [2, 0, 1, 1]~, 1, 1, [1, 0, 1, 1]~]
S=[0, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 1] rk(A_S)=1 A_S=[4]
S=[0, 1, 0] rk(A_S)=2 A_S=[2147483648, 4]
S=[0, 1, 1] rk(A_S)=3 A_S=[2147483648, 1073741824, 8]
S=[1, 0, 0] rk(A_S)=1 A_S=[4]
S=[1, 0, 1] rk(A_S)=3 A_S=[1073741824, 4, 2]
S=[1, 1, 0] rk(A_S)=3 A_S=[2147483648, 1073741824, 8]
S=[1, 1, 1] rk(A_S)=5 A_S=[2147483648, 1073741824, 1073741824, 8, 2]
```

**Remark 3.2.** A more complete table shows some rules:

- (i) For  $q \equiv 3 \pmod{8}$ ,  $\mathcal{T}_{K,S} = 1$  for  $S = \emptyset$  and  $S = P = \{\mathfrak{p}\}$ ;
- (ii) For  $q \equiv 5 \pmod{8}$ ,  $\mathcal{T}_{K,\emptyset} = \mathcal{C}_K \simeq \mathbb{Z}/4\mathbb{Z}$  and  $\mathcal{T}_{K,P} = 1$  for  $P = \{\mathfrak{p}\}$  (which means that the 2-Hilbert class field of  $K$  is contained in the compositum of the  $\mathbb{Z}_2$ -extensions of  $K$ );
- (iii) For  $q \equiv 7 \pmod{16}$ , for  $S = \{\mathfrak{p}\}$  with  $e_{\mathfrak{p}} = 2$ , we get  $\mathcal{T}_{K,S} \simeq \mathbb{Z}/4\mathbb{Z}$  and for  $S = \{\mathfrak{p}^*\}$  with  $e_{\mathfrak{p}^*} = 1$ , we get  $\mathcal{T}_{K,S} = 1$ ; then  $\mathcal{T}_{K,P} \simeq \mathbb{Z}/2\mathbb{Z}$ .

These properties may be proved easily and are left to the reader as exercises on the  $\text{Log}_S$ -function (Definition A.4): consider first the arithmetic of the subfield  $k = \mathbb{Q}(\sqrt{-q})$  and use fixed point formulas (A.5) in  $K/k$ .

- (iv) For  $q \equiv 15 \pmod{16}$ , the results do not follow any obvious rule and offers some interesting examples as the following ones:

```

q=5503
[2, [-1, 0, 0, 1]~, 1, 1, [0, 0, 0, 1]~]
[2, [0, 1, -1, 0]~, 2, 1, [1, 1, 0, 0]~]
[2, [2, 0, 1, 1]~, 1, 1, [1, 0, 1, 1]~]
S=[0, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 1] rk(A_S)=1 A_S=[512]
S=[0, 1, 0] rk(A_S)=2 A_S=[2147483648, 8]
S=[0, 1, 1] rk(A_S)=3 A_S=[2147483648, 1073741824, 16]
S=[1, 0, 0] rk(A_S)=1 A_S=[512]
S=[1, 0, 1] rk(A_S)=3 A_S=[1073741824, 512, 2]
S=[1, 1, 0] rk(A_S)=3 A_S=[2147483648, 1073741824, 16]
S=[1, 1, 1] rk(A_S)=5 A_S=[2147483648, 1073741824, 1073741824, 16, 2]

q=8191
[2, [-1, 0, 0, 1]~, 1, 1, [0, 0, 0, 1]~]
[2, [0, 1, -1, 0]~, 2, 1, [1, 1, 0, 0]~]
[2, [2, 0, 1, 1]~, 1, 1, [1, 0, 1, 1]~]
S=[0, 0, 0] rk(A_S)=0 A_S=[]
S=[0, 0, 1] rk(A_S)=1 A_S=[64]
S=[0, 1, 0] rk(A_S)=2 A_S=[2147483648, 64]
S=[0, 1, 1] rk(A_S)=3 A_S=[2147483648, 1073741824, 128]
S=[1, 0, 0] rk(A_S)=1 A_S=[64]
S=[1, 0, 1] rk(A_S)=3 A_S=[1073741824, 64, 2]
S=[1, 1, 0] rk(A_S)=3 A_S=[2147483648, 1073741824, 128]
S=[1, 1, 1] rk(A_S)=5 A_S=[2147483648, 1073741824, 1073741824, 128, 2]

```

## APPENDIX A. HISTORY OF ABELIAN $p$ -RAMIFICATION

**A.1. Motivations.** We intend, in this detailed survey, to give a maximum of practical information and results about the torsion groups  $\mathcal{T}_{K,S}$  that we have numerically computed in the first part of the paper with a PARI/GP program.

For convenience, we indicate both the original historical contributions and the corresponding results processed systematically in our book [Gra03].

We will not detail the immense domains of pro- $p$ -groups and Galois cohomology, whose main purpose is for instance the existence of infinite towers

of  $S$ -ramified extensions and the Fontaine–Mazur conjecture studied by various schools of mathematicians (for this, see, e.g., [NSW00, § 10]), nor the analytic aspects as the non-vanishing at  $s = 1$  of complex  $L$ -series associated to elliptic curves . . . Similarly, we shall not consider the context of Iwasawa’s theory because this efficient tool does not exempt from having the “basic” arithmetical properties of the corresponding objects.

Note that the solutions of the analogous problems of  $S$ -ramification over local fields are not sufficient for a “globalization” over a number field  $K$  as remarked by Nguyen Quang Do in [Nqd82, § 9]. Indeed, the global theory depends on Leopoldt’s conjecture (usually assumed) and the torsion groups  $\mathcal{T}_{K,S}$  are, in some sense, refinements of this conjecture.

So we will focus, mainly, on class field theory and on these specific deep  $p$ -adic properties or conjectures which are, in our opinion, the main obstructions for many contemporary researches.

We will not give the most general statements but restrict ourselves to the case of  $S$ -ramification,  $S \subseteq P$ , without decomposition of finite or infinite places (indeed, in these more elaborate cases, the formalism is identical and may be found in our book). Since the properties of  $S$ -ramification may be used by many researchers working on different subjects, we will try to explain the numerous steps of its progress. This must be understood for practical information and will be an opportunity to clarify the vocabulary and the main contributions.

We apologize for the probable lack of references (and citation of their authors). Any suggestion will be welcome to further versions.

**A.2. Prehistory.** The origin of interest for  $S$ -ramification theory over a number field is probably a paper of Brumer [Bru66], following Serre’s book [Ser64] and seems also due to a lecture by Šafarevič (1963) showing the importance of the subject. In [Sha64], Šafarevič gives the cohomological characteristics of the group  $\mathcal{G}_{K,S}$  (number of generators and relations, cohomological dimension . . .).

Recall at this step the Golod–Šafarevič theorem (1964), named soon after the theorem of Golod–Šafarevič–Gaschütz–Vinberg, saying that if a pro- $p$ -group  $\mathcal{G}$  is finite, then  $r(\mathcal{G}) > \frac{1}{4}(d(\mathcal{G}))^2$  where  $d(\mathcal{G})$  (resp.  $r(\mathcal{G})$ ) is the minimal number of generators (resp. relations) for the presentation of  $\mathcal{G}$ . All of this was developed in Koch’s book [Koch70] from the works of many German mathematicians and is amply improved in [NSW00] (see also in [HM01, HM02b] a good introduction on the subject and some of its developments [HM02a, Mai10, Mai18, HM18a, HM18b]).

More precisely, in [Sha64, Théorème I], Šafarevič gives, for any number field  $K$  and any set of places  $S$ , the main formula (1.2) that we recall:

A.2.1. *Šafarevič formula.* The  $p$ -rank of the  $\mathbb{Z}_p$ -module  $\mathcal{A}_{K,S}$  (giving the minimal number of generators  $\dim_{\mathbb{F}_p}(\mathbb{H}^1(\mathcal{G}_{K,S}, \mathbb{Z}/p\mathbb{Z}))$  of  $\mathcal{G}_{K,S}$ ) is:

$$(A.1) \quad \begin{aligned} \mathrm{rk}_p(\mathcal{A}_{K,S}) &= \mathrm{rk}_p(V_{K,S}/K_{(S)}^{\times p}) \\ &+ \sum_{\mathfrak{p} \in S \cap P} [K_{\mathfrak{p}} : \mathbb{Q}_p] + \sum_{\mathfrak{p} \in S} \delta_{\mathfrak{p}} - \delta_K - (r_1 + r_2 - 1), \end{aligned}$$

where  $K_{(S)}^{\times} := \{\alpha \in K^{\times}, \alpha \text{ prime to } S\}$ ,  $V_{K,S} := \{\alpha \in K_{(S)}^{\times}, (\alpha) = \mathfrak{a}^p\}$ , then  $\delta_{\mathfrak{p}} = 1$  or  $0$  according as the completion  $K_{\mathfrak{p}}$  contains  $\mu_p$  or not, and  $\delta_K = 1$  or  $0$  according as  $K$  contains  $\mu_p$  or not.

Of course,  $\dim_{\mathbb{F}_p}(\mathbb{H}^2(\mathcal{G}_{K,S}, \mathbb{Z}/p\mathbb{Z}))$ , giving the minimal number of relations, is easily obtained only when  $P \subseteq S$  (equal to  $\mathrm{rk}_p(\mathcal{T}_{K,S})$  under Leopoldt's conjecture), which shall explain the forthcoming studies about this (e.g., [Koch70, Neu76, Hab78, Win89, Win91, Yam93, NSW00, Mai05, Lab06, Vog07, Sch10, ElHZ18]...).

A.2.2. *Kubota formalism.* Mention that Kubota [Kub57] begins the study of the structure of the dual  $\mathcal{A}_{K,S}^*$  of  $\mathcal{A}_{K,S}$ , study which is based on the Grunwald–Wang theorem and which leads to a characterization of this group in terms of its fundamental invariants called, following Kaplansky, the “Ulm invariants”.

Then in [Miki78], Miki uses this formalism, about  $\ell(=p)$ -ramification, then class field theory, Iwasawa's theory, in direction of Leopoldt's conjecture. Some statements, equivalent to some results that we shall recall in this survey (as well as the notion of  $p$ -rationality and its main properties), should be mentioned in his paper, despite the difficulty of translating vocabulary and technique.

**A.3. Main developments after the pioneering works.** The computation of  $\mathrm{rk}_p(\mathcal{T}_{K,P})$ , from Kummer theory, is already given in [BP72], then in [Gra82, Théorèmes I.2, I.3, Corollaire 1] and by many authors, for instance by means of cohomological techniques (e.g., [Mov90, Proposition 3]).

This will give reflection formulas.

