Practice of incomplete p-ramification over a number field – History of abelian p-ramification

Georges Gras

PRACTICE OF INCOMPLETE p-RAMIFICATION OVER A NUMBER FIELD

APPENDIX: HISTORY OF ABELIAN p-RAMIFICATION

GEORGES GRAS

ABSTRACT. The theory of p-ramification in the maximal pro-p-extension of a number field K, unramified outside p and ∞, is well known including numerical experiments with PARI/GP programs. The case of incomplete "pro-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 method 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 $\mathrm{Gal}(H_{K,S}/K)$ (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 our purpose.

CONTENTS

Date: April 23, 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.

1. Introduction and basic results

Let $p\geq 2$ be a prime number and let K be a number field; we denote by $P:=\{\mathfrak{p}\text{ prime},\ \mathfrak{p}\mid p\}$ 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 at the real infinite places 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 [Se1964], Šafarevič [Sha1964], Brumer [Br1966], and has been largely extended, from the 1980's, in much works considering S-ramification (eventually with decomposition of another set Σ of places). The analogous theory for a local base field has also a long history that we shall not consider in this article.

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

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

Denote by (r_1, r_2) the signature of K (so that $r_1 + 2\,r_2 = [K : \mathbb{Q}]$); then, the $\mathbb{F}_p$-dimension of $\mathrm{H}^2(\mathcal{G}_{K,P}, \mathbb{Z}/p\mathbb{Z})$, which gives the minimal number of relations between these generators, is the p-rank of the torsion group $\mathcal{T}_{K,P}$ of $\mathcal{A}_{K,P}$, so that we have the relation:

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

In the general case for S (possibly containing tame places) we have:

$$\mathcal{A}_{K,S} = \Gamma_{K,S} \bigoplus \mathcal{T}_{K,S}, \;\; \Gamma_{K,S} \simeq \mathbb{Z}_p^{\widetilde{r}_{K,S}}, \tag{1.1}$$

where $\mathcal{T}_{K,S} := \mathrm{tor}_{\mathbb{Z}_p}(\mathcal{A}_{K,S})$ and $\widetilde{r}_{K,S} \geq 0$. Without any p-adic assumption on the units, we still have $\mathrm{rk}_p(\mathrm{H}^1(\mathcal{G}_{K,S}, \mathbb{Z}/p\mathbb{Z})) = \mathrm{rk}_p(\mathcal{A}_{K,S})$, given by the Šafarevič formula, but $\widetilde{r}_{K,S}$ is more difficult; $\mathrm{rk}_p(\mathcal{A}_{K,S})$ is computable in complete generality with the invariants of class field theory for K as follows. 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 (with $S_p := S \cap P$):

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

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

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

where $\widetilde{r}_{K,S}$ defined by (1.1) is given by the following formula:

$$\widetilde{r}_{K,S} = \sum_{\mathfrak{p} \in S_p} [K_{\mathfrak{p}} : \mathbb{Q}_p] - \dim_{\mathbb{Q}_p}\big(\mathbb{Q}_p \log_{S_p}(E_K)\big), \tag{1.4}$$

where E_K is the group of global units of K and:

$$\log_{S_p} := \big(\log_{\mathfrak{p}}\big)_{\mathfrak{p} \in S_p}$$

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

the family of p-adic logarithms over S_p with values in $\bigoplus_{\mathfrak{p}\in S_p} K_\mathfrak{p}$. Note that for $S=P$, $r_{K,P} := \dim_{\mathbb{Q}_p}\big(\mathbb{Q}_p\log_P(E_K)\big)$ is also the p-adic rank of E_K.

The Šafarevič and reflection formulas, generalized with decomposition, may be obtained via [Gr2003/2005, Exercise II.5.4.1] or other references.

In general, $\widetilde{r}_{K,S}$ is non-obvious and varies from 0 to r_2+1 (see [Ya1993, M2002, M2003, M2005] 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).

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

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

if $S=\emptyset$ then $\mathcal{A}_{K,S}=\mathcal{T}_{K,S}=:\mathcal{C}\ell_K$, 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*), [Neu1975], [Ng1986, Corollary 4.3], [Gr2003/2005, Deployment Theorem III.4.1.5], where the $F_\mathfrak{l}$ are the residue fields:

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

For some more 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 the set P of places of K dividing p and when $K/\mathbb{Q}$ is not necessarily Galois.

Of course, this highly depends on the decomposition of the prime p in K, so the most tricky invariants are $\mathcal{T}_{K,S}$ and $\widetilde{r}_{K,S}=\mathrm{rk}_p(\mathcal{A}_{K,S})-\mathrm{rk}_p(\mathcal{T}_{K,S})=\dim_{\mathbb{Q}_p}\big(\mathbb{Q}_p\log_S(E_K)\big)$.

2. General 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 (= unramified) in the class fields under consideration).

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 $K_\mathfrak{p}$, and let $\overline{E}_K^S$ be the closure of the diagonal image of E_K in $U_{K,S}$ (i.e., the projection of the closure $\overline{E}_K^P$ on $U_{K,S}$). We denote by $W_{K,S}=\bigoplus_{\mathfrak{p}\in S}\mu_{K_\mathfrak{p}}$ the p-torsion group of $U_{K,S}$.

Note that if $S \subsetneq P$, $U_{K,S}$ is in general not a Galois module, even if $K/\mathbb{Q}$ is a Galois extension.

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

Lemma 2.1. *We have the exact sequence:*

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

Proof. To simplify, put $\log := \log_S$. The surjectivity comes from the fact that if $u \in U_{K,S}$ is such that $p^n \log(u) = \log(\overline{\varepsilon})$, $\overline{\varepsilon} \in \overline{E}_K^S$, then $u^{p^n} = \overline{\varepsilon} \cdot \xi$ 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 $\mathrm{tor}_{\mathbb{Z}_p}\big(U_{K,S}/\overline{E}_K^S\big)$. If $u \in U_{K,S}$ is such that $\log(u) \in \log(\overline{E}_K^S)$, then $u = \overline{\varepsilon} \cdot \xi$ as above, giving the kernel equal to $\overline{E}_K^S \cdot W_{K,S}/\overline{E}_K^S = W_{K,S}/\mathrm{tor}_{\mathbb{Z}_p}(\overline{E}_K^S)$. □

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

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

Lemma 2.2. *Assume $S = P$. Let μ_K be the group of global roots of unity of p-power order of K. Then, under the Leopoldt conjecture for p in K, we have $\mathrm{tor}_{\mathbb{Z}_p}(\overline{E}_K^P) = \mu_K$; thus in that case $W_{K,P}/\mathrm{tor}_{\mathbb{Z}_p}(\overline{E}_K^P) = W_{K,P}/\mu_K$.*

Proof. From [Ja1998, Définition 2.11, Proposition 2.12] or [Gr2003/2005, Theorem III.3.6.2 (vi)]. □

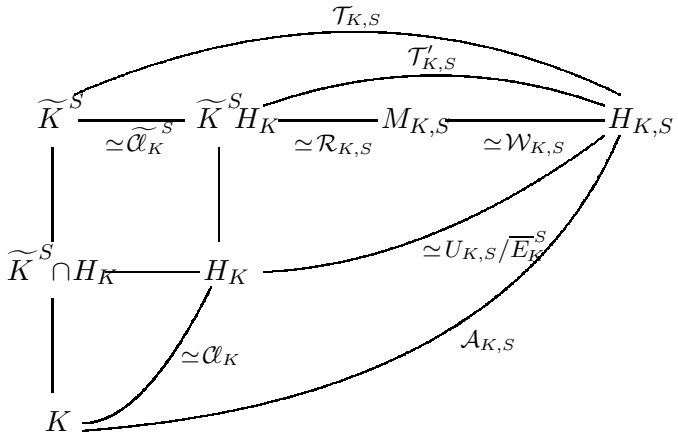
Note that for $S \subsetneq P$, we do not know if $\mathrm{tor}_{\mathbb{Z}_p}(\overline{E}_K^S) = \mu_K$ (as subgroups of $W_{K,S}$), even under the Leopoldt conjecture.

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

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

Remark 2.3. When $S = P$, we have $\mathrm{Gal}(H_{K,P}/H_K) \simeq U_{K,P}/\overline{E}_K^P$, in which the image of $\mathcal{W}_{K,P}$ fixes $M_{K,P} =: H_K^{\mathrm{bp}}$, the Bertrandias–Payan field, $\mathrm{Gal}(H_K^{\mathrm{bp}}/\widetilde{K}^P)$ being the Bertrandias–Payan module [BP1972] as named by Nguyen Quang Do.