A.3.1. *Reflection and rank formulas.* [Gra98, Chapitre III, § 10]. From the Šafarevič formula and Kummer theory when  $K$  contains the group  $\mu_p$  of  $p$ th roots of unity, writing:

$$P = S \cup \Sigma \text{ with } S \cap \Sigma = \emptyset,$$

one obtains the reflection theorem in its simplest form:

$$(A.2) \quad \mathrm{rk}_p(\mathcal{A}_{K,S}^{\Sigma}) - \mathrm{rk}_p(\mathcal{A}_{K,\Sigma}^{S \text{ res}}) = \#S - \#\Sigma + \sum_{\mathfrak{p} \in S} [K_{\mathfrak{p}} : \mathbb{Q}_p] - r_1 - r_2,$$

where  $\mathcal{A}_{K,S}^{\Sigma}$  is the Galois group of the maximal abelian pro- $p$ -extension of  $K$  in  $H_{K,S}$ , which is  $\Sigma \cup \{\infty\}$ -split (i.e., in which all the places of  $\Sigma \cup \{\infty\}$  split completely), and similarly for the definition of  $\mathcal{A}_{K,\Sigma}^{S \text{ res}}$ , in the restricted sense for  $p = 2$  (i.e., only  $S$ -split).

The case  $S = P$  leads to the following well-known result:

**Theorem A.1.** [Gra03, Proposition III.4.2.2] *Let  $K$  be any number field fulfilling the Leopoldt conjecture for the prime  $p$ . Let  $K' := K(\mu_p)$ ,  $P'$  the set of  $p$ -places above  $P$  in  $K'$ , and let  $P^{\text{dec}}$  be the set of  $p$ -places of  $K$  totally split in  $K'$ . Let  $\omega$  be the Teichmüller character and denote by  $\text{rk}_\omega$  the  $p$ -rank of an isotopic  $\omega$ -component for  $\text{Gal}(K'/K)$ :*

$$\text{rk}_p(\mathcal{T}_{K,P}) = \text{rk}_\omega(\mathcal{C}_{K'}^{P',\text{res}}) + \#P^{\text{dec}} - \delta_K,$$

where  $\mathcal{C}_{K'}^{P',\text{res}}$  is the quotient of the  $p$ -class group  $\mathcal{C}_{K'}^{\text{res}}$  by the subgroup generated by the classes of  $P'$  (in the restricted sense for  $p = 2$ ).

(i) If  $\mu_p \subset K$ , we then have  $\text{rk}_p(\mathcal{T}_{K,P}) = \text{rk}_p(\mathcal{C}_K^{P,\text{res}}) + \#P - 1$ .

(ii) We have  $\mathcal{T}_{K,P} = 1$  if and only if:

- $\mu_p \not\subset K$ : then  $P^{\text{dec}} = \emptyset$  and the  $\omega$ -component of  $\mathcal{C}_K^{\text{res}}$  is trivial;
- $\mu_p \subset K$ :  $p$  does not split in  $K/\mathbb{Q}$  and the unique  $\mathfrak{p} \in P$  generates  $\mathcal{C}_K^{\text{res}}$ .

**Example A.2.** For  $K = \mathbb{Q}(\mu_p) =: \mathbb{Q}(\zeta_p)$ ,  $p \neq 2$ , taking  $\Sigma = \emptyset$  and  $S = P$ :

$$\text{rk}_p(\mathcal{A}_{K,S}) - \text{rk}_p(\mathcal{A}_{K,\emptyset}^P) = 1 + p - 1 - \frac{p-1}{2} = \frac{p+1}{2}.$$

Since  $\mathcal{A}_{K,\emptyset}^P = \mathcal{C}_K / \langle \mathcal{C}_K(\mathfrak{p}) \rangle$ , with  $\mathfrak{p} = (1 - \zeta_p)$ , and  $\mathcal{A}_{K,P} \simeq \mathbb{Z}_p^{\frac{p+1}{2}} \oplus \mathcal{T}_{K,P}$ , this yields:

$$(A.3) \quad \text{rk}_p(\mathcal{T}_{K,P}) = \text{rk}_p(\mathcal{C}_K),$$

as well as the writing  $\text{rk}_p(\mathcal{T}_{K,P}^\pm) = \text{rk}_p(\mathcal{C}_K^\mp)$  (for analogous equalities with pairs of isotopic components associated by means of the mirror involution, and the consequences for Vandiver's conjecture, see [Gra19b, § 3.1]).

If the condition  $S \cup \Sigma = P$  is not fulfilled, we have (still assuming  $\mu_p \subset K$ ) the reflection formula, where  $\mathfrak{m}^* := \prod_{\mathfrak{p} \in \Sigma} \mathfrak{p}^{pe_{\mathfrak{p}}+1} \cdot \prod_{\mathfrak{p} \in P \setminus S \cup \Sigma} \mathfrak{p}^{pe_{\mathfrak{p}}}$ :

$$(A.4) \quad \text{rk}_p(\mathcal{A}_{K,S}^\Sigma) - \text{rk}_p(\mathcal{C}_K^{S,\text{res}}(\mathfrak{m}^*)) = \#S - \#\Sigma + \sum_{\mathfrak{p} \in S} [K_{\mathfrak{p}} : \mathbb{Q}_p] - r_1 - r_2,$$

where  $\mathcal{C}_K^{S,\text{res}}(\mathfrak{m}^*)$  is the  $S$ -split  $p$ -ray class group of modulus  $\mathfrak{m}^*$  (see [Gra03, Exercise II.5.4.1 (iii)] and (iv) for the case  $p = 2$ ). Note that  $\mathcal{C}_K^{S,\text{res}}(\mathfrak{m}^*)$  is isomorphic to a quotient of  $\mathcal{A}_{K,P \setminus S}^{S,\text{res}}$ .

Finally, if  $K$  does not contain  $\mu_p$ , but assuming  $P = S \cup \Sigma$  with  $S \cap \Sigma = \emptyset$ , the general formula is:

$$(A.5) \quad \text{rk}_p(\mathcal{T}_{K,S}^\Sigma) = \text{rk}_\omega(\mathcal{A}_{K',\Sigma'}^{S,\text{res}}) + \sum_{\mathfrak{p} \in S} \delta_{\mathfrak{p}} - \delta_K - \#\Sigma - (r_1 + r_2 - 1 - r_{K,S}^\Sigma),$$

where  $r_{K,S}^\Sigma = \sum_{\mathfrak{p} \in S} [K_{\mathfrak{p}} : \mathbb{Q}_p] - \tilde{r}_{K,S}^\Sigma$ ; here,  $\tilde{r}_{K,S}^\Sigma \leq r_2 + 1$  is the  $\mathbb{Z}_p$ -rank of  $\mathbb{Z}_p \log_S(I_{K,S})$  modulo  $\mathbb{Q}_p \log_S(E_K^\Sigma)$  dealing with the group of  $\Sigma$ -units of  $K$  (see also [Mai05, Vog07] for some applications).

One can restrict some of the above equalities to  $p$ -class groups, giving only inequalities on the  $p$ -ranks (Hecke theorem (1910), Scholz theorem (1932), Leopoldt Spiegelungssatz (1958), Armitage–Fröhlich–Serre, Oriat, for  $p = 2$ . For reflection theorems and formulas with characters, see [Gra03, II.5.4, Theorem II.5.4.5]) from [Gra98, Ch. I, Theorem 5.18] where  $p$ -rank formulas link  $p$ -class groups and torsion groups as in Theorem A.1 (a context used by Ellenberg–Venkatesh in [EV07] for the  $\varepsilon$ -conjecture on  $p$ -class groups).

For the annihilation of the Galois module  $\mathcal{T}_{K,P}$ , of real abelian extensions  $K/\mathbb{Q}$ , in relation with the construction of  $p$ -adic  $L$ -functions and reflection principle, see [Gra18c] and its bibliography. There is probably *equivalent information* whatever the process (algebraic or analytic), as shown by Oriat in [Ori86]. This logical aspect should deserve further investigation.

**A.3.2. Regulators and  $p$ -adic residues of the  $\zeta_p$ -functions.** We continue the story with the  $p$ -adic analytic computations of the residue of the  $p$ -adic  $\zeta$ -function at  $s = 1$  of real abelian fields  $K$  by Amice–Fresnel [AF72], from Kubota–Leopoldt  $L_p$ -functions (1964), by Coates [Coa77], Serre [Ser78] introducing  $p$ -adic pseudo-measures, then by Colmez [Col88] in full generality, via the formula  $\frac{1}{2^{[K:\mathbb{Q}]-1}} \lim_{s \rightarrow 1} (s-1) \zeta_{K,p}(s) = \frac{R_p h E_p(1)}{\sqrt{D}}$ , where  $R_p$  is the classical  $p$ -adic regulator,  $h$  the class number,  $D$  the discriminant of  $K$  and  $E_p(1)$  the eulerian factor  $\prod_{\mathfrak{p}|p} (1 - N\mathfrak{p}^{-1})$ .

The normalised  $p$ -adic regulator  $\mathcal{R}_{K,P}$  (2.2), for totally real fields, is given (under Leopoldt’s conjecture) by the expression [Gra18a, Proposition 5.2]:

$$\#\mathcal{R}_{K,P} \sim \frac{1}{2} \cdot \frac{(\mathbb{Z}_p : \log(N_{K/\mathbb{Q}}(U_{K,P})))}{\#\mathcal{W}_{K,P} \cdot \prod_{\mathfrak{p}|p} N\mathfrak{p}} \cdot \frac{R_p}{\sqrt{D}},$$

where  $\sim$  means equality up to a  $p$ -adic unit factor; whence:

$$\frac{1}{2^{[K:\mathbb{Q}]-1}} \lim_{s \rightarrow 1} (s-1) \zeta_{K,p}(s) = \frac{1}{p^{[K \cap \mathbb{Q}^c:\mathbb{Q}]}} \#\mathcal{T}_{K,P},$$

where  $\mathbb{Q}^c$  is the  $\mathbb{Z}_p$ -cyclotomic extension of  $K$ .

Mention the relative version of the Coates formula in the totally real case:

**Theorem A.3.** [Gra82, Théorème III.3]. *Let  $L/K$  be an abelian extension of totally real number fields fulfilling the Leopoldt conjecture. Let  $\mathcal{N}_{L/K}$  be the group of local norms and let  $\mathcal{C}_{L/K}^{\text{gen}} := \text{Gal}(H_L^{\text{ab}}/LH_K)$  be the  $p$ -genus group in  $L/K$ ; the superscript  $*$  denotes  $\text{Ker}(N_{L/K})$ . Then:*

$$\begin{aligned} \#\mathcal{T}_{L,P} &\sim \frac{\#\mathcal{T}_{K,P}}{[L \cap H_{K,P} : L \cap K^c]} \times \\ &\frac{\prod_{\mathfrak{p}|p} e_{\mathfrak{p},p}}{[L : L \cap H_{K,P}]} \times \#\mathcal{C}_{L/K}^{\text{gen}} \times (E_K \cap \mathcal{N}_{L/K} : N_{L/K}(E_L)) \times \\ &(\log_P(U_{L,P}^*) : \log_P(\overline{E}_L^*)) \times \#(\text{tor}_{\mathbb{Z}_p}(U_{L,P}^*)/\mu_p^*), \end{aligned}$$

where  $\mu_p^* = 1$  for  $p \neq 2$  and  $\#\mu_2^* = \text{gcd}(2, [L : K])$ .



A.3.3. *Cohomological interpretation.* In [Nqd86], Nguyen Quang Do gives the cohomological interpretation of the dual of  $\mathcal{T}_{K,P}$ :  $\mathcal{T}_{K,P}^* \simeq \mathrm{H}^2(\mathcal{G}_{K,P}, \mathbb{Z}_p)$ , considered as the first of the mysterious non positive twists  $\mathrm{H}^2(\mathcal{G}_{K,P}, \mathbb{Z}_p(i))$  of the motivic cohomology; for concrete results of genus type about the corresponding case of motivic tame kernels, see [AM19] and its important bibliography.

It is indeed well known that  $\mathrm{H}^2(\mathcal{G}_{K,P}, \mathbb{Z}_p)$  does appear as a tricky obstruction in many questions of Galois theory over number fields, whatever the technical approach.

But considering the two “equivalent” invariants  $\mathrm{H}^2(\mathcal{G}_{K,P}, \mathbb{Z}_p)$  and  $\mathcal{T}_{K,P}$ , only the last one may be used, with arithmetic or analytic tools, to obtain numerical experiments and to understand the true intrinsic  $p$ -adic difficulties.

A.3.4. *Principal Conjectures and Theorems.* Considering the invariants  $\mathcal{C}_K$  and  $\mathcal{T}_{K,P}$  as fundamental objects, we have given, for the abelian fields  $K$ , the conjectural behaviour of their isotopic  $\chi$ -components for irreducible  $p$ -adic characters  $\chi$  [Gra77]; the proofs of these conjectures and of some improvements in Iwasawa’s theory are well known and the reader may refer to the illuminating paper of Ribet [Rib08] about the so-called “Principal Theorem” stemming from Bernoulli–Kummer–Herbrand then Ribet–Mazur–Wiles–Thaine–Rubin–Kolyvagin–Greither works on cyclotomy and  $p$ -adic  $L$ -functions, as a prelude of wide generalizations in the same spirit.

A.4. **Basic  $p$ -adic properties of  $\mathcal{A}_{K,P}$  &  $\mathcal{T}_{K,P}$ .** During the 1980’s, we have written in [Gra82, Gra83, Gra84] the main properties of the groups  $\mathcal{T}_{K,P}$  with their behaviour in any extension  $L/K$  and proved (assuming Leopoldt’s conjecture in the Galois closure of  $L$ ) that the transfer maps:

$$\mathcal{A}_{K,P} \longrightarrow \mathcal{A}_{L,P} \quad \& \quad \mathcal{T}_{K,P} \longrightarrow \mathcal{T}_{L,P}$$

are always injective [Gra82, Théorème I.1]; which has major consequences for the arithmetic of number fields (e.g., non-capitulation in an extension contrary to class groups). Of course, this property has been obtained soon after by Jaulent, Nguyen Quang Do and others with different techniques.

A.4.1. *The  $p$ -adic  $\mathrm{Log}_S$ -functions.*

**Definition A.4.** [Gra83, § 2, Théorème 2.1],[Gra03, § III.2.2]. Let  $I_{K,P}$  be the group of prime to  $p$  ideals of  $K$ . We define the logarithm function:

$$\mathrm{Log}_P : I_{K,P} \longrightarrow \left( \bigoplus_{\mathfrak{p} \in P} K_{\mathfrak{p}} \right) / \mathbb{Q}_p \log_P(E_K)$$

as follows. For any ideal  $\mathfrak{a} \in I_{K,P}$  let  $m$  be such that  $\mathfrak{a}^m =: (\alpha)$ ,  $\alpha \in K^\times$ , then  $\mathrm{Log}_P(\mathfrak{a}) := \frac{1}{m} \log_P(\alpha) \pmod{\mathbb{Q}_p \log_P(E_K)}$ .

The main property of  $\mathrm{Log}_P$  is that for any ideal  $\mathfrak{a} \in I_{K,P}$ ,  $\mathrm{Log}_P(\mathfrak{a})$  defines the Artin symbol in the compositum  $\widetilde{K}^P$  of the  $\mathbb{Z}_p$ -extensions of  $K$  by means

of the canonical exact sequence:

$$1 \rightarrow \mathcal{T}_{K,P} \rightarrow \mathcal{A}_{K,P} \xrightarrow{\text{Log}_P} \text{Log}_P(I_{K,P}) \simeq \text{Gal}(\widetilde{K}^P/K) \rightarrow 1,$$

which may be generalized with arbitrary  $S \subseteq P$ :

$$1 \rightarrow \mathcal{T}_{K,S} \rightarrow \mathcal{A}_{K,S} \xrightarrow{\text{Log}_S} \text{Log}_S(I_{K,S}) \simeq \text{Gal}(\widetilde{K}^S/K) \rightarrow 1,$$

with an obvious definition of  $\text{Log}_S(\mathfrak{a})$  in  $\bigoplus_{\mathfrak{p} \in S} K_{\mathfrak{p}}$  modulo  $\mathbb{Q}_p \log_S(E_K)$ .

This formalism is equivalent to that given by the theory of profinite  $p$ -groups (here  $\mathcal{G}_{K,P}$ ), but may yield numerical computations as follows:

The formula for  $\#\mathcal{T}_{K,S}$ ,  $S \subseteq P$ , is the following [Gra86, Theorems III.2.5], [Gra03, Corollary III.2.6.1] (under Leopoldt's conjecture):

$$(A.6) \quad \#\mathcal{T}_{K,S} = \#\mathcal{W}_{K,S} \times \#\mathcal{R}_{K,S} \times \frac{\#\mathcal{C}_K}{(\mathbb{Z}_p \text{Log}_S(I_{K,S}) : \mathbb{Z}_p \text{Log}_S(P_{K,S}))},$$

where  $P_{K,S}$  is the group of principal ideals prime to  $S$ , so that  $\mathbb{Z}_p \text{Log}_S(P_{K,S})$  depends obviously on  $\log_S(U_{K,S})$ . When  $S \subsetneq P$ ,  $\mathcal{W}_{K,S}$  is not necessarily equal to  $\text{tor}_{\mathbb{Z}_p}(U_{K,S})/\iota_S(\mu_K)$  (cf. Lemmas 2.1, 2.2).

The denominator in (A.6) gives the degree  $[\widetilde{K}^S \cap H_K : K]$ .

For  $S = P$ , the  $\text{Log}_P$ -function allows, when  $\mu_p \subset K$ , the numerical determination of the initial Kummer radical contained in  $\widetilde{K}^P$  [Gra85, Jau86].

**A.4.2. Fixed point formula.** Then we have obtained a fixed point formula for  $S = P$  which, contrary to Chevalley's formula for class groups in cyclic extensions [Che33], does exist whatever the Galois extension  $L/K$  ([Gra83, § 5], [Jau84, Section 2 (c)], [Gra86, Proposition 6], [Mov88, Appendice I],[MN90, Appendice]):

**Theorem A.5.** [Gra03, § IV.3, Theorem 3.3]. *Let  $L/K$  be a Galois extension of number fields and  $G := \text{Gal}(L/K)$ . Let  $p$  be a prime number; we assume that  $L$  satisfies the Leopoldt conjecture for  $p$ . Then:*

$$\#\mathcal{T}_{L,P}^G = \#\mathcal{T}_{K,P} \times \frac{\prod_{\mathfrak{l} \nmid p} e_{\mathfrak{l},p}}{\left( \sum_{\mathfrak{l} \nmid p} \frac{1}{e_{\mathfrak{l},p}} \mathbb{Z}_p \text{Log}_P(\mathfrak{l}) + \mathbb{Z}_p \text{Log}_P(I_{K,P}) : \mathbb{Z}_p \text{Log}_P(I_{K,P}) \right)},$$

where  $e_{\mathfrak{l},p}$  is the  $p$ -part of the ramification index of  $\mathfrak{l}$  in  $L/K$ .

**Remark A.6.** Contrary to the computation of  $\text{tor}_{\mathbb{Z}_p}(U_{K,P}/\overline{E}_K^P)$ , that of the  $\mathbb{Q}_p$ -vector space  $\mathbb{Q}_p \log_P(E_K)$  does not need the knowledge of the group of units  $E_K$ ; it only depends of Leopoldt's conjecture (assumed) and its  $\mathbb{Q}_p$ -dimension is  $r_1 + r_2 - 1$ ; the case of  $\mathbb{Q}_p \log_S(E_K)$  is more mysterious.

The case of totally real fields is easier since the  $\text{Log}$ -function trivializes because we have  $\bigoplus_{\mathfrak{p} \in P} K_{\mathfrak{p}} = \mathbb{Q}_p \log_P(E_K) \oplus \mathbb{Q}_p$ , which allows explicit computations [Gra82, Théorème III.1]:

**Corollary A.7.** [Gra03, Exercise IV.3.3.1]. *In the case of a totally real number field  $L$ , the above formula becomes (under Leopoldt's conjecture):  $\#\mathcal{T}_{L,P}^G = \mathcal{T}_{K,P} \cdot p^{\rho-r} \cdot \prod_{\mathfrak{l}|p} e_{\mathfrak{l},p}$ , where  $p^r \sim [L : K]$  and  $\rho$  only depends on the decomposition of the ramified primes  $\mathfrak{l} \nmid p$  in  $L/K$ .*

A.4.3.  *$p$ -primitive ramification.* The fixed point formula of Theorem A.5 allows to characterize the case where  $\#\mathcal{T}_{L,P} = 1$  in a  $p$ -extension  $L/K$ :

**Corollary A.8.** *Let  $L/K$  be any finite  $p$ -extension. Then  $\mathcal{T}_{L,P} = 1$  if and only if the two following conditions are fulfilled (under Leopoldt's conjecture):*

- (i)  $\mathcal{T}_{K,P} = 1$ ;
- (ii)  $\left( \sum_{\mathfrak{l}|p} \frac{1}{e_{\mathfrak{l},p}} \mathbb{Z}_p \text{Log}_P(\mathfrak{l}) + \mathbb{Z}_p \text{Log}_P(I_{K,P}) : \mathbb{Z}_p \text{Log}_P(I_{K,P}) \right) = \prod_{\mathfrak{l}|p} e_{\mathfrak{l},p}$ .

**Definition A.9.** [Gra03, §IV.3, (b)]. When the condition (ii) is fulfilled, we say that the  $p$ -extension  $L/K$  is  $p$ -primitively ramified and that the set  $T$  of tame places  $\mathfrak{l}$ , ramified in  $L/K$ , is primitive [Gra86, Ch. III, Definition & Remark], which is equivalent (in terms of Frobenius automorphisms) to:

$$(A.7) \quad \text{Gal}(\widetilde{K}^P/K) \simeq \mathcal{A}_{K,P}/\mathcal{T}_{K,P} = \bigoplus_{\mathfrak{l} \in T} \langle \left( \frac{\widetilde{K}^P}{\mathfrak{l}} \right) \rangle.$$

Of course, any  $P$ -ramified extension is  $p$ -primitively ramified.