The group $\mathcal{R}_{K,P}$ is then isomorphic to $\mathrm{Gal}(H_K^{\rm bp}/\widetilde{K}^P H_K)$.
The "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 [Gr2017, Proposition 5.2]).



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

2.3. **Local computations.** We note that [Gr2017/2018, Theorem 2.1 & Corollary 2.2] are still valid for a test of any incomplete p-ramification for an arbitrary support S:

Theorem 2.4. *For any $\mathfrak{p} \mid p$ in K and any $j \geq 1$, 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 any subset $S \subseteq P$, denote by $\mathfrak{m}_S$ the modulus $\prod_{\mathfrak{p}\in S}\mathfrak{p}$.
For a modulus of the form $\mathfrak{m}_S^n$, $n \geq 0$, let $\mathcal{C}\ell_K(\mathfrak{m}_S^n)$ be the corresponding ray class group. Then for $m \geq n \geq 0$, we have the inequalities:

$$0 \leq \mathrm{rk}_p(\mathcal{C}\ell_K(\mathfrak{m}_S^m)) - \mathrm{rk}_p(\mathcal{C}\ell_K(\mathfrak{m}_S^n)) \leq \sum_{\mathfrak{p}\in S} \mathrm{rk}_p\big((U_{\mathfrak{p}}^1)^p\, U_{\mathfrak{p}}^{n\cdot e_{\mathfrak{p}}}/(U_{\mathfrak{p}}^1)^p\, U_{\mathfrak{p}}^{m\cdot e_{\mathfrak{p}}}\big),$$

where $e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p} \in S$ in $K/\mathbb{Q}$.

Proof. See for instance [Gr2003/2005, Theorem I.4.5 & Corollary I.4.5.4] in the ordinary sense. □

Corollary 2.5. *We have $\mathrm{rk}_p(\mathcal{C}\ell_K(\mathfrak{m}_S^m)) = \mathrm{rk}_p(\mathcal{C}\ell_K(\mathfrak{m}_S^n)) = \mathrm{rk}_p(\mathcal{A}_{K,S})$ 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 $\mathrm{rk}_p(\mathcal{C}\ell_K(\mathfrak{m}_S^{n_0})) = \widetilde{r}_{K,S}$.

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:

$$\mathrm{rk}_p(\mathcal{C}\ell_K(\mathfrak{m}_S^n)) = \mathrm{rk}_p(\mathcal{C}\ell_K(\mathfrak{m}_S^m)) = \widetilde{r}_{K,S} + \mathrm{rk}_p(\mathcal{T}_{K,S}) \text{ as } m \to \infty,$$

giving $\mathrm{rk}_p(\mathcal{C}\ell_K(\mathfrak{m}_S^n)) = \widetilde{r}_{K,S} + \mathrm{rk}_p(\mathcal{T}_{K,S})$ 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 $n > \frac{p}{p-1}$ [FV2002, Chapter I, § 5.8, Corollary 2] giving the value of n_0; furthermore, $\mathscr{C}\!\ell_K(\mathfrak{m}_S^{n_0})$ gives the p-rank of $\mathcal{T}_{K,S}$ as soon as $\widetilde{r}_{K,S}$ is known. □

2.4. **Practical computation of $\widetilde{r}_{K,S}$.** Let $S \subseteq P$. From (1.4), we have $\widetilde{r}_{K,S} = \sum_{\mathfrak{p}\in S}[K_{\mathfrak{p}} : \mathbb{Q}_p] - r_{K,S}$, where $r_{K,S} := \dim_{\mathbb{Q}_p}\big(\mathbb{Q}_p\log_S(E_K)\big)$ in $\bigoplus_{\mathfrak{p}\in S} K_{\mathfrak{p}}$.
In [M2002, M2003] 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 [Ja1985].

In the Galois case $K/\mathbb{Q}$, this rank has been studied by Nelson [Nel2013] giving formulas (or lower bounds) under the p-adic Schanuel conjecture.

We have proposed, in [Gr2003/2005, III, § 4 (f)], a conjecture in the general non-Galois case.

But all these approaches, in terms of representations and Galois descent, are very difficult for programming and not so obvious for random K, so we shall preferably give extensive computations via PARI/GP [P2016] since ray class fields are well computed. But it remains the problem of "computing" $\widetilde{r}_{K,S}$ when no theoretical value is known.

We conclude by the following:

Remark 2.6. If $\mathcal{T}_{K,P} = 1$ (i.e., the field K is called p-rational as proposed by Movahhedi in [Mo1988]), 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 $\mathcal{T}_{K,P} \neq 1$ (non-p-rationality), but often $\mathcal{T}_{K,S} = 1$ for $S \subsetneq P$.

This intricate aspects have been studied by Maire [M2005, Section 3] in which he introduces the notion of "S-cohomologcal condition" (i.e., when $\mathrm{H}^2(\mathcal{G}_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$, knowing that $\mathcal{G}_{K,S}$ is a free pro$p$-group if and only if $\mathrm{H}^2(\mathcal{G}_{K,S}, \mathbb{Q}_p/\mathbb{Z}_p)$ and $\mathcal{T}_{K,S}$ are trivial) and that of "S-arithmetical condition" (when the map $E_K \otimes \mathbb{Z}_p \to U_{K,S}$ is injective), and compare them which, of course, coincide for $S = P$; we know that the S-arithmetical condition implies the S-cohomologcal 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 (giving a free-S-ramified pro-p-extension $H_{K,S}/K$). Note also that $H_{K,S}$ is the subfield of $H_{K,P}$ fixed by the decomposition groups of the places $\mathfrak{p} \in P \setminus S$ (see numerical approach in [Gr2003/2005, § III.5]).

This is also justified by the fact that many variants of the definitions may be given, as those of Jaulent–Sauzet [JS1997, JS2000] and Bourbon–Jaulent [BJ2013], where are defined and studied the case of singleton $S = \{\mathfrak{p}\}$ or the property of "2-birationality" of quadratic extensions of totally real fields when $S = \{\mathfrak{p}, \mathfrak{p}'\}$.

3. General program for S-ramification

The principle is to consider a modulus $\mathfrak{m}_S := \prod_{\mathfrak{p}\in S} \mathfrak{p}^{\lambda_\mathfrak{p}}$, of support $S \subseteq P$, for which $\lambda_\mathfrak{p} \gg 0$ for all $\mathfrak{p} \in S$ to "read" the structure of $\mathcal{A}_{K,S}$. The practice shows that the more convenient modulus is of the form:

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

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 decomposition of p in K, given by PARI/GP, and compute with ideals.

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

3.1.1. *Instructions for use.* The reader has only to copy and past the verbatim of the programs 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

Give some instructions for its use (warning: in some journals, the exponent symbol ^ is not the PARI/GP one and must be replaced):

(i) It is assumed that the irreducible monic polynomial P defining K is given and that the interval [bp, Bp] of tested primes p is also given by the user.

(ii) The program computes the decomposition of p into d prime ideals; for instance, the following data gives, for $\mathsf{P} = \mathsf{x}^3 + 197 * \mathsf{x}^2 + 718 * \mathsf{x} + 508$ and $p = 2$, the decomposition $(p) = \mathfrak{p}\mathfrak{p}'$ 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 $[2, [0,0,1]^\sim, 1, 2, [0,1,0]^\sim]$, the 3th component is its ramification index, the 4th component is its residue degree. For the computation of the modulus $\mathfrak{m}_S$ (to be considered at the power n), we replace each prime ideal $\mathfrak{p} \in S$ by $\mathfrak{p}^{e_\mathfrak{p}}$ using the function idealpow.

(iii) Then for each modulus of support S (for all $S \subseteq P$), the program gives the p-rank of $\mathcal{A}_{K,S}$ and the $\mathbb{Z}$-structure of $\mathcal{A}_{K,S}/\mathcal{A}_{K,S}^{p^N}$ under the form:

$$[a_1, \cdots, a_r;\ b_1, \cdots, b_t],$$

where the coefficients $a_1, \cdots, a_r$ increase as the exponent n increses, so in the non-ambiguous cases, $b_1, \cdots, b_t$ give the group-invariants of $\mathcal{T}_{K,S}$ and r is the p-rank $\widetilde{r}_{K,S}$ of $\mathrm{Gal}(\widetilde{K}^S/K)$. Of course, if the rank $\widetilde{r}_{K,S}$ 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".