Then in [Gra86, Ch. III, §2, Theorem 2 & Corollary] are characterized, for  $p = 2$  and  $p = 3$ , the abelian  $p$ -extensions  $K$  of  $\mathbb{Q}$  such that  $\mathcal{T}_{K,P} = 1$ . This is connected with the “regular kernel” of  $K$  which, from results of Tate, follows similar properties which have been explained in a joint work with Jaulent [GJ89] and developped in [JN93]. We can state:

**Theorem A.10.** [Gra03, Theorem III.4.2.5, Theorem IV.3.5]. *Let  $K$  be any number field. The following properties are equivalent:*

- (i)  $K$  satisfies the Leopoldt conjecture at  $p$  and  $\mathcal{T}_{K,P} = 1$ ;
- (ii)  $\mathcal{A}_{K,P} := \mathcal{G}_{K,P}^{\text{ab}} = \text{Gal}(H_{K,P}/K) \simeq \mathbb{Z}_p^{r_2+1}$ ,
- (iii) the Galois group  $\mathcal{G}_{K,P}$  is a free pro- $p$ -group on  $r_2 + 1$  generators, which is equivalent to fulfill the following four conditions:

- $K$  satisfies the Leopoldt conjecture at  $p$ ,
- $\mathcal{C}_K \simeq \mathbb{Z}_p \text{Log}_P(I_{K,P}) / (\log_P(U_{K,P}) + \mathbb{Q}_p \log_P(E_K))$ ,
- $\text{tor}_{\mathbb{Z}_p}(U_K) = \mu_p(K)$ ,
- $\mathbb{Z}_p \log_P(E)$  is a direct summand in  $\log_P(U_{K,P})$ .

## A.5. New formalisms and use of pro- $p$ -group theory.

A.5.1. *Infinitesimal arithmetic.* [Jau84, Jau86, Jau94]. At the same time, in his Thesis, Jaulent defines the *infinitesimal arithmetic* in a number field proving, in a nice conceptual framework, generalizations of our previous results, especially in the new context of *logarithmic classes*, adding Iwasawa theory results, study of the  $p$ -regularity (replacing  $\mathcal{T}_{K,P}$  by the tame kernel  $K_2(Z_K)$  of the ring of integers of  $K$ ), and genus theory.

In the same technical context Jaulent writes in [Jau98, Jau02] a  $\ell (= p)$ -adic class field theory and a logarithmic class field theory developed later in much papers, including computational methods [BJ16]. He studies the logarithmic class group  $\tilde{\mathcal{C}}_K$  whose finiteness is equivalent to the Gross conjecture (a survey is given in [Gra03, § III.7]).

**A.5.2. Pro- $p$ -group theory version.** Shortly after, at the end of the 1980's, in his thesis, Movahhedi [Mov88, Mov90] gives a wide study of the abelian  $p$ -ramification theory, using mainly the properties of the pro- $p$ -group  $\mathcal{G}_{K,S}$  and deduces again most of the previous items, then gives the main structural and cohomological properties of  $\mathcal{G}_{K,P}$  and the classical characterization of the triviality of  $\mathcal{T}_{K,P}$ . He proposes for this to speak of “ $p$ -rational fields” [Mov90, Definitionn 1], that is to say the number fields  $K$  such that Leopoldt's conjecture holds for  $p$  and  $\mathcal{T}_{K,P} = 1$  (cf. A.10); this was inspired by the fact that  $\mathbb{Q}$  is (obviously)  $p$ -rational for all  $p$ . This vocabulary has been adopted by the arithmeticians.

Then Movahhedi gives properties of  $p$ -rational extensions  $L/K$  and the reciprocal of our result characterizing the  $p$ -rationality in a  $p$ -extension  $L/K$ , in other words the “going up” of the  $p$ -rationality:

**Theorem A.11.** [Mov88, Théorème 3, § 3] *Let  $L/K$  be a  $p$ -extension of number fields. The field  $L$  is  $p$ -rational if and only if  $K$  is  $p$ -rational and the set  $T$  of tame primes, ramified in  $L/K$ , is  $p$ -primitive in  $K$ . Moreover, under these conditions, the extension  $T(L)$  of  $T$  to  $L$  is  $p$ -primitive.*

This implies that if  $K$  is  $p$ -rational and  $T$   $p$ -primitive, then any  $T$ -ramified  $p$ -extension  $L/K$  fulfills the Leopoldt conjecture and  $T(L)$  is  $p$ -primitive (a particular case was given in [Gra82, Théorème III.4] for totally real fields).

**Remark A.12.** In practice, in research papers, one assumes in general an universal Leopoldt conjecture, so the above statement becomes:

*$L$  is  $p$ -rational if and only if  $K$  is  $p$ -rational and  $T$  is  $p$ -primitive*  
(equivalent to the fixed point formula of Theorem A.5 and Corollary A.8).

In the 1990's, the classical results on  $p$ -ramification and  $p$ -regularity, about the triviality of the tame kernel  $K_2(\mathbb{Z}_K)$ , are amply illustrated in various directions by Movahhedi, Nguyen Quang Do, Jaulent (see [Mov90, MN90, JN93] and [BG92, JS97, Jau98]): pro- $p$ -group theory with explicit determination of a system of generators and relations for  $\mathcal{G}_{K,S}$ , Galois cohomology, Iwasawa's theory, Leopoldt and Gross conjectures.

Recall that in [Jau87, Scolie, p. 112] Jaulent shows that the nullity of the  $p$ -Hilbert kernel  $H_2(L) \otimes \mathbb{Z}_p$  implies Leopoldt and Gross conjectures. Moreover [Jau98] deals with ramification and decomposition.

Under the assumptions:  $\mu_p \subset K$ ,  $H_2(L) \otimes \mathbb{Z}_p = 0$  and the existence of  $\mathfrak{p}_0 \in S$  such that  $\mu_{K_{\mathfrak{p}_0}} = \mu_K$ , some results in [Nqd91], after [Mov88, MN90] on the primitive reciprocity laws, describe (by means of generators and relations) the Galois group  $\mathcal{G}_{K,S}$ .

A.5.3. *Synthesis 2003–2005.* Because our Crellé papers, were written in french, whence largely ignored, all the results and consequences, that we have given in [Gra77, Gra82, Gra83, Gra84, Gra85, Gra86, Gra98], were widely developed in [Gra03] where a systematic and general use of ramification and decomposition is considered, the infinite places playing a specific role (decomposition or complexification).

Furthermore, [Gra03, Theorem V.2.4 and Corollary V.2.4.2] give a characterisation (with explicit governing fields) of the existence of degree  $p$  cyclic extensions of  $K$  with given ramification and decomposition. This criteria has been used by Hajir–Maire and Hajir–Maire–Ramakrishna in several of their papers for results on  $S$ -ramified pro- $p$ -groups (see, e.g., [HMR19a, Theorem 5.3], [HMR19b, Remark 2.2.] for the most recent publications).

**A.6. Present theoretical and algorithmic aspects.** One may say that there is no important progress for  $p$ -rationality, for itself, since  $p$ -rational fields are in some sense the “simplest fields”, but that the significance of the  $p$ -adic properties of the groups  $\mathcal{T}_{K,S}$ , in much domains of number theory, has given a great lot of heuristics, conjectures, computations; so we shall now describe some of these aspects with some illustrations (it is not possible to be comprehensive since the concerned literature becomes enormous).

A.6.1. *Absolute abelian Galois group  $A_K$  of  $K$ .* Let  $K^{\text{ab}}$  be the maximal abelian extension of  $K$ . In [AS13] Angelakis–Stevenhagen, after some work by Onabe [Ona76] and Kubota [Kub57], provide a direct computation of the profinite group  $A_K := \text{Gal}(K^{\text{ab}}/K)$  for imaginary quadratic fields  $K$ , and use it to obtain many different  $K$  that all have the same “minimal” absolute abelian Galois group, which is in some sense a condition of minimality of the groups  $\mathcal{T}_{K,P}$  for all primes  $p$ . They obtain for instance, among other results and numerical illustrations:

**Theorem A.13.** [AS13, Theorem 4.1 & Section 7]. *An imaginary quadratic field  $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2})$  of class number 1 has absolute abelian Galois group isomorphic to  $\widehat{\mathbb{Z}}^2 \times \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$ .*

This corresponds to the fact that such fields are  $p$ -rational for all  $p$  (up to the factors  $\mathcal{W}_{K,P}$  for  $p = 2, 3$ ). Then the generalization to an arbitrary  $K$  involves the  $\mathcal{T}_{K,P}$  for all primes  $p$ , giving:

**Theorem A.14.** [Gra14, Theorem 2.1 & Corollary 2.1]. *Let  $K^{\text{ab}}$  be the maximal Abelian pro-extension of  $K$ . Let  $\mathcal{H}_K$  be the compositum, over  $p$ , of the maximal  $P$ -ramified Abelian pro- $p$ -extensions  $H_{K,P}$  of  $K$ . Under the Leopoldt conjecture, there exists an Abelian extension  $L_K$  of  $K$  such that  $\text{Gal}(L_K/K) \simeq \prod_p \mathcal{T}_{K,P}$  and such that  $\mathcal{H}_K$  is the direct compositum over  $K$  of  $L_K$  and the maximal  $\widehat{\mathbb{Z}}$ -extension of  $K$ , and such that we have the non-canonical isomorphism (for some explicit integers  $\delta$  and  $w$ ):*

$$\text{Gal}(K^{\text{ab}}/L_K) = \widehat{\mathbb{Z}}^{r_2+1} \times \text{Gal}(K^{\text{ab}}/\mathcal{H}_K) \simeq \widehat{\mathbb{Z}}^{r_2+1} \times \prod_{n \geq 1} \left( (\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/wn\mathbb{Z} \right).$$

Angelakis–Stevenhagen conjecture in [AS13, Conjecture 7.1] the infiniteness of imaginary quadratic fields  $K$  such that  $A_K \simeq \widehat{\mathbb{Z}}^2 \times \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$ .

Note that when the  $p$ -class group of  $K$  is non-trivial,  $K$  is  $p$ -rational if and only if  $\mathcal{C}_K$  is cyclic and if the  $p$ -Hilbert class field  $H_K$  is contained in  $\widetilde{K}^P$  (assuming  $\mathcal{W}_{K,P} = 1$ ).

Whence the importance of fields  $K$  being  $p$ -rational for all  $p$  (or more precisely such that  $\mathcal{T}_{K,P} = \mathcal{W}_{K,P}$  for all  $p$ ); it is an easier problem only for  $\mathbb{Q}$  and imaginary quadratic fields, but dreadfully difficult when  $K$  contains units of infinite order since it is an analogous question as for Fermat’s quotients of algebraic numbers (various heuristics and conjectures in [Gra16]), or values of  $L$ -functions which intervene as in [CL18, CL19, Gor01], and more or less, in many papers as [BGKK18] when the normalized  $p$ -adic regulator is a unit. We have conjectured that, in any given number field  $K$ ,  $\mathcal{T}_{K,P} = 1$  for almost all  $p$ .

**A.6.2. Greenberg’s conjecture on Iwasawa’s  $\lambda$ ,  $\mu$ .** [Gre76]. For a totally real number field  $K$ , consider (under the Leopoldt conjecture) the cyclotomic  $\mathbb{Z}_p$ -extension  $K^c$  of  $K$ . Then Greenberg has conjectured that the Iwasawa’s invariants  $\lambda$  and  $\mu$  are zero.