(iv) The data $\mathsf{S} = [\delta_1, ..., \delta_\mathsf{d}]$, $\delta_i \in \{0, 1\}$, indicates, by abuse of notation, that the S-modulus considered is:

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

We have choosen $n = n_0 + \frac{30}{p}$ 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 $\mathsf{S} = [0, ..., 0]$ one obtains the p-class group $\mathcal{C}\ell_K$.

3.1.2. *The PARI/GP program.* We illustrate the program with an example where K (a cubic field) is not S-rational for some small p and some $S \subseteq P$; but in almost all cases, K is S-rational ($\mathsf{Galoisgroup} = [6, -1, 1, \text{"S3"}]$ in the PARI/GP notation [2] and $\mathsf{Discriminant} = [769, 1; 1390573, 1]$):

```
================================================================================
{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))}
================================================================================
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]
```

[2] 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=[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]
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=[49466509645380638539234 91, 3371]
```

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

```
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=[17763568394002504646778106689453125, 390625]
```

Whence a non-trivial $\mathcal{T}_{K,S} \simeq \mathbb{Z}/5^8\mathbb{Z}$ for $S_1 = \{\mathfrak{p}\}$ (for the prime of residue degree 2) and $S_2 = P$. Note that once the substantial computation of $\mathsf{K} = \mathsf{bnfinit}(\mathsf{P}, 1)$ (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 $n \to \infty$ to see that the data 390625 remains constant.

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));
```

3.1.3. *Example with p totally split in degree* 5. For $P = x^5 - 5$, $n = 5$, and $p = 31$ (totally split) one finds one case of non S–rationality:
$\mathsf{S} = [1, 0, 0, 0, 1]$ $\mathsf{rk}(\mathsf{A_S}) = 1$ $\mathsf{A_S} = [961]$, i.e., $\widetilde{r}_{K,S} = 0$, $\mathcal{T}_{K,S} \simeq \mathbb{Z}/31^2\mathbb{Z}$:

```
p=31
[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 examples:

```
p=43
[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., $\widetilde{r}_{K,S} = 0$ 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 [JS1997], 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 $\mathcal{T}_{K,P} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Many other numerical examples are available in [JS1997, § 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^(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);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=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 [Le2018, § 5] for their p-class groups and these fields have some remarkable properties. For instance if log is the discrete logarithm for $\mathbb{Z}/p\mathbb{Z}$ 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 $\mathcal{C}\ell_K$ (from a result of Calegari–Emerton proved again in [Le2018, Theorem 1.1], after other similar results of Iimura).

So we shall give the general caculations, 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 (recal 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("N mod p=",lift(Mod(N,p))," 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^(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))}

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 - 19
```

```
[3, [-2, -1, 0]~, 1, 1, [2, 2, 1]~]
[3, [0, 1, 0]~, 2, 1, [2, 0, 1]~]
T=Mod(0,3) S=[0,0] rk(A_S)=1 A_S=[3]
T=Mod(0,3) S=[0,1] rk(A_S)=2 A_S=[129140163, 9]
T=Mod(0,3) S=[1,0] rk(A_S)=1 A_S=[3]
T=Mod(0,3) S=[1,1] rk(A_S)=3 A_S=[129140163,129140163, 9]

P=x^3 - 103
[3, [-1, 1, 0]~, 3, 1, [1, 1, 1]~]
T=Mod(1,3) S=[0] rk(A_S)=1 A_S=[3]
T=Mod(1,3) S=[1] rk(A_S)=3 A_S=[387420489,129140163, 3]

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 - 487
[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)=2 A_S=[129140163, 27]
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)=3 A_S=[129140163,129140163, 27]

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 - 31
[5, [-1, 1, 0, 0, 0]~, 5, 1, [1, 1, 1, 1, 1]~]
T=Mod(2,5) S=[0] rk(A_S)=2 A_S=[5, 5]
T=Mod(2,5) S=[1] rk(A_S)=4 A_S=[6103515625,6103515625,6103515625, 5]

P=x^5 - 101
[5, [0, 0, 0, 0, 1]~, 1, 1, [4, 3, 2, 0, 1]~]
[5, [1, 0, 0, 0, -1]~, 4, 1, [4, 3, 2, 1, 1]~]
T=Mod(0,5) S=[0,0] rk(A_S)=1 A_S=[5]
T=Mod(0,5) S=[0,1] rk(A_S)=3 A_S=[30517578125,1220703125, 25]
T=Mod(0,5) S=[1,0] rk(A_S)=1 A_S=[25]
```

```
T=Mod(0,5) S=[1,1] rk(A_S)=4 A_S=[30517578125,1220703125,1220703125, 25]

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 - 43
[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)=1 A_S=[7]
T=Mod(2,7) S=[1] rk(A_S)=5 A_S=[96889010407,13841287201,13841287201,
1977326743, 7]

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 - 23
[11, [-1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0]~, 11, 1,
                                    [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]~]
T=Mod(10,11) S=[0] rk(A_S)=1 A_S=[11]
T=Mod(10,11) S=[1] rk(A_S)=6 A_S=[285311670611,25937424601,25937424601,
25937424601,25937424601,25937424601]

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, 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,
25937424601,25937424601,25937424601, 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, 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,
137858491849,137858491849,137858491849,137858491849]

P=x^13 - 157
[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, 1]~]
T=Mod(7,13) S=[0] rk(A_S)=1 A_S=[13]
T=Mod(7,13) S=[1] rk(A_S)=8 A_S=[1792160394037,137858491849,137858491849,
137858491849,137858491849,137858491849,10604499373, 13]

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,
137858491849,137858491849,10604499373,10604499373, 169]
```

3.3. **The fields $K = \mathbb{Q}\big(\sqrt{-\sqrt{-q}}\big)$ associated to elliptic curves.** These fields, used in [CoL2019] 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 for our purpose.

Note once for all that the signature of K is $[0, 2]$, the Galois closure of K is of degree 8 with Galois group $[8, -1, 1, \text{"D(4)"}]$ and $D_K = 2^m\, q^3$.

3.3.1. *Programs for various p.* In this part, we fix the prime number q and compute the structure of $\mathcal{A}_{K,S}$ for all sets $S \subseteq P$. Recal that the role of the parameter $\mathsf{n} = \mathsf{n0} + \mathsf{floor}(30/\mathsf{p})$ is 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;if(polisirreducible(P)==0,break);
print("P=",P);bp=2;Bp=500;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);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 p-rank of $\mathcal{A}_{K,S}$ is 0 or 1.

3.3.2. *Programs for various q and $p = 2$.* The analogous program is the following:

```
{bq=3;Bq=1000;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^(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)))}
```

We give an example of each congruence class of q modulo 16:

```
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 $q \equiv 3 \pmod 8$ ($\#P = 1$), then $\mathcal{T}_{K,S} = 1$ for all S;

(ii) For $q \equiv 5 \pmod 8$ ($\#P = 1$), then $\mathcal{T}_{K,\emptyset} = \mathcal{C}\ell_K \simeq \mathbb{Z}/4\mathbb{Z}$ and $\mathcal{T}_{K,P} = 1$ (which means that the 2-Hilbert class field of K is contained in the compositum of of the $\mathbb{Z}_2$-extensions of K);

(iii) For $q \equiv 7 \pmod{16}$ ($\#P = 2$), then 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 from classical calculations and are left to the reader as exercises on the Log_S-function (consider first the arithmetic of the subfield $k = \mathbb{Q}(\sqrt{-q})$ and use fixed point formulas in K/k).

(iv) For $q \equiv 15 \pmod{16}$, the situation is more complex 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 theoretical and practical information about the torsion groups $\mathcal{T}_{K,S}$ that we have numerically computed in the first part of this paper.

We shall not consider the immense domain of pro-p-groups like $\mathcal{G}_{K,S}$, 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, nor the analytic ones as the non-vanishing at $s = 1$ of complex L-series associated to elliptic curves... Similarly, we shall not consider the Iwasawa's theory framework because this 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 explained in [Ng1982, § 9].

So we will focus mainly on class field theory and specific deep p-adic properties or conjectures generalizing Leopoldt's conjecture 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, $S \subseteq P$, whithout 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 use and will be an opportunity to clarify the vocabulary and the main contributions, especially until the end of the 20th century.

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 the interest for S-ramification theory is probably a paper of Brumer [Br1966], following Serre's book [Se1964] and seems also due to a lecture by Šafarevič (1963) showing the importance of the subject.

In his paper, Šafarevič gives the main 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 this has been amply developed in the book of Koch [Ko1970/2002] (see also in [HM2001, HM2002'] a good introduction on the subject and its developments [HM2002, M2010, M2017, HM2017/2019, HM2018]).

More precisely, in [Sha1964, Théorème I], Šafarevič gave, 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 $\dim_{\mathbb{F}_p}(\mathrm{H}^1(\mathcal{G}_{K,S},\mathbb{F}_p))$ of $\mathcal{G}_{K,S}$) is:

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

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 $K_\mathfrak{p}$ contains μ_p or not, and $\delta_K = 1$ or 0 according as K contains μ_p or not.

Of course, $\dim_{\mathbb{F}_p}(\mathrm{H}^2(\mathcal{G}_{K,S},\mathbb{F}_p))$ giving the minimal number of relations is a very deep invariant and is easily obtained only when $P \subseteq S$, which explain the forthcoming studies about this (e.g., [Hab1978, Ko1970/2002, Neu1976, Win1989, Win1991, Ya1993, Lab2006, Sch2010]).

A.2.2. *Kubota formalism.* Mention that Kubota [Kub1957] began 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 [Mi1978], Miki used 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 recalled in this survey (as well as the notion of p-rationality and its 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 still used in [BP1972] and by many authors; see, e.g., [Gr1982, Théorèmes I.2, I.3, Corollaire 1].

A.3.1. *Reflection formula. Rank formulas.* From the Šafarevič formula and Kummer theory when K contains the group μ_p of pth roots of unity, one obtains the reflection theorem in its simplest form, writing $P = S \cup \Sigma$ with $S \cap \Sigma = \emptyset$:

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

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 Σ-decomposed (i.e., in which all the places of Σ split completely), and similarly for the definition of $\mathcal{A}_{K,\Sigma}^{S\mathrm{res}}$ in the restricted sense for $p = 2$.

Theorem A.1. [Gr2003/2005, 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 $P^{\rm dec}$ be the set of p-places of K totaly split in K'. Then (where ω is the Teichmüller character):*

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

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

(i) If $\mu_p \subset K$ (i.e., $\omega = 1$), we then have:

$$\mathrm{rk}_p(\mathcal{T}_{K,P}) = \mathrm{rk}_p(\mathcal{C}\ell_K^{P\mathrm{res}}) + \#P - 1,$$

where $\mathcal{C}\ell_K^{P\mathrm{res}}$ is the quotient of the p-class group $\mathcal{C}\ell_K^{\rm res}$ by the subgroup generated by the classes of P.

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

- *If K does not contain μ_p, then the p-places of K are not totally split in $K(\mu_p)/K$ and the ω-component of the p-class group of $K(\mu_p)$ is trivial;*
- *if $\mu_p \subset K$, p does not split in $K/\mathbb{Q}$ and the unique $\mathfrak{p} \in P$ in K generates the p-class group of K (in the restricted sense for $p=2$).*

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

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

Thus, since $\mathcal{A}_{K,\emptyset}^P = \mathcal{O}_K/\mathcal{o}_K(\mathfrak{p})$, with $\mathfrak{p} = (1-\zeta_p)$, and $\mathcal{A}_{K,P} \simeq \mathbb{Z}_p^{\frac{p+1}{2}} \bigoplus \mathcal{T}_{K,P}$, this yields:

$$\mathrm{rk}_p(\mathcal{T}_{K,P}) = \mathrm{rk}_p(\mathcal{C}\ell_K), \tag{A.3}$$

which may be precised with the writing $\mathrm{rk}_p(\mathcal{T}_{K,P}^{\pm}) = \mathrm{rk}_p(\mathcal{C}\ell_K^{\mp})$ (see [Gr2019, § 3.1] *for analogous equality with p-adic characters associated by means of the mirror involution).*

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

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

where $\mathcal{A}_{K,\mathfrak{m}^*}^S$ is the Galois group of the p-ray class field of modulus $\mathfrak{m}^*$ and S-split. See [Gr2003/2005, Exercise II.5.4.1] for the case $p=2$ which needs to consider the infinite places, and for some generalizations and applications.

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

$$\mathrm{rk}_p(\mathcal{T}_{K,S}^{\Sigma}) = \mathrm{rk}_\omega(\mathcal{C}\ell_{K',\Sigma'}^{S'\mathrm{res}}) - \sum_{\mathfrak{p}\in\Sigma}\big([K_\mathfrak{p} : \mathbb{Q}_p] - 1\big) + \sum_{\mathfrak{p}\in S}\delta_\mathfrak{p} - \delta_K + \big(r_2 + 1 - \widetilde{r}_{K,S}^{\Sigma}\big),$$

where $\widetilde{r}_{K,S}^{\Sigma} \leq r_2+1$ is the $\mathbb{Z}_p$-rank of $\mathbb{Z}_p\mathrm{Log}_S^{\Sigma}(I_{K,S})$ modulo the $\mathbb{Q}_p$-space $\mathbb{Q}_p\log_S(E_K^{\Sigma})$ dealing here with the group of Σ-units of K (see also [M2005] 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 Spiegelunssatz (1958), Armitage–Fröhlich–Serre for $p=2$, Oriat for some improvements.

For reflection theorems and formulas with characters, see [Gr2003/2005, II.5.4, Theorem II.5.4.5)] from [Gr1998, Ch. I, Theorem 5.18] where p-rank formulas link p-class groups and $\mathcal{T}_K$ groups as in Theorem A.1 (a context used by Ellenberg–Venkatesh in [EV2007] for the ε-conjecture about p-class groups).

For the annihilation of $\mathcal{T}_K$ for the real abelian extensions, in relation with the construction of p-adic L-functions and reflection principle, see [Gr2018'] and its bibliography.

A.3.2. *Regulators and p-adic residues of the ζ_p-functions.* We continue the story with the p-adic analytic computations of the residue of the p-adic ζ-function at $s=1$ of real abelian fields K by Amice–Fresnel [AF1972], from Kubota–Leopoldt L_p-functions (1964), by Coates [Co1977], Serre [Se1978] introducing p-adic pseudo measures, then by Colmez [Col1988] in full generality, via the formula:

$$\tfrac{1}{2^{[K:\mathbb{Q}]-1}}\ \lim_{s\to 1}(s-1)\,\zeta_{K,p}(s) = \frac{R_p\,h\,E_p(1)}{\sqrt{D}},$$

where R_p is the p-adic regulator, h the class number, D the discriminant of K and $E_p(1)$ an eulerian factor.

The normalised p-adic regulator $\mathcal{R}_K$ (2.2), for totally real fields, is given (under Leopoldt's conjecture) by:

$$\#\mathcal{R}_K \sim \frac{1}{2}\cdot\frac{\big(\mathbb{Z}_p : \log(\mathrm{N}_{K/\mathbb{Q}}(U_K))\big)}{\#\mathcal{W}_K\cdot\prod_{\mathfrak{p}\mid p}\mathrm{N}\mathfrak{p}}\cdot\frac{R_p}{\sqrt{D}},$$

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

$$\tfrac{1}{2^{[K:\mathbb{Q}]-1}}\lim_{s\to 1}(s-1)\,\zeta_{K,p}(s) = \tfrac{1}{p\,[K\cap\mathbb{Q}^{\mathrm{c}}:\mathbb{Q}]}\,\#\mathcal{T}_K,$$

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

A.3.3. *Cohomological interpretation.* In [Ng1986], Nguyen Quang Do gave the cohomological interpretation:

$$\mathcal{T}_{K,P} \simeq \mathrm{H}^2(\mathcal{G}_{K,P},\mathbb{Z}_p)^*,$$

considered as the first of the non positive twists $\mathrm{H}^2(\mathcal{G}_{K,P},\mathbb{Z}_p(i))$ of the motivic cohomology.

It is indeed well known that this cohomological invariant does appear as a tricky obstruction in many questions of Galois theory over number fields, whatever the technical approach.

But it is clear that 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 arithmetical tools, to obtain numerical experiments and to understand the true p-adic difficulties.

A.3.4. *Principal Conjectures and Theorems.* Then considering the invariants $\mathcal{C}\ell_K$ (p-class group) and $\mathcal{T}_{K,P}$ (p-torsion group in P-ramification) as fundamental objects, we have given, for the abelian fields, the conjectural behaviour of their χ-components for irreducible p-adic characters χ [Gr1977]; 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 [Ri2008] about the so-called "Principal Theorem" stemming from Bernoulli–Kummer–Herbrand, then Mazur–Wiles–Thaine–Kolyvagin–Greither works on cyclotomy and p-adic L-functions, as a prelude of wide generalizations.