Many equivalent formulations of this conjecture have been given (we give up to provide a bibliography), but we must mention that the two invariants  $\mathcal{T}_{K,P}$  and  $\widetilde{\mathcal{C}}_K$  (the logarithmic class group of Jaulent) are in some sense “governing invariants” for the Greenberg conjecture; for instance, as soon as  $\mathcal{T}_{K,P} = 1$  or  $\widetilde{\mathcal{C}}_K = 1$ , Greenberg’s conjecture is true for trivial reasons. For this, see [Gra17a, Théorèmes 3.4, 4.8, 6.3] and [Gra18b] about  $\mathcal{T}_{K,P}$ , then the interpretation by Jaulent with the group of universal norms [Jau19b] and the following criterion (under the Gross-Leopoldt conjecture):

**Theorem A.15.** [Jau18a, Théorème 7, § 1.4]. *The totally real number field  $K$  fulfills the conjecture of Greenberg if and only if its logarithmic class group  $\widetilde{\mathcal{C}}_K$  capitulates in  $K^c$ .*

If Greenberg’s conjecture is true (which is no doubt), such general condition of capitulation is very reassuring since we recall that, on the contrary, the group  $\mathcal{T}_{K,P}$  *never capitulates*. Moreover the property of capitulation (well known in Hilbert’s class fields) is more general for generalized ray class groups and, especially, is possible in *absolute abelian extensions* as shown in many papers including [Gra97, Bos09, Jau18b, Jau19a].

**A.6.3. Galois representations with open image.** [Gre16]. For constructions by Greenberg of continuous Galois representations  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_n(\mathbb{Z}_p)$  with open image, the  $p$ -rational fields play a great role, and the first obvious case is that of  $p$ -regular cyclotomic fields  $\mathbb{Q}(\mu_p)$  which are  $p$ -rational (yet reported by [Sha64], [Gra86], and generalized by introducing in [GJ89] the notion of  $p$ -regularity of number fields that we do not develop in this paper, for short, but which behaves as  $p$ -rationality; see a survey in [JN93]).

Then, an interesting typical conjecture is the following:

**Conjecture A.16.** [Gre16, Conjecture 4.2.1]. *For any odd prime  $p$  and for any  $t \geq 1$ , there exists a  $p$ -rational field  $K$  such that  $\text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^t$ .*

Numerical examples and statistics have been given for various  $p$  and  $t$ ; see [Gre16] and (by Robert Bradshaw) the 3-rationality of:

$$K = \mathbb{Q}(\sqrt{13}, \sqrt{145}, \sqrt{209}, \sqrt{269}, \sqrt{373}, \sqrt{-1}).$$

Some PARI/GP programs are given in [Pit10, PV15], and [Gra17c, §5.2] showing the 3-rationality of:

$$K = \mathbb{Q}(\sqrt{-2}, \sqrt{-5}, \sqrt{7}, \sqrt{17}, \sqrt{-19}, \sqrt{59}).$$

For fixed  $p$  (e.g.,  $p = 3$ ), the probability of  $p$ -rationality decreases dramatically when  $t \rightarrow \infty$ .

A.6.4. *Order of magnitude of  $\mathcal{T}_{K,P}$  and conjectures.* We have conjectured in [Gra16, Conjecture 8.11] that for a fixed number field  $K$ ,  $\mathcal{T}_{K,P} = 1$  for all  $p \gg 0$ . Moreover, all numerical calculations show that the non- $p$ -rationality constitutes an exception.

In another direction, fixing  $p$  and taking  $K$  in some given infinite family  $\mathcal{K}$  (e.g., real fields of given degree  $d$ ) we have given extensive numerical computations in direction of the following “ $p$ -adic Brauer–Siegel” theorem:

**Conjecture A.17.** [Gra19a, Conjecture 8.1]. *There exists a constant  $\mathcal{C}_p(\mathcal{K})$  such that:*

$$v_p(\#\mathcal{T}_{K,p}) \leq \mathcal{C}_p(\mathcal{K}) \cdot \frac{\log_\infty(\sqrt{D_K})}{\log_\infty(p)},$$

for all  $K \in \mathcal{K}$ , where  $\log_\infty$  is the usual complex logarithm.

Thus there are two questions about  $C_p(K) := \frac{v_p(\#\mathcal{T}_{K,p}) \cdot \log_\infty(p)}{\log_\infty(\sqrt{D_K})}$  and the quantities  $\mathcal{C}_p := \sup_K(C_p(K))$ ,  $\mathcal{C}_K := \sup_p(C_p(K))$ .

(i) The existence of  $\mathcal{C}_K < \infty$ , for a given  $K$ , only says that the Conjecture:  $\mathcal{T}_{K,P} = 1 \forall p \gg 0$  is true for the field  $K$ ; for this field,  $\limsup_p(C_p(K)) = 0$ .

(ii) If  $\mathcal{C}_p < \infty$  does exist for a given  $p$ , we have an universal  $p$ -adic analog of Brauer–Siegel theorem (the above Conjecture A.17).

These questions being out of reach, many results give, on the contrary, the infinteness of primes  $p$  yielding the  $p$ -rationality of a field  $K$ , in general under the  $abc$  conjecture, and following the method given by [Sil88, GM13, BGKK18, MR19b]; for instance:

**Theorem A.18.** [MR19b, Corollary to Theorem A] *Let  $K$  be a real quadratic field or an imaginary  $S_3$ -extension. If the generalized  $abc$ -conjecture holds for  $K$ , then  $\#\{p \leq x, K \text{ is } p\text{-rational}\} \geq c \cdot \log(x)$  as  $x \rightarrow \infty$ , for some constant  $c > 0$  depending on  $K$ .*

This shows the awesome distance between the two aspects of the problem; indeed, for  $K = \mathbb{Q}(\sqrt{5})$ , no prime number (up to  $p < 10^{14}$  from Elsenhans–Jahnel <https://oeis.org/A060305>) is known giving  $\mathcal{T}_{K,P} \neq 1$ .

A.6.5. *Fermat curves.* To study Fermat curves of exponent  $p$ , one uses the base field  $K = \mathbb{Q}(\mu_p)$  and works in some Kummer extensions; for instance:

(i) Shu [Shu18] gives general formulae of the root numbers of the Jacobian varieties of the Fermat curves  $X^p + Y^p = \delta$ , where  $\delta$  is an integer, and studies their distribution. In this article the Vandiver conjecture or the regularity of  $p$  implies some precise properties of the Selmer groups of these Jacobian varieties.

(ii) Davis–Pries [DP18] work in  $P$ -ramified Kummer extensions of  $K$  with  $P = \{\mathfrak{p} = (1 - \zeta_p)\}$ , as follows. Let  $L \subset H_{K,P}$  be defined by:

$$L = K(\sqrt[r]{\zeta_p}, \sqrt[r]{1 - \zeta_p}, \dots, \sqrt[r]{1 - \zeta_p^r}), \quad r = \frac{p-1}{2},$$

The Kummer radical of  $L$  is also generated by the real cyclotomic units and the numbers  $\zeta_p, 1 - \zeta_p$ . In the same way as previously, non-Vandiver’s conjecture or non-regularity for  $p$  are crucial obstructions.

Under the *Vandiver conjecture*, this radical is of  $p$ -rank  $r + 1$  since it is then given by  $E_K \cdot \langle 1 - \zeta_p \rangle$  modulo  $K^{\times p}$ .

Under the *regularity of  $p$* , we get  $\mathcal{T}_{K,P} = 1$  (reflection theorem (A.3)) and  $L$  is the maximal  $p$ -elementary subextension of  $H_{K,P}$ ;  $L/K$  being  $p$ -ramified, whence  $p$ -primitively ramified (A.4.3), this gives the  $p$ -rationality of  $L$ .

Let  $E$  be the maximal  $p$ -elementary subextension of  $H_{L,P}$ ; since  $\mathcal{T}_{L,P} = 1$  with  $E/L$   $p$ -ramified,  $\mathcal{T}_{E,P} = 1$  and  $\text{rk}_p(\text{Gal}(E/L)) = r \cdot p^{r+1} + 1$ . One can deduce that  $\mathcal{C}_L = \mathcal{C}_E = 1$  since  $E/K$  is totally ramified at  $\mathfrak{p}$  (Theorem A.1 and Chevalley’s formula in any successive  $p$ -cyclic extensions in  $E/K$ ).

In simple cases as  $p = 37$ , where  $\#\mathcal{C}_K = p$  and where  $H_K \subseteq L$  in which  $p$  splits, the formula of Theorem A.1 gives  $\text{rk}_p(\mathcal{T}_{L,P}) = \text{rk}_p(\mathcal{C}_L^P) + p - 1$ , whence  $\text{rk}_p(\text{Gal}(E/L)) = r \cdot p^{r+1} + 2r + 1 + \text{rk}_p(\mathcal{C}_L^P)$  depending on  $\mathcal{C}_L^P$ .

The purpose of [DP18] is to get information on  $H^1(\text{Gal}(E/K), M)$  for some  $\text{Gal}(E/K)$ -modules  $M$ , subquotients of the relative homology  $H_1(U, Y; \mathbb{F}_p)$  of the Fermat curve, where  $U$  is the affine curve  $x^p + y^p = 1$  and  $Y$  the set of  $2p$  cusps where  $xy = 0$ . They completely elucidate the case  $p = 3$ .

**A.7. Computational references and numerical tables.** Many references may be cited. The first table for the computation of  $\#\mathcal{T}_{K,P}$  for imaginary quadratic fields is that of Charifi [Cha82], using formula (A.6). In [Hat87, Hat88] the computations correspond to statistics about the values (modulo  $p$ ) of the normalized regulator  $\mathcal{R}_{K,P}$  of real fields as  $K = \mathbb{Q}(\sqrt{5})$  by the way of Fibonacci numbers and values at  $2 - p$  of zeta-functions.

A very precise study of  $p$ -rationality of imaginary quadratic fields is given by Angelakis–Stevenhagen in [AS13, Section 7].



A wide study of  $\mathcal{T}_{K,P}$ , with tables and publication of PARI/GP programs, is done by Pitoun [Pit10, Chapitre 4], but these more conceptual programs are not so easy to manage by the reader. Then some statistical results with tables are given by Pitoun–Varescon in [PV15].

In [HZ16] Hofmann–Zhang compute the valuation of the (usual)  $p$ -adic regulators of cyclic cubic fields with discriminant up to  $10^{16}$ , for  $3 \leq p \leq 100$ , and observe the distribution of these valuations.

About the conjecture of Greenberg [Gre16] Kraft–Schoof [KS95] have computed such Iwasawa’s invariants and confirm the conjecture for  $p = 3$  and conductors  $f$  of real quadratic fields  $f \not\equiv 1 \pmod{3}$  up to  $10^4$ . In [Gra17c], some heuristics on the conjecture and numerical examples are given with programs; then we illustrate the following conjecture of Hajir–Maire [HM18b, Conjecture 4.16]:

*Given a prime  $p$  and an integer  $m \geq 1$ , coprime to  $p$ , there exist a totally imaginary field  $K_0$  and a degree  $m$  cyclic extension  $K/K_0$  such that  $K$  is  $p$ -rational; it is conjectured that the statement is true taking for  $K_0$  an imaginary  $p$ -rational quadratic field.*

In [BR17, Table 1, § 2], Barbulescu–Ray give explicit  $p$ -rational large compositum of quadratic fields. We may cite some works by Bouazzaoui [Bou18], El Habibi–Ziane [ElHZ18] based on  $p$ -rationality of quadratic fields.