A.4. **Basic p-adic properties of $\mathcal{A}_{K,P}$ & $\mathcal{T}_{K,P}$.** During the 1980's, we have written in [Gr1982, Gr1983, Gr1984] 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:

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

are always injective [Gr1982, Théorème I.1]; which has major consequences for the arithmetic of number fields. Of course, this property has been obtained by Jaulent, Nguyen Quang Do and their students in other contexts (see Section A.5).

A.4.1. *The p-adic Log_P-function.*

Definition A.3. Let $I_{K,P}$ be the group of prime to p ideals of K. We define the logarithm function:

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

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 Log_P ([Gr1983, § 2, Théorème 2.1]), is that for any ideal $\mathfrak{a}\in I_{K,P}$, $\mathrm{Log}_P(\mathfrak{a})$ is the Artin symbol in the compositum $\widetilde{K}^P$ of the $\mathbb{Z}_p$-extensions of K in the canonical exact sequence:

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

which may be generalized with arbitrary S:

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

with an obvious definition of Log_S 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 [Gr1986, Theorems III.2.5] (under Leopoldt's conjecture):

$$\#\mathcal{T}_{K,S} = \#\mathcal{W}_{K,S} \times \#\mathcal{R}_{K,S} \times \frac{\#\mathcal{C}\ell_K}{\big(\mathbb{Z}_p\mathrm{Log}_S(I_{K,S}) : \mathbb{Z}_p\mathrm{Log}_S(P_{K,S})\big)}, \tag{A.5}$$

where $P_{K,S}$ is the group of principal ideals prime to S, so that $\mathbb{Z}_p\mathrm{Log}_S(P_{K,S})$ depends in an obvious manner of $\log_S(U_{K,S})$. Note that when $S \subsetneq P$ we can not write $\mathcal{W}_{K,S} = \mathrm{tor}_{\mathbb{Z}_p}(U_{K,S})/\mu_K$ (cf. Lemmas 2.1, 2.2).
For instance, for $S = P$, the Log_P-function allows, when $\mu_p \subset K$, the determination of the initial Kummer radical contained in $\widetilde{K}^P$ [Gr1985, Ja1986].

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, does exist whatever the Galois extension L/K:

Theorem A.4. [Gr1986, Proposition 6], [Ja1984, Section 2 (c)]. *Let L/K be a Galois extension of number fields and $G := \mathrm{Gal}(L/K)$. Let p be a prime number; we assume that L satisfies the Leopoldt conjecture for p. Then:*

$$\#\mathcal{T}_{L,P}^G = \#\mathcal{T}_{K,P} \times \frac{\prod\limits_{\mathfrak{l}\nmid p} e_{\mathfrak{l},p}}{\Big(\sum\limits_{\mathfrak{l}\nmid p} \frac{1}{e_{\mathfrak{l},p}}\mathbb{Z}_p\mathrm{Log}_P(\mathfrak{l}) + \mathbb{Z}_p\mathrm{Log}_P(I_{K,P}) : \mathbb{Z}_p\mathrm{Log}_P(I_{K,P})\Big)},$$

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

Remark A.5. Note that, contrary to the computation of $\mathrm{tor}_{\mathbb{Z}_p}(\overline{E}_K^S)$, 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 the Leopoldt conjecture (assumed) and its $\mathbb{Q}_p$-dimension is $r_1 + r_2 - 1$; for instance in the totally real case, we have $\bigoplus_{\mathfrak{p}\in P} K_{\mathfrak{p}} = \mathbb{Q}_p\log_P(E_K) \bigoplus \mathbb{Q}_p$, which allows explicit computations.

Corollary A.6 (invariant classes formula–totally real case)**.** *In the case of a totally real field L, the above formula becomes (still under Leopoldt's conjecture): $\#\mathcal{T}_{L,P}^G = \mathcal{T}_{K,P}^G \cdot p^{\rho-r} \cdot \prod_{\mathfrak{l}\nmid p} e_{\mathfrak{l},p}$, where $p^r \sim [L : K]$ and ρ is an obvious integer depending on the decomposition of the ramified primes $\ell \nmid p$ in L/K* [Gr1982, Théorème III.1].

A.4.3. *p-primitive ramification.* The fixed point formula allows to characterize the case where $\#\mathcal{T}_{L,P} = 1$ in a Galois p-extension L/K, which is equivalent to the two conditions, only depending on the base field K:

- $\#\mathcal{T}_{K,P} = 1$;
- $\Big(\sum\limits_{\mathfrak{l}\nmid p} \frac{1}{e_{\mathfrak{l},p}}\mathbb{Z}_p\mathrm{Log}_P(\mathfrak{l}) + \mathbb{Z}_p\mathrm{Log}_P(I_{K,P}) : \mathbb{Z}_p\mathrm{Log}_P(I_{K,P})\Big) = \prod\limits_{\mathfrak{l}\nmid p} e_{\mathfrak{l},p}$.

When the second condition above is fulfilled, we say, by definition, that the p-extension L/K is p-primitively ramified [Gr1986, Ch. III, Definition & Remark, p. 330] and that the set Σ of tame places $\mathfrak{l}$, ramified in L/K, is primitive, which is equivalent to say that:

$$\mathrm{Gal}(\widetilde{K}^P/K) \simeq \mathcal{A}_{K,P}/\mathcal{T}_{K,P} = \bigoplus_{\mathfrak{l}\in\Sigma} \left\langle \left(\frac{\widetilde{K}^P/K}{\mathfrak{l}}\right)\right\rangle \tag{A.6}$$

in terms of Frobenius automorphisms. Of course, any P-ramified extension is p-primitively ramified.

Then in [Gr1986, Ch. III, § 2, Theorem 2 and 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 [GJ1989]. We can state:

Theorem A.7. *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) $\mathcal{A}_{K,P} := \mathrm{Gal}(H_{K,P}/K) \simeq \mathbb{Z}_p^{r_2+1}$,

(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,*
- *$\mathcal{C}\ell_K \simeq \mathbb{Z}_p\mathrm{Log}_P(I_{K,P})/\log_P(U_K) \pmod{\mathbb{Q}_p\log_P(E)}$,*
- *$\mathrm{tor}_{\mathbb{Z}_p}(U_K) = \mu_p(K)$,*
- *$\mathbb{Z}_p\log_P(E)$ is a direct summand in $\log_P(U_K)$.*

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

A.5.1. *Infinitesimal arithmetic.* At the same time, in his Thesis [Ja1984, Ja1986], Jaulent defined the "infinitesimal" arithmetic in a number field proving, in a nice conceptual framework, generalizations of our previous results, adding Iwasawa theory results, study of the p-regularity (replacing $\mathcal{T}_{K,P}$ by the tame kernel $\mathrm{K}_2(Z_K)$ of the ring of integers of K), and genus theory.

In the same technical context Jaulent would write in [Ja1998, Ja2002] a $\ell\,(= p)$-adic class field theory and a logarithmic class field theory developed later in much papers, including computational methods [BJ2016]. He defines the logarithmic class group $\widetilde{\mathcal{C}\ell}_K$ whose finitness is equivalent to the Gross conjecture.

A.5.2. *Pro-p-group theory version for the study of $\mathcal{G}_{K,S}$.* Shortly after, at the end of the 1980's, in his thesis [Mo1988, Mo1990], Movahhedi gave a wide study of the abelian p-ramification theory, using mainely the properties of the pro-p-group $\mathcal{G}_{K,S}$ and deducing most of the previous items, then giving the main structural and cohomological properties of $\mathcal{G}_{K,P}$ and the characterization of the triviality of $\mathcal{T}_{K,P}$.

He proposes for this to speak of "p-rational fields" [Mo1990, Definitionn 1], that is to say the number fields K such that Leopoldt's conjecture holds for p and $\mathcal{T}_{K,P} = 1$; 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.8. [Mo1988, 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 Σ_K of tame primes, ramified in L/K, is p-primitive in K. Moreover, the extension Σ_L of Σ_K to L is p-primitive.*

For instance, this implies that if K is p-rational and Σ_K primitive, then any Σ_K-ramified p-extension L/K fulfills the Leopoldt conjecture and Σ_L is primitive.

Remark A.9. In practice, in research papers, one assumes in general an universal Leopoldt conjecture, so the statement becomes:

L is p-rational if and only if K is p-rational and Σ_K p-primitive

(equivalent to fix points formula).