In the similar context, a new PARI/GP package allows the computation of the logarithmic class group  $\tilde{\mathcal{C}}_K$  of a number field by Belabas–Jaulent [BJ16] that we can illustrate as follows where the invariants  $[X, Y, Z]$  are linked by the exact sequence  $1 \rightarrow X \rightarrow Y := \tilde{\mathcal{C}}_K \rightarrow Z := \mathcal{C}_K^P := \mathcal{C}_K / \langle \mathcal{d}_K(P) \rangle \rightarrow 1$ :

```
{P=x^2+3;bp=2;Bp=10^8;K=bnfinit(P,1);print("P=",P);
forprime(p=bp,Bp,H=bnflog(K,p);if(H!=[[],[],[]],print("p=",p,"  ",H)))}
P=x^2 + 3
p=13      [[13], [13], []]
p=181     [[181], [181], []]
p=2521    [[2521], [2521], []]
p=76543   [[76543], [76543], []]
p=489061  [[489061], [489061], []]
p=6811741 [[6811741], [6811741], []]
P=x^2+5
p=5881    [[5881], [5881], []]
```

The case of real quadratic fields is studied in [Gra17a, § 5.2] with a table and in [Jau18a, § 2.4], after the work of Ozaki–Taya [OT95] and others.

More computations would give heuristics to see if the analogous conjecture: “ $\tilde{\mathcal{C}}_K = 1$  for all  $p \gg 0$ ”, is credible or not since the rarefaction of non-trivial cases is similar to that of the groups  $\mathcal{T}_{K,P}$ .

In another direction, the paper [MR19a] of Maire–Rougnant gives examples of triviality of isotopic components of the torsion groups  $\mathcal{T}_{K,P}$ ; more precisely the fields  $K$  are cyclic extensions of  $\mathbb{Q}$  of degrees 3 and 4 (from polynomials of Balady, Lecacheux, Balady–Washington) and  $S_3$ -extensions of  $\mathbb{Q}$ .

In [Gra19a], are given numerous programs to test some heuristics and conjectures about the order of magnitude of the groups  $\mathcal{T}_{K,P}$  in totally real number fields in a Brauer–Siegel framework.

**A.8. Conclusion and open questions.** In all the aspects of  $p$ -rationality that we have developed (theoretical and computational), some interesting applications are done today, including for instance, for the most recent ones, [HM18b] by Hajir–Maire on the  $\mu$ -invariant in Iwasawa’s theory, then [HMR19a] by Hajir–Maire–Ramakrishna, showing the existence of  $p$ -rational fields having large  $p$ -rank of the class group, or [HMR19b] about the existence of a solvable number field  $L$ ,  $P$ -ramified, whose  $p$ -Hilbert class field tower is infinite. See the bibliographies of these articles to expand the list of contributions.

Of course it is not possible to evoke all the studied families of pro- $p$ -groups having some logical links with  $S$ -ramification (with more general sets  $S$  regarding  $P$ ) as, for instance, that of “mild groups” introduced by Labute [Lab06] dealing with the numbers of generators  $d(G)$  and of relations  $r(G)$  and defined as follows:

*A class of finitely presented pro- $p$ -groups  $G$  of cohomological dimension 2 such that  $r(G) \geq d(G)$  and  $d(G) \geq 2$  arbitrary.*

Many articles were then published giving an overview of the wide variety of such groups as the following short excerpt of a result of Schmidt about global fields [Sch10, Theorem 1.1]:

*Let  $S, T, \mathcal{M}$  be pairwise disjoint sets of places of  $K$ , where  $S$  and  $T$  are finite and  $\mathcal{M}$  has Dirichlet density 0. Then there exists a finite set of places  $S_0$  of  $K$  which is disjoint from  $S \cup T \cup \mathcal{M}$  and such that the group  $\mathcal{G}_{K, S \cup S_0}^T$  has cohomological dimension 2.*

But let’s go back to the basic abelian invariants, asking two open questions:

(i) We know the fixed point formula in a  $p$ -extension  $L/K$  (under Leopoldt’s conjecture), but, even in a  $p$ -cyclic extension with Galois group  $G$ , and contrary to the case of  $p$ -class groups (as done in [Gra17b] after a very long history), we do not know how to compute the filtration  $(M_i)_{i \geq 0}$ , of  $M := \mathcal{T}_{K,P}$ , defined inductively by:

$$M_0 = 1 \text{ and } M_{i+1}/M_i := (M/M_i)^G, \text{ for all } i \geq 0.$$

(ii) The explicit computation of the  $p$ -rank,  $\tilde{r}_{K,S}$  (1.4), of  $\mathcal{A}_{K,S}/\mathcal{T}_{K,S}$  for  $S \subseteq P$ , is available only in favorable Galois cases with an algebraic reasoning on the canonical representation  $\mathbb{Q}_p \log_S(E_K)$  given by the Herbrand theorem on units under Leopoldt’s conjecture (see § 2.4).

In the definition of  $\mathcal{W}_{K,S} := W_{K,S}/\text{tor}_{\mathbb{Z}_p}(\overline{E}_K^S)$ , we do not know how to compute  $\text{tor}_{\mathbb{Z}_p}(\overline{E}_K^S) \supseteq \iota_S(\mu_K)$  when  $S \subsetneq P$ . We ignore, in a  $p$ -adic framework, if Leopoldt’s conjecture is sufficient to obtain the responses apart from a Galois context.

A reasonable conjecture is that  $\text{tor}_{\mathbb{Z}_p}(\overline{E}_K^S) = \iota_S(\mu_K)$  whatever  $K$ ,  $p$  and  $S$ ; but this must be deepened.

We hope that our programs 3.1.1 may help to give heuristics about this.

#### ACKNOWLEDGMENTS

I would like to thank Christian Maire and Jean-François Jaulent for fruitful discussions and information concerning some aspects of pro- $p$ -groups and  $S$ -ramification.

#### REFERENCES

- [AF72] Amice, Y., Fresnel, J., *Fonctions zêta  $p$ -adiques des corps de nombres abéliens réels*, Acta Arithmetica **20** (1972), no. 4, 353–384.  
<http://matwbn.icm.edu.pl/ksiazki/aa/aa20/aa2043.pdf>
- [AM19] Assim, J., Movahhedi, A., *Galois codescent for motivic tame kernels* (2019).  
<https://arxiv.org/pdf/1901.07219>
- [AS13] Angelakis, A., Stevenhagen, P., *Absolute abelian Galois groups of imaginary quadratic fields*, In: proceedings volume of ANTS-X, UC San Diego 2012, E. Howe and K. Kedlaya (eds), OBS 1 (2013).  
<http://msp.org/obs/2013/1-1/obs-v1-n1-p02-p.pdf>
- [BG92] Berger, R.I., Gras, G., *Regular fields: normic criteria in  $p$ -extensions*, Publ. Math. Fac. Sci. Besançon (Théorie des Nombres), Années 1991/92.  
[http://pmb.univ-fcomte.fr/1992/Berger\\_Gras.pdf](http://pmb.univ-fcomte.fr/1992/Berger_Gras.pdf)
- [BGKK18] Boeckle, G., Guiraud, D.-A., Kalyanswamy, S., Khare, C., *Wieferich Primes and a mod  $p$  Leopoldt Conjecture* (2018). <https://arxiv.org/abs/1805.00131>
- [BJ13] Bourbon, C., Jaulent, J-F., *Propagation de la 2-birationalité*, Acta Arithmetica **160** (2013), 285–301. <https://doi.org/10.4064/aa160-3-5>
- [BJ16] Belabas, K., Jaulent, J-F., *The logarithmic class group package in PARI/GP*, Pub. Math. Besançon (2016), 5–18.  
[http://pmb.univ-fcomte.fr/2016/pmb\\_2016.pdf](http://pmb.univ-fcomte.fr/2016/pmb_2016.pdf)
- [Bos09] Bosca, S., *Principalization of ideals in abelian extensions of number fields*, International Journal of Number Theory **5** (2009), no. 03, 527–539.  
<https://doi.org/10.1142/S1793042109002213>
- [Bou18] Bouazzaoui, Z., *Fibonacci sequences and real quadratic  $p$ -rational fields* (2019).  
<https://arxiv.org/abs/1902.04795>
- [BP72] Bertrandias, F., Payan, J-J.,  *$\Gamma$ -extensions et invariants cyclotomiques*, Ann. Sci. Ec. Norm. Sup. 4e série, **5** (1972), no. 4, 517–548.  
<https://doi.org/10.24033/asens.1236>
- [Bru66] Brumer, A., *Galois groups of extensions of algebraic number fields with given ramification*, Michigan Math. J. **13** (1966), 33–40.  
<https://projecteuclid.org/euclid.mmj/1028999477>
- [BR17] Barbulescu, R., Ray, J., *Some remarks and experimentations on Greenberg’s  $p$ -rationality conjecture* (2017). <https://arxiv.org/pdf/1706.04847>
- [Cha82] Charifi, A., *Groupes de torsion attachés aux extensions Abéliennes  $p$ -ramifiées maximales (cas des corps totalement réels et des corps quadratiques imaginaires)*, Thèse de 3<sup>e</sup> cycle, Mathématiques, Université de Franche-Comté (1982), 50 pp.
- [Che33] Chevalley, C., *Sur la théorie du corps de classes dans les corps finis et les corps locaux* (Thèse no. 155), Jour. of the Faculty of Sciences Tokyo **2** (1933), 365–476.  
[http://archive.numdam.org/item/THESE\\_1934\\_\\_155\\_\\_365\\_0/](http://archive.numdam.org/item/THESE_1934__155__365_0/)
- [Coa77] Coates, J.,  *$p$ -adic  $L$ -functions and Iwasawa’s theory*, In: Proc. of Durham Symposium 1975, New York-London (1977), 269–353.

- [CL18] Coates, J., Li, Y., *Non-vanishing theorems for central  $L$ -values of some elliptic curves with complex multiplication* (2018). <https://arxiv.org/abs/1811.07595>
- [CL19] Coates, J., Li, Y., *Non-vanishing theorems for central  $L$ -values of some elliptic curves with complex multiplication II* (2019). <https://arxiv.org/abs/1904.05756>
- [Col88] Colmez, P., *Résidu en  $s = 1$  des fonctions zêta  $p$ -adiques*, Invent. Math. **91** (1988), 371–389. <https://eudml.org/doc/143545>
- [DP18] Davis, R., Pries, R., *Cohomology groups of Fermat curves via ray class fields of cyclotomic fields* (2018). <https://arxiv.org/pdf/1806.08352>.
- [ELHZ18] El Habibi, A., Ziane, M.,  *$p$ -Rational Fields and the Structure of Some Modules* (2018). <https://arxiv.org/abs/1804.10165>
- [EV07] Ellenberg, J. S., Venkatesh, A., *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. **2007** (2007), no. 1. <https://doi.org/10.1093/imrn/rnm002>
- [FV02] Fesenko, I. B., Vostokov, S. V., *Local Fields and Their Extensions*, American Math Society, Translations of Math Monographs **121**, Second Edition 2002. <https://www.maths.nottingham.ac.uk/personal/ibf/book/vol.pdf>
- [GJ89] Gras, G., Jaulent, J-F., *Sur les corps de nombres réguliers*, Math. Z. **202** (1989), no. 3, 343–365. <https://eudml.org/doc/174095>
- [GM13] Graves, H., Murty, M.R., *The abc conjecture and non-Wieferich primes in arithmetic progressions*, Journal of Number Theory **133** (2013), no. 6, 1809–1813. <http://www.sciencedirect.com/science/article/pii/S0022314X12003368>
- [Gor01] Goren, E.Z., *Hasse invariants for Hilbert modular varieties*, Isr. J. Math. **122** (2001), 157–174. <https://link.springer.com/article/10.1007/BF02809897>
- [Gra77] Gras, G., *Étude d'invariants relatifs aux groupes des classes des corps abéliens*, Journées Arithmétiques de Caen (Univ. Caen, Caen, 1976), pp. 35–53. Astérisque No. 41–42, Soc. Math. France, Paris (1977). [http://www.numdam.org/book-part/AST\\_1977\\_\\_41-42\\_\\_35\\_0/](http://www.numdam.org/book-part/AST_1977__41-42__35_0/)
- [Gra82] Gras, G., *Groupe de Galois de la  $p$ -extension abélienne  $p$ -ramifiée maximale d'un corps de nombres*, J. reine angew. Math. **333** (1982), 86–132. <https://eudml.org/doc/152440> <https://www.researchgate.net/publication/243110955>
- [Gra83] Gras, G., *Logarithme  $p$ -adique et groupes de Galois*, J. reine angew. Math. **343** (1983), 64–80. <https://doi.org/10.1515/crll.1983.343.64>
- [Gra84] Gras, G., *Sur la  $p$ -ramification abélienne*, Conférence donnée à l'University Laval, Québec, Mathematical series of the department of mathematics **20** (1984), 1–26. <https://www.dropbox.com/s/fusia63znk0kcky/Lectures1982.pdf?dl=0>
- [Gra85] Gras, G., *Plongements kummériens dans les  $\mathbb{Z}_p$ -extensions*, Compositio Mathematica **55** (1985), no. 3, 383–396. [http://www.numdam.org/item/?id=CM\\_1985\\_\\_55\\_3\\_383\\_0](http://www.numdam.org/item/?id=CM_1985__55_3_383_0)
- [Gra86] Gras, G., *Remarks on  $K_2$  of number fields*, Jour. Number Theory **23** (1986), no. 3, 322–335. <http://www.sciencedirect.com/science/article/pii/0022314X86900776>
- [Gra97] Gras, G., *Principalisation didéaux par extensions absolument abéliennes*, J. Number Th. **62** (1997), no. 2, 403–421. <https://doi.org/10.1006/jnth.1997.2068>
- [Gra98] Gras, G., *Théorèmes de réflexion*, J. Théor. Nombres Bordeaux **10** (1998), no. 2, 399–499. [http://www.numdam.org/item/JTNB\\_1998\\_\\_10\\_2\\_399\\_0/](http://www.numdam.org/item/JTNB_1998__10_2_399_0/)
- [Gra03] G. Gras, *Class Field Theory: from theory to practice*, corr. 2nd ed., Springer Monographs in Mathematics, Springer, 2005, xiii+507 pages.
- [Gra14] Gras, G., *On the structure of the Galois group of the Abelian closure of a number field*, J. Théorie Nombres Bordeaux **26** (2014), no. 3, 635–654. [http://www.numdam.org/article/JTNB\\_2014\\_\\_26\\_3\\_635\\_0.pdf](http://www.numdam.org/article/JTNB_2014__26_3_635_0.pdf)
- [Gra16] Gras, G., *Les  $\theta$ -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> <https://arxiv.org/pdf/1701.02618>

- [Gra17a] Gras, G., *Approche  $p$ -adique de la conjecture de Greenberg pour les corps totalement réels*, Ann. Math. Blaise Pascal **24** (2017), no. 2, 235–291.  
[http://ambp.cedram.org/item?id=AMBP\\_2017\\_\\_24\\_2\\_235\\_0](http://ambp.cedram.org/item?id=AMBP_2017__24_2_235_0)
- [Gra17b] 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. <https://www.ias.ac.in/article/fulltext/pmsc/127/01/0001-0034>
- [Gra17c] Gras, G., *On  $p$ -rationality of number fields. Applications—PARI/GP programs*, Publ. Math. Fac. Sci. Besançon (Théorie des Nombres), Années 2017/2018.  
<https://arxiv.org/pdf/1709.06388>
- [Gra18a] Gras, G., *The  $p$ -adic Kummer-Leopoldt Constant: Normalized  $p$ -adic Regulator*, Int. J. Number Theory **14** (2018), no. 2, 329–337.  
<https://doi.org/10.1142/S1793042118500203>
- [Gra18b] Gras, G., *Normes d'idéaux dans la tour cyclotomique et conjecture de Greenberg*, Annales mathématiques du Québec, Online: 17 October 2018, 1–32.  
<https://doi.org/10.1007/s40316-018-0108-3>
- [Gra18c] Gras, G., *Annihilation of  $\text{tor}_{\mathbb{Z}_p}(\mathcal{G}_{K,S}^{\text{ab}})$  for real abelian extensions  $K/\mathbb{Q}$* , Communications in Advanced Mathematical Sciences **1** (2018), no. 1, 5–34.  
<http://dergipark.gov.tr/download/article-file/543993>
- [Gra19a] Gras, G., *Heuristics and conjectures in the direction of a  $p$ -adic Brauer–Siegel theorem*, Math. Comp. **88** (2019), no. 318, 1929–1965.  
<https://doi.org/10.1090/mcom/3395>
- [Gra19b] Gras, G., *Test of Vandiver's conjecture with Gauss sums—Heuristics* (2019).  
<https://arxiv.org/abs/1808.03443>
- [Gre76] Greenberg, R., *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), no. 1, 263–284. <http://www.jstor.org/stable/2373625?>
- [Gre16] Greenberg, R., *Galois representations with open image*, Annales de Mathématiques du Québec, special volume in honor of Glenn Stevens, **40** (2016), no. 1, 83–119. <https://link.springer.com/article/10.1007/s40316-015-0050-6>
- [Hab78] Haberland, K., *Galois cohomology of algebraic number fields*. With two appendices by Helmut Koch and Thomas Zink, V.E.B. Deutscher Verlag der Wissenschaften 1978.
- [Hat87] Hatada, K., *Mod 1 distribution of Fermat and Fibonacci quotients and values of zeta functions at  $2 - p$* , Comment. Math. Univ. St. Pauli **36** (1987), 41–51.
- [Hat88] Hatada, K., *Chi-square tests for mod 1 distribution of Fermat and Fibonacci quotients*, Sci. Rep. Fac. Educ., Gifu Univ., Nat. Sci. **12** (1988), 1–2.
- [HM01] Hajir, F., Maire, C., *Tamely ramified towers and discriminant bounds for number fields*, Compositio Math. **128** (2001), no. 1, 35–53.  
<https://doi.org/10.1023/A:1017537415688>
- [HM02a] Hajir, F., Maire, C., *Extensions of number fields with wild ramification of bounded depth*, International Mathematics Research Notices **13** (2002), 667–696.  
<http://people.math.umass.edu/~hajir/hajir-imrn.pdf>
- [HM02b] Hajir, F., Maire, C., *Tamely ramified towers and discriminant bounds for number fields II*, Journal of Symbolic Computation **33** (2002), no. 4, 415–423.  
<https://doi.org/10.1006/jsc.2001.0514>
- [HM18a] Hajir, F., Maire, C., *Analytic Lie extensions of number fields with cyclic fixed points and tame ramification* (2018). <https://arxiv.org/abs/1710.09214>
- [HM18b] Hajir, F., Maire, C., *Prime decomposition and the Iwasawa  $\mu$ -invariant*, Math. Proc. Camb. Phil. Soc. **166** (2019), 599–617. Published online: 26 April 2018.  
<https://doi.org/10.1017/S0305004118000191>
- [HMR19a] Hajir, F., Maire, C., Ramakrishna, R., *Cutting towers of number fields* (2019).  
<https://arxiv.org/abs/1901.04354>
- [HMR19b] Hajir, F., Maire, C., Ramakrishna, R., *Infinite class field towers of number fields of prime power discriminant* (2019). <https://arxiv.org/pdf/1904.07062>

- [HZ16] Hofmann, T., Zhang, Y., *Valuations of  $p$ -adic regulators of cyclic cubic fields*, Journal of Number Theory **169** (2016), 86–102.  
<https://doi.org/10.1016/j.jnt.2016.05.016>
- [Jau84] Jaulent, J-F.,  *$S$ -classes infinitésimales d'un corps de nombres algébriques*, Ann. Sci. Inst. Fourier **34** (1984), no. 2, 1–27. <https://doi.org/10.5802/aif.960>
- [Jau85] Jaulent, J-F., *Sur l'indépendance  $\ell$ -adique de nombres algébriques*, J. Number Theory **20** (1985), 149–158. [https://doi.org/10.1016/0022-314X\(85\)90035-6](https://doi.org/10.1016/0022-314X(85)90035-6)
- [Jau86] Jaulent, J-F., *L'arithmétique des  $\ell$ -extensions* (Thèse de doctorat d'Etat), Pub. Math. Besançon (1986), 1–349. [http://pmb.univ-fcomte.fr/1986/Jaulent\\_these.pdf](http://pmb.univ-fcomte.fr/1986/Jaulent_these.pdf)
- [Jau87] Jaulent, J-F., *Sur les conjectures de Leopoldt et de Gross*, Actes des Journées Arithmétiques de Besançon (1985), Astérisque **147/148** (1987), 107–120.  
[http://www.numdam.org/item/AST\\_1987\\_147-148\\_107\\_0/](http://www.numdam.org/item/AST_1987_147-148_107_0/)
- [Jau94] Jaulent, J-F., *Classes logarithmiques des corps de nombres*, J. Théor. Nombres Bordeaux **6** (1994), 301–325.  
[http://www.numdam.org/article/JTNB\\_1994\\_6\\_2\\_301\\_0.pdf](http://www.numdam.org/article/JTNB_1994_6_2_301_0.pdf)
- [Jau98] Jaulent, J-F., *Théorie  $\ell$ -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](http://www.numdam.org/article/JTNB_1998_10_2_355_0.pdf)
- [Jau02] Jaulent, J-F., *Classes logarithmiques des corps totalement réels*, Acta Arithmetica **103** (2002), 1–7.  
<https://www.math.u-bordeaux.fr/~jjaulent/Articles/CLogTR.pdf>
- [Jau18a] Jaulent, J-F., *Note sur la conjecture de Greenberg*, J. Ramanujan Math. Soc. **34** (2019), 59–80. <https://arxiv.org/pdf/1612.00718>
- [Jau18b] Jaulent, J-F., *Principalisation abélienne des groupes de classes de rayons* (2018).  
<https://arxiv.org/abs/1801.07173>
- [Jau19a] Jaulent, J-F., *Principalization of logarithmic class groups* (2019).  
<https://arxiv.org/abs/1801.07176>
- [Jau19b] Jaulent, J-F., *Normes universelles et conjecture de Greenberg* (2019).  
<https://arxiv.org/abs/1904.07014>
- [JN93] Jaulent, J-F., Nguyen Quang Do, T., *Corps  $p$ -rationnels, corps  $p$ -réguliers et ramification restreinte*, J. Théor. Nombres Bordeaux **5** (1993), 343–363.  