In the 1990's, the classical results on p-ramification and p-regularity (about the triviality of the tame kernel $\mathrm{K}_2(Z_K)$), are amply illustrated in various directions: pro-p-group theory with explicit determination of a system of generators and relations for $\mathcal{G}_{K,S}$, primitive reciprocity laws, Galois cohomology, Iwasawa's theory, Leopoldt and Gross conjectures) by Movahhedi, Nguyen Quang Do, Jaulent [Mo1990, MN1990, JN1993] and also [BG1991/1992, JS1997, Ja1998].

Recall that in [Ja1987, Scolie, p. 112] Jaulent shows that the nullity of the p-Hilbert kernel $\mathrm{H}_2(L) \otimes \mathbb{Z}_p$ implies Leopoldt and Gross conjectures. Moreover [Ja1998] deals with ramification and decomposition.

Under the assumptions: $\mu_p \subset K$, $\mathrm{H}_2(L) \otimes \mathbb{Z}_p = 0$ and the existence of $\mathfrak{p}_0 \in S$ such that $\mu_{K_{\mathfrak{p}_0}} = \mu_K$, Nguyen Quang Do [Ng1991], after [Mo1988, MN1990] on the primitive reciprocity laws, describes (by means of generators and relations) the Galois group $\mathcal{G}_{K,S}$.

A.5.3. *Synthesis* 2003 – 2005. Because, among others, our Crelle papers were written in french, thus relatively ignored, all results and consequences, given in [Gr1977, Gr1982, Gr1983, Gr1984, Gr1985, Gr1986, Gr1998], were widely developed in [Gr2003/2005] where a systematic use of ramification and decomposition is considered, the infinite places playing a specific role (decomposition or complexification).

For instance [Gr2003/2005, Theorem V.2.4, Corollary V.2.4.2] gives 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., [HMR2018, Theorem 5.3], [HMR2019, Remark 2.2.] for the more recent ones).

A.6. **Present theoretical and algorithmic aspects.** One may say that there is no important progress for p-rationality, for itself, 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, numerical 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 $K^{\rm ab}$ be the maximal abelian extension of K. In [AS2013] Angelakis and Stevenhagen, after some work by Onabe [On1976] and by [Kub1957], provide a direct computation of the *profinite group* $A_K := {\rm Gal}(K^{\rm ab}/K)$ 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 all the groups $\mathcal{T}_{K,P}$ for all prime p. They obtain for instance, among other results and numerical illustrations [AS2013, Section 7]:

Theorem A.10. *An imaginary quadratic field $K \neq \mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$ of class number 1 has absolute abelian Galois group isomorphic to $\widehat{\mathbb{Z}}^2 \times \prod\limits_{n\geq 1} \mathbb{Z}/n\mathbb{Z}$.*

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 in [Gr2014] the generalization to an arbitrary K involves the $\mathcal{T}_{K,P}$ for all primes p, giving:

Theorem A.11. *Let $K^{\rm ab}$ 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 ${\rm Gal}(L_K/K) \simeq \prod_p \mathcal{T}_{K,P}$ and such that 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 (for some obvious integers δ and w):*

$$ {\rm Gal}\big(K^{\rm ab}/L_K\big) = \widehat{\mathbb{Z}}^{r_2+1} \times {\rm Gal}\big(K^{\rm ab}/\mathcal{H}_K\big) \overset{\rm nc}{\simeq} \widehat{\mathbb{Z}}^{r_2+1} \times \prod_{n\geq 1} \Big((\mathbb{Z}/2\,\mathbb{Z})^{\delta} \times \mathbb{Z}/w\,n\,\mathbb{Z} \Big). $$

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), an easy 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 [Gr2016]), or values of L-functions which intervenne as in [CoL2019, Go2001], and more or less, in many papers as [BGKK2018] when the normalized p-adic regulator is a unit. We have conjectured that $\mathcal{T}_{K,P} = 1$ for almost all p.

A.6.2. *Greenberg's conjecture on Iwasawa's λ, μ.* For a totally real number field K, consider (under the Leopoldt conjecture) the cyclotomic $\mathbb{Z}_p$-extension K_∞ of K. Then Greenberg has conjectured in [Gre1976] that the Iwasawa's invariants λ and μ 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 $\widetilde{\mathcal{C}\ell}_K$ (the logarithmic class group of Jaulent) are in some sense "governing invariants" for the Greenberg conjecture; for this, see [Gr2016/2017, Théorèmes 3.4, 4.8, 6.3], [Gr2018] about $\mathcal{T}_{K,P}$, then an interpretation by Jaulent with the group of universal norms [Ja2019] and the following criterion:

Theorem A.12. [Ja2018, Théorème 7, § 1.4]. *The totally real number field K fulfills the conjecture of Greenberg if and only if its logarithmic class group capitulates in K_∞.*

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 groups $\mathcal{T}_{K,P}$ *never capitulate*. Moreover the property of capitulation (well-known in Hilbert's class fields) is more general for generalized ray class groupsand, especially, is possible in *absolute abelian extensions* as shown in many papers including [Gr1997, Bos2009, Ja2018', Ja2018/2019].

A.6.3. *Galois representations with open image.* For constructions by Greenberg of continuous Galois representations $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{Z}_p)$ with open image [Gre2016], the p-rational fields play a great role, and the first obvious case is that of regular cyclotomic fields $\mathbb{Q}(\mu_p)$ which are p-rational (yet reported by [Sha1964], [Gr1986], and generalized by introducing in [GJ1989] the notion of p-regularity that we do not develop in this survey, for short, but which behaves as p-rationality).

Then, an interesting typical conjecture is the following:

Conjecture A.13. [Gre2016, Conjecture 4.2.1]. *For any odd prime p and for any t, there exists a p-rational field K such that* $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^t$.

Numerical examples have been given for various p and t [Gre2016, BR2017, Bou2018, MR2018/2019]. Some PARI/GP programs are given in [Pi2010, PV2015], [Gr2017/2018, § 5.2] showing the 3-rationality of:

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

A.6.4. *Rarity of cases of non-triviality of $\mathcal{T}_{K,P}$. Conjectures.* We have conjectured in [Gr2016, 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 [Gr2018/1919, Conjecture 8.1]:

Conjecture A.14. *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 $\mathcal{C}_p := \sup\limits_K(C_p(K))$, $\mathcal{C}_K := \sup\limits_p(C_p(K))$.

(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, $\limsup\limits_p(C_p(K)) = 0$.

(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.14).

These questions being out of reach, many results give, on the contrary, the infinteness of primes p giving p-rationality of a field K, in general under the $a\,b\,c$ conjecture, and following the method given by [Si1988, GM2013, BGKK2018, MR2019]; for instance:

Theorem A.15. [MR2019, Corollary to Theorem A] *Let K be a real quadratic field or an imaginary S_3-extension. If the generaalized abc-conjecture holds for K, then $\#\{p \leq x,\ K$ is p-rational$\} \geq c \cdot \log(x)$ as $x \to \infty$, for some constant $c > 0$ depending on K.*

This show the awesome distance between the two aspects of the problem; indeed, for $K = \mathbb{Q}(\sqrt{5})$, no prime number 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 [Shu2018] gives general formulae of the root numbers of the Jacobian varieties of the Fermat curves $X^p + Y^p = \delta$, where δ is an integer, and studies their distribution.

(ii) Davis–Pries [DP2018] work in P-ramified Kummer extensions with $P = \{\mathfrak{p} = (1-\zeta_p)\}$, as follows. Let $L \subset H_{K,P}$ be defined by:

$$L = K\big(\sqrt[p]{\zeta_p},\ \sqrt[p]{1-\zeta_p}, \cdots,\ \sqrt[p]{1-\zeta_p^r}\big),\ \ r = \tfrac{p-1}{2},$$

The Kummer radical of L is also generated by the real cyclotomic units and the two numbers ζ_p and $1-\zeta_p$; so, under Vandiver's 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 $\mathrm{rk}_p(\mathrm{Gal}(E/L)) = r \cdot p^{r+1} + 1$. One can deduce that $\mathcal{C}\ell_L = \mathcal{C}\ell_E = 1$ 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 $\#\mathcal{C}\ell_K = p$ and where $H_K \subseteq L$ in which p splits, the formula of Theorem A.1 gives $\mathrm{rk}_p(\mathcal{T}_{L,P}) = \mathrm{rk}_p(\mathcal{C}\ell_L^P) + p - 1$, whence $\mathrm{rk}_p(\mathrm{Gal}(E/L)) = r \cdot p^{r+1} + 2r + 1 + \mathrm{rk}_p(\mathcal{C}\ell_L^P)$ depending on $\mathcal{C}\ell_L^P$.