[http://www.numdam.org/article/JTNB\\_1993\\_5\\_2\\_343\\_0.pdf](http://www.numdam.org/article/JTNB_1993_5_2_343_0.pdf)
- [JS97] Jaulent, J-F., Sauzet, O., *Pro- $\ell$ -extensions de corps de nombres  $\ell$ -rationnels*, J. Number Th. **65** (1997), 240–267; *ibid.* **80** (2000), 318–319.  
<https://doi.org/10.1006/jnth.1997.2158>
- [JS00] Jaulent, J-F., Sauzet, O., *Extensions quadratiques 2-birationnelles de corps de nombres totalement réels*, Pub. Mathématiques **44** (2000), 343–351.  
<https://www.math.u-bordeaux.fr/~jjaulent/Articles/Ext2bi.pdf>
- [Koch70] Koch, H., *Galois theory of  $p$ -extensions* (English translation of “Galoissche Theorie der  $p$ -Erweiterungen”, 1970), Springer Monographs in Math., Springer 2002.
- [KS95] Kraft, J.S., Schoof, R., *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. **97** (1995), 135–155.  
[http://www.numdam.org/item/CM\\_1995\\_97\\_1-2\\_135\\_0/](http://www.numdam.org/item/CM_1995_97_1-2_135_0/)
- [Kub57] Kubota, T., *Galois group of the maximal abelian extension of an algebraic number field*, Nagoya Math. J. **12** (1957), 177–189.
- [Lab06] Labute, J., *Mild pro- $p$ -groups and Galois groups of  $p$ -extensions of  $\mathbb{Q}$* , J. Reine Angew. Math. **596** (2006), 155–182. <https://doi.org/10.1515/CRELLE.2006.058>
- [Lec18] Lecouturier, E., *On the Galois structure of the class group of certain Kummer extensions*, J. London Math. Soc. (2) **98** (2018), 35–58.  
<https://doi:10.1112/jlms.12123>
- [Mai02] Maire, C., *On the  $\mathbb{Z}_\ell$ -rank of abelian extensions with restricted ramification*, Journal of Number Theory **92** (2002), 376–404.  
<https://doi:10.1006/jnth.2001.2712>

- [Mai03] Maire, C., *On the  $\mathbb{Z}_\ell$ -rank of abelian extensions with restricted ramification (addendum)*, Journal of Number Theory **98** (2003), 217–220.  
[https://doi.org/10.1016/S0022-314X\(02\)00028-8](https://doi.org/10.1016/S0022-314X(02)00028-8)
- [Mai05] Maire, C., *Sur la dimension cohomologique des pro- $p$ -extensions des corps de nombres*, J. Théor. Nombres Bordeaux **17** (2005), no. 2, 575–606.  
[http://www.numdam.org/item/JTNB\\_2005\\_\\_17\\_2\\_575\\_0/](http://www.numdam.org/item/JTNB_2005__17_2_575_0/)
- [Mai10] Maire, C., *Cohomology of number fields and analytic pro- $p$ -groups*, Mosc. Math. J. **10** (2010), no. 2, 399–414, 479.  
<http://www.ams.org/distribution/mmj/vol10-2-2010/maire.pdf>
- [Mai18] Maire, C., *On the quotients of the maximal unramified 2-extension of a number field*, Documenta Mathematica **23** (2018), 1263–1290.
- [Miki78] Miki, H., *On the maximal abelian  $\ell$ -extension of a finite algebraic number field with given ramification*, Nagoya Math. J. **70** (1978), 183–202.  
<https://doi.org/10.1017/S0027763000021875>
- [MN90] Movahhedi, A., Nguyen Quang Do, T., *Sur l'arithmétique des corps de nombres  $p$ -rationnels*, Séminaire de Théorie des Nombres, Paris 1987–88, Progress in Math. **81** (1990), 155–200. [https://doi.org/10.1007/978-1-4612-3460-9\\_9](https://doi.org/10.1007/978-1-4612-3460-9_9)
- [Mov88] Movahhedi, A., *Sur les  $p$ -extensions des corps  $p$ -rationnels*, Thèse, Univ. Paris VII (1988). [http://www.unilim.fr/pages\\_perso/chazad.movahhedi/These\\_1988.pdf](http://www.unilim.fr/pages_perso/chazad.movahhedi/These_1988.pdf)
- [Mov90] Movahhedi, A., *Sur les  $p$ -extensions des corps  $p$ -rationnels*, Math. Nachr. **149** (1990), 163–176. <http://onlinelibrary.wiley.com/doi/10.1002/mana.19901490113/>
- [MR19a] Maire, C., Rougnant, M., *Composantes isotypiques de pro- $p$ -extensions de corps de nombres et  $p$ -rationalité*, Publ. Math. Debrecen **94** (2019), no. 1/2, 123–155.  
[https://lmb.univ-fcomte.fr/IMG/pdf/maire-rougnant-08\\_22\\_2018.pdf](https://lmb.univ-fcomte.fr/IMG/pdf/maire-rougnant-08_22_2018.pdf)
- [MR19b] Maire, C., Rougnant, M., *A note on  $p$ -rational fields and the abc-conjecture* (2019). <https://arxiv.org/abs/1903.11271>
- [Nel13] Nelson, D., *A variation on Leopoldt's conjecture: some local units instead of all local units* (2013). <https://arxiv.org/abs/1308.4637>
- [Neu75] Neumann, O., *On  $p$ -closed number fields and an analogue of Riemann's existence theorem*. Algebraic number fields:  $L$ -functions and Galois properties, Proc. Sympos., Univ. Durham (1975), pp. 625–647. Academic Press, London, 1977.
- [Neu76] Neumann, O., *On  $p$ -closed algebraic number fields with restricted ramification*, Izv. Akad. Nauk USSR, ser. Math. **39**, 2 (1975), 259–271; English translation: Math. USSR, Izv. **9** (1976), 243–254.
- [Nqd82] Nguyen Quang Do, T., *Sur la structure galoisienne des corps locaux et la théorie d'Iwasawa*, Compositio Mathematica **46** (1982), no. 1, 85–119.  
[http://www.numdam.org/item/?id=CM\\_1982\\_\\_46\\_1\\_85\\_0](http://www.numdam.org/item/?id=CM_1982__46_1_85_0)
- [Nqd86] Nguyen Quang Do, T., *Sur la  $\mathbb{Z}_p$ -torsion de certains modules galoisiens*, Ann. Inst. Fourier **36** (1986), no. 2, 27–46. <https://doi.org/10.5802/aif.1045>
- [Nqd91] Nguyen Quang Do, T., *Lois de réciprocité primitives*, manuscripta math. **72** (1991), no. 1, 307–324. <https://doi.org/10.1007/BF02568282>
- [NSW00] Neukirch, J., Schmidt, A., Wingberg, K., *Cohomology of Number Fields* (2000), 2nd edition, Grundlehren der Math. Wissenschaften 323, Springer-Verlag (2008).
- [Ona76] Onabe, M., *On the isomorphisms of the Galois groups of the maximal abelian extensions of imaginary quadratic fields*, Natur. Sci. Rep. Ochanomizu Univ. **27** (1976), no. 2, 155–161. <https://www.researchgate.net/publication/37823146>
- [Ori86] Oriat, B., *Lien algébrique entre les deux facteurs de la formule analytique du nombre de classes dans les corps abéliens*, Acta Arithmetica **46** (1986), 331–354.  
<https://doi.org/10.4064/aa-46-4-331-354>
- [OT95] Ozaki, M., Taya, H., *A note on Greenberg's conjecture for real abelian number fields*, Manuscripta Math. **88** (1995), no. 1, 311–320.  
<http://link.springer.com/article/10.1007/BF02567825>
- [Pari16] The PARI Group –PARI/GP, version 2.9.0, Université de Bordeaux (2016).

- <http://pari.math.u-bordeaux.fr/>
- [Pit10] Pitoun, F., *Calculs théoriques et explicites en théorie d'Iwasawa*, Thèse de doctorat en Mathématiques, Laboratoire de Mathématiques, Université de Franche-comté Besançon (2010). <https://www.theses.fr/220448329>
- [PV15] Pitoun, F., Varescon, F., *Computing the torsion of the  $p$ -ramified module of a number field*, *Math. Comp.* **84** (2015), no. 291, 371–383.  
<https://doi.org/10.1090/S0025-5718-2014-02838-X>
- [Rib08] Ribet, K. A., Bernoulli numbers and ideal classes, *Gaz. Math.* **118** (2008), 42–49.  
[http://smf4.emath.fr/Publications/Gazette/2008/118/smf\\_gazette\\_118\\_42-49.pdf](http://smf4.emath.fr/Publications/Gazette/2008/118/smf_gazette_118_42-49.pdf)
- [Sch10] Schmidt, A., *Über pro- $p$ -fundamentalgruppen markierter arithmetischer kurven*, *J. Reine Angew. Math.* **640** (2010), 203–235.  
<https://www.mathi.uni-heidelberg.de/~schmidt/papers/marked.pdf>
- [Ser64] Serre, J-P., *Cohomologie galoisienne*, Lect. Notes in Math. 5, Springer-Verlag 1964, cinquième édition 1991; English translation: *Galois cohomology*, Springer 1997; corrected second printing: Springer Monographs in Math. 2002.
- [Ser78] Serre, J-P., *Sur le résidu de la fonction zêta  $p$ -adique d'un corps de nombres*, *C.R. Acad. Sci. Paris* **287** (1978), Série I, 183–188.
- [Sha64] Šafarevič, I.R., *Extensions with given points of ramification*, *Publ. Math. Inst. Hautes Etudes Sci.* 18 (1964), 71–95; *American Math. Soc. Transl., Ser. 2*, **59** (1966), 128–149. [http://www.numdam.org/article/PMIHES\\_1963\\_\\_18\\_93\\_0.pdf](http://www.numdam.org/article/PMIHES_1963__18_93_0.pdf)
- [Shu18] Shu, J., *Root numbers and Selmer groups for the Jacobian varieties of Fermat curves* (2018). <https://arxiv.org/pdf/1809.09285>
- [Sil88] Silverman, J.H., *Wieferich's criterion and the abc-conjecture*, *Journal of Number Theory* **30** (1988), 226–237. [https://doi.org/10.1016/0022-314X\(88\)90019-4](https://doi.org/10.1016/0022-314X(88)90019-4)
- [Vog07] Vogel, D.,  *$p$ -extensions with restricted ramification – The mixed case* (2007).  
<https://www.mathi.uni-heidelberg.de/~vogel/mixed>
- [Win89] Wingberg, K., *On Galois groups of  $p$ -closed algebraic number fields with restricted ramification*, *J. Reine Angew. Math.* **400** (1989), 185–202.  
<https://eudml.org/doc/153168>
- [Win91] Wingberg, K., *On Galois groups of  $p$ -closed algebraic number fields with restricted ramification II*, *J. Reine Angew. Math.* **416** (1991), 187–194.  
<https://doi.org/10.1515/crll.1991.416.187>
- [Yam93] Yamagishi, M., *A note on free pro- $p$ -extensions of algebraic number fields*, *Journal de théorie des nombres de Bordeaux* **5** (1993), no. 1, 165–178.  
[http://www.numdam.org/item/JTNB\\_1993\\_5\\_1\\_165\\_0/](http://www.numdam.org/item/JTNB_1993_5_1_165_0/)

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