The purpose of [DP2018] is to get information on $\mathrm{H}^1(\mathrm{Gal}(E/K), M)$ for $\mathrm{Gal}(E/K)$-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 $xy = 0$.

A.6.6. *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 [Cha1982]. In [Hat1987, Hat1988] the computations correspond to statistics about the values (modulo p) of the normalized regulator $\mathcal{R}_{K,P}$ of $K = \mathbb{Q}(\sqrt{5})$.

A most precise study of p-rationality of imaginary quadratic fields is given by Angelakis–Stevenhagen in [AS2013, Section 7].

A wide study of $\mathcal{T}_{K,P}$ with tables and publication of PARI/GP programs is done by Pitoun–Varescon [Pi2010, PV2015]; but these more conceptual programs are not so easy to be used by the reader.

In [HZ2016] 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 [Gre2016] Barbulescu–Ray [BR2017] give explicit p-rational large compositum of quadratic fields. We may cite some similar works by Bouazzaoui [Bou2018], by El Habibi–Ziane [ElHZ2018], then [Gr2017/2018] with programs.

In the similar context, a new PARI/GP program allows the computation of the logarithmic class groups of a number field by Belabas–Jaulent [BJ2016].

In another direction, the paper [MR2018/2019] of Maire–Rougnant gives non-trivial examples of "p-rationalities" 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 [Gr2018/1919], 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.7. **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, [HM2017/2019] by Hajir–Maire on the μ-invariant in Iwasawa's theory, then [HMR2018] by Hajir–Maire–Ramakrishna, showing the existence of p-rational fields having a large p-rank of the class group, or [HMR2019] showing the existence of a solvable number field L, P-ramified, whose p-Hilbert class field tower is infinite.

Of course it is not possible to evoque 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, the notion of "mild groups" introduced by Labute [Lab2006] dealing with the numbers of generators $d(G)$ and of relations $r(G)$:

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 where then published giving an overview of the wide variety of such groups as the following short excerpt of a result of Schmidt [Sch2010, 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 returning to the basic invariants, we may indicate two open questions:

(i) We know the fixed points 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 [Gr2015/2016] after a very long hystory), we do not know how to compute the filtration $(M_i)_{i\geq 0}$, of $M := \mathcal{T}_{K,P}$, defined inductively by $M_0 = 1$ and $M_{i+1}/M_i := (M/M_i)^G$ for all $i \geq 0$.

(ii) The explicit computation of the p-rank, $\widetilde{r}_{K,S}$ (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). Then one may think that the result depends, for fixed Galois groups, on a finite number of cases regarding the possible families of decomposition groups of p and ∞. In the definition of $\mathcal{W}_{K,S} := W_{K,S}/\mathrm{tor}_{\mathbb{Z}_p}(\overline{E}_K^S)$, we do not know how to compute $\mathrm{tor}_{\mathbb{Z}_p}(\overline{E}_K^S)$. We ignore, in a p-adic framework, if Leopoldt's conjecture is sufficient to obtain the responses apart from a Galois context.

We hope that our programs 3.1.2 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

[AF1972] Y. Amice et J. Fresnel, *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

[AS2013] Angelakis, A. and 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

[BG1991/1992] Berger, R.I. and 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

[BGKK2018] Boeckle, G., Guiraud, D.-A., Kalyanswamy, S. and Khare, C., *Wieferich Primes and a mod p Leopoldt Conjecture* (2018). arXiv:1805.00131

[BJ2013] Bourbon, C. et Jaulent, J-F., *Propagation de la* 2*-birationalité*, Acta Arithmetica 160 (2013), 285–301. https://doi.org/10.4064/aa160-3-5

[BJ2016] Belabas, K. and 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

[Bos2009] 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

[Bou2018] Bouazzaoui, Z., *Fibonacci sequences and real quadratic p-rational fields* (2019). https://arxiv.org/abs/1902.04795v1

[BP1972] Bertrandias, F. et Payan, J-J., Γ*-extensions et invariants cyclotomiques*, Ann. Sci. Ec. Norm. Sup. 4, 5 (1972), 517–548. https://doi.org/10.24033/asens.1236

[Br1966] 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

[BR2017] Barbulescu, R. and Ray, J., *Some remarks and experimentations on Greenberg's p-rationality conjecture* (2017). https://arxiv.org/pdf/1706.04847.pdf

[Cha1982] 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^e cycle, Mathématiques, Université de Franche-Comté (1982), 50 pp.

[Co1977] Coates, J., *p-adic L-functions and Iwasawa's theory*, In: Proc. of Durham Symposium 1975, New York-London (1977), 269–353.

[Col1988] Colmez, P., *Résidu en* $s = 1$ *des fonctions zêta p-adiques*, Invent. Math. 91 (1988), 371–389.https://eudml.org/doc/143545

[CoL2019] Coates, J. and Li, Y., *Non-vanishing theorems for central L-values of some elliptic curves with complex multiplication*. https://arxiv.org/abs/1811.07595

[DP2018] Davis, R.; Pries, R., *Cohomology groups of Fermat curves via ray class fields of cyclotomic fields* (2018). https://arxiv.org/pdf/1806.08352.pdf.

[ElHZ2018] El Habibi, A. and Ziane, M., *p-Rational Fields and the Structure of Some Modules* (2018). https://arxiv.org/abs/1804.10165

[EV2007] Ellenberg, J. S. and 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

[FV2002] Fesenko, I. B. and Vostokov, S. V., *Local Fields and Their Extensions*, American Math Society, Translations of Math Monographs, vol. 121, Second Edition 2002.https://www.maths.nottingham.ac.uk/personal/ibf/book/vol.pdf

[GJ1989] Gras, G. and Jaulent, J-F., *Sur les corps de nombres réguliers*, Math. Z. **202**(3) (1989), 343–365. https://eudml.org/doc/174095

[GM2013] Graves, H. and Murty, M.R., *The abc conjecture and non-Wieferich primes in arithmetic progressions*, Journal of Number Theory 133 (2013), 1809–1813. http://www.sciencedirect.com/science/article/pii/S0022314X12003368

[Go2001] Goren, E.Z., *Hasse invariants for Hilbert modular varieties*, Isr. J. Math. (2001) 122 (2001), 157–174. https://link.springer.com/article/10.1007/BF02809897

[Gr1977] 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/

[Gr1982] 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://www.researchgate.net/publication/243110955 https://eudml.org/doc/152440

[Gr1983] 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

[Gr1984] 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

[Gr1985] 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

[Gr1986] Gras, G., *Remarks on K_2 of number fields*, Jour. Number Theory **23**(3) (1986), 322–335. http://www.sciencedirect.com/science/article/pii/0022314X86900776

[Gr1997] Gras, G., *Principalisation didéaux par extensions absolument abéliennes*, J. Number Th. 62 (1997), 403–421. https://doi.org/10.1006/jnth.1997.2068

[Gr1998] 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/

[Gr2003/2005] Gras, G., *Class Field Theory: from theory to practice*, G. Gras, *Class Field Theory: from theory to practice*, corr. 2nd ed., Springer Monographs in Mathematics, Springer, 2005, xiii+507 pages.

[Gr2014] Gras, G., *On the structure of the Galois group of the Abelian closure of a number field*, J. de théorie des nombres de Bordeaux **26**(3) (2014), 635–654. http://www.numdam.org/article/JTNB_2014__26_3_635_0.pdf

[Gr2015/2016] Gras, G., *Invariant generalized ideal classes–Structure theorems for p-class groups in p-extensions*, Proc. Indian Acad. Sci. (Math. Sci.)First Online: 17 January 2017, 127, no. 1, 1–34. https://www.ias.ac.in/article/fulltext/pmsc/127/01/0001-0034

[Gr2016] Gras, G., *Les θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques*, Canadian Journal of Mathematics **68**(3) (2016), 571–624. http://dx.doi.org/10.4153/CJM-2015-026-3 https://arxiv.org/pdf/1701.02618.pdf

[Gr2016/2017] 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

[Gr2017] Gras, G., *The p-adic Kummer-Leopoldt Constant: Normalized p-adic Regulator*, Int. J. Number Theory **14** (2018), no. 2, 329–337 (Published 29 August 2017). https://doi.org/10.1142/S1793042118500203

[Gr2017/2018] 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.pdf

[Gr2018] Gras, G., *Normes d'idéaux dans la tour cyclotomique et conjecture de Greenberg*, Annales mathématiques du Québec, Online: 17 October 2018. https://doi.org/10.1007/s40316-018-0108-3

[Gr2018'] Gras, G., *Annihilation of* $\mathrm{tor}_{\mathbb{Z}_p}(\mathcal{G}_{K,S}^{\mathrm{ab}})$ *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

[Gr2018/1919] Gras, G., *Heuristics and conjectures in direction of a p-adic Brauer–Siegel theorem*, Math. Comp. (2018). https://doi.org/10.1090/mcom/3395

[Gr2019] Gras, G., *Test of Vandiver's conjecture with Gauss sums – Heuristics* (preprint 2019). https://arxiv.org/abs/1808.03443

[Gre1976] 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?

[Gre2016] Greenberg, R., *Galois representations with open image*, Annales de Mathématiques du Québec, special volume in honor of Glenn Stevens, **40**(1) (2016), 83–119. https://link.springer.com/article/10.1007/s40316-015-0050-6

[Hab1978] 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.

[Hat1987] 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.

[Hat1988] 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.

[HM2001] Hajir, F. and Maire, C., *Tamely ramified towers and discriminant bounds for number fields*, Compositio Math. 128 (2001), 35–53. https://doi.org/10.1023/A:1017537415688

[HM2002] Hajir, F. and Maire, C. *Extensions of number fields with wild ramification of bounded depth*, International Mathematics Research Notices (2002), No. 13, 667–696. http://people.math.umass.edu/~hajir/hajir-imrn.pdf

[HM2002'] Hajir, F. and 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/jsco.2001.0514

[HM2017/2019] Hajir, F. and 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

[HM2018] Hajir, F. and Maire, C. *Analytic Lie extensions of number fields with cyclic fixed points and tame ramification* (2018). arXiv:1710.09214

[HMR2018] Hajir, F. and Maire, C., Ramakrishna, R., *Cutting towers of number fields* (2019). https://arxiv.org/abs/1901.04354

[HMR2019] Hajir, F. and Maire, C., Ramakrishna, R., *Infinite class field towers of number fields of prime power discriminant* (2019). https://arxiv.org/pdf/1904.07062.pdf

[HZ2016] Hofmann, T. and 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

[Ja1984] 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

[Ja1985] Jaulent, J-F., *Sur lindépendance ℓ-adique de nombres algébriques*, J. Number Theory (20) (1985), 149–158. https://doi.org/10.1016/0022-314X(85)90035-6

[Ja1986] Jaulent, J-F., *L'arithmétique des ℓ-extensions* (Thèse de doctorat d'Etat), Pub. Math. Besanon (1986), 1–349. http://pmb.univ-fcomte.fr/1986/Jaulent_these.pdf

[Ja1987] 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/

[Ja1998] Jaulent, J-F., *Théorie ℓ-adique globale du corps de classes*, J. Théorie des Nombres de Bordeaux **10**(2) (1998), 355–397. http://www.numdam.org/article/JTNB_1998__10_2_355_0.pdf

[Ja2002] 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

[Ja2018] Jaulent, J-F., *Note sur la conjecture de Greenberg*, J. Ramanujan Math. Soc. 34 (2019) 59–80. https://arxiv.org/pdf/1612.00718.pdf

[Ja2018'] Jaulent, J-F., *Principalisation abélienne des groupes de classes de rayons* (preprint 2018). https://arxiv.org/abs/1801.07173

[Ja2018/2019] Jaulent, J-F., *Principalization of logarithmic class groups* (preprint 2019). https://arxiv.org/abs/1801.07176

[Ja2019] Jaulent, J-F., *Normes universelles et conjecture de Greenberg* (preprint 2019).

https://arxiv.org/abs/1904.07014

[JN1993] Jaulent, J-F. et 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

[JS1997] Jaulent et J-F., Sauzet, O. *Pro-ℓ-extensions de corps de nombres ℓ-rationnels*, J. Number Th. 65 (1997), 240–267; ibid. 80 (2000), 318–319. https://doi.org/10.1006/jnth.1997.2158

[JS2000] Jaulent, J-F. et Sauzet, O., *Extensions quadratiques* 2*-birationnelles de corps de nombres totalement réels*, Pub. Matemàtiques 44 (2000), 343–351. https://www.math.u-bordeaux.fr/~jjaulent/Articles/Ext2bi.pdf

[Ko1970/2002] Koch, H., *Galois theory of p-extensions* (English translation of *"Galoissche Theorie der p-Erweiterungen"*, 1970), Springer Monographs in Math., Springer-Verlag 2002.

[Kub1957] Kubota, T., *Galois group of the maximal abelian extension of an algebraic number field*, Nagoya Math. J. 12 (1957), 177–189.

[Lab2006] 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

[Le2018] 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

[M2002] 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

[M2003] 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

[M2005] 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/

[M2010] 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

[M2017] Maire, C., *On the quotients of the maximal unramified* 2*-extension of a number field*, Documenta Mathematica 23 (2018), 1263–1290.

[Mi1978] Miki, H., *On the maximal abelian ℓ-extension of a finite algebraic number field with given ramification*, Nagoya Math. J. 70 (1978), 183–202. https://doi.org/10.1017/S0027763000021875

[MN1990] Movahhedi, A. et Nguyen Quang Do, T., *Sur l'arithmétique des corps de nombres p-rationnels*, Séminaire de Théorie des Nombres, Paris 1987–88, Progress in Math., Volume 81, 1990, 155–200. https://doi.org/10.1007/978-1-4612-3460-9_9

[Mo1988] Movahhedi, A., *Sur les p-extensions des corps p-rationnels*, Sur les p-extensions des corps p-rationnels, Thèse, Université Paris VII (1988). http://www.unilim.fr/pages_perso/chazad.movahhedi/These_1988.pdf

[Mo1990] 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/

[MR2018/2019] Maire, C. et 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

[MR2019] Maire, C. and Rougnant, M., *A note on p-rational fields and the abc-conjecture* (2019). arXiv:1903.11271

[Nel2013] Nelson, D., *A variation on Leopoldt's conjecture: some local units instead of all local units*. https://arxiv.org/abs/1308.4637

[Neu1975] 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.

[Neu1976] 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.

[Ng1982] Nguyen Quang Do, T., *Sur la structure galoisienne des corps locaux et la théorie d'Iwasawa*, Compositio Mathematica, Tome 46 (1982), no. 1, 85–119. http://www.numdam.org/item/?id=CM_1982__46_1_85_0

[Ng1986] Nguyen Quang Do, T., *Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens*, Ann. Inst. Fourier 36, 2 (1986), 27–46. https://doi.org/10.5802/aif.1045

[Ng1991] Nguyen Quang Do, T., *Lois de réciprocité primitives*, manuscripta math. 72 (1991), no. 1, 307–324. https://doi.org/10.1007/BF02568282

[On1976] Onabe, M., *On the isomorphisms of the Galois groups of the maximal abelian extensions of imaginary quadratic fields*, Natur. Sci. Rep. Ochanomizu Univ. **27**(2) (1976), 155–161. http://teapot.lib.ocha.ac.jp/ocha/bitstream/10083/2243/1/

[P2016] The PARI Group–*PARI/GP, version `2.9.0`*, Université de Bordeaux (2016). http://pari.math.u-bordeaux.fr/

[Pi2010] 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

[PV2015] Pitoun, F. and Varescon, F., *Computing the torsion of the p-ramified module of a number field*, Math. Comp. **84**(291) (2015), 371–383. https://doi.org/10.1090/S0025-5718-2014-02838-X

[Ri2008] 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

[Sch2010] 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

[Se1964] Serre, J-P., *Cohomologie galoisienne*, Lect. Notes in Math. 5, Springer-Verlag 1964, cinquième édition 1991; English translation: *Galois cohomology*, Springer-Verlag 1997; corrected second printing: Springer Monographs in Math. 2002.

[Se1978] Serre, J-P., *Sur le résidu de la fonction zêta p-adique d'un corps de nombres*, C.R. Acad. Sci. Paris 287, Série I (1978), 183–188.

[Sha1964] 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

[Shu2018] Shu, J., *Root numbers and Selmer groups for the Jacobian varieties of Fermat curves* (preprint 2018). https://arxiv.org/pdf/1809.09285v2.pdf

[Si1988] 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

[Win1989] 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

[Win1991] 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

[Ya1993] Yamagishi, M., *A note on free pro-p-extensions of algebraic number fields*, Journal de théorie des nombres de Bordeaux, Tome 5 (1993) no. 1,165–178. 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