Numerical verification of the Cohen-Lenstra-Martinet heuristics and of Greenberg's p-rationality conjecture

Razvan Barbulescu, Jishnu Ray

SOME REMARKS AND EXPERIMENTS ON GREENBERG'S p-RATIONALITY CONJECTURE

RAZVAN BARBULESCU AND JISHNU RAY

Abstract. A recent result of Greenberg raises the question of solving the inverse Galois problem for p-rational number fields. In this article we recall the cases which are directly inferred from the literature and the cases that are consequences of conjectures in the literature. We propose new algorithms to compute the density of p-rational fields faster than by applying the algorithm of Pitoun and Varescon.

1. Introduction

The notion of p-rationality of number fields naturally appears in several branches of number theory. In Iwasawa theory, the study of Galois groups of infinite towers of number fields, a celebrated conjecture of Greenberg concerns the λ-invariant [Gre76] which has been connected to p-rationality [Sau98, Th. 1.1]. In the study of the inverse Galois problem, Greenberg [Gre16] proposed a method to prove that a p-adic Lie group appears as a Galois group over $\mathbb{Q}$ under the assumption of existence of p-rational fields. In algorithmic number theory, the density of p-rational number fields is related to the Cohen-Lenstra-Martinet heuristic [CL84b, CM90] and to the valuation of the p-adic regulator [Gra14, HZ16].

The context in which the notion of p-rationality was introduced includes the work of Shafarevich [Sha66] which, for any regular prime p, proved properties of the p-part of the Ray class group of the p-th cyclotomic fields. Gras and Jaulent [GJ89] defined p-regular number fields, which have similar properties to cyclotomic fields associated to regular primes. Movahhedi [Mov88, Chap II] defined the p-rational fields in his thesis. Nguyen Quang Do and Jaulent [JNQD93] proved that there is a large intersection between the set of p-regular and p-rational fields. The object of this paper is to describe families of p-rational Galois fields over $\mathbb{Q}$.

Let K be a Galois number field of signature (r_1, r_2), p an odd prime, $\mu(K)_p$ the roots of unity in K whose order is a power of p, S_p the set of prime ideals of K above p, M the compositum of all finite p-extensions of K which are unramified outside S_p and M^{ab} the maximal abelian extension of K contained in M. Note that the group $\Gamma := \mathrm{Gal}(M/K)$ is a pro-p group and that $\Gamma^{ab} \cong \mathrm{Gal}(M^{ab}/K)$ is the maximal abelian quotient of Γ.

Proposition-Definition 1.1 ([MNQD90] and [Mov90])**.** The number field K is said to be p-rational if the following equivalent conditions are satisfied:

(1) $\mathrm{rank}_{\mathbb{Z}_p}(\Gamma^{ab}) = r_2 + 1$ and Γ^{ab} is torsion-free as a $\mathbb{Z}_p$-module,
(2) Γ is a free pro-p group with $r_2 + 1$ generators,
(3) Γ is a free pro-p group.

If K satisfies Leopoldt's conjecture [Was97, Sec 5.5] (e.g. K is abelian) then the above conditions are also equivalent to

(4)
- $\left\{\alpha \in K^\times \mid \begin{array}{c}\alpha\mathcal{O}_K = \mathfrak{a}^p \text{ for some fractional ideal } \mathfrak{a} \\ \text{and } \alpha \in (K_\mathfrak{p}^\times)^p \text{ for all } \mathfrak{p} \in S_p\end{array}\right\} = (K^\times)^p$
- and the map $\mu(K)_p \to \prod_{\mathfrak{p}\in S_p} \mu(K_\mathfrak{p})_p$ is an isomorphism.

The equivalent conditions of $1, 2$, 3 and 4 can also be found in [Gre16, Sec. 3] and chapter II of Movahhedi's thesis [Mov88]. One can directly prove that a field is p-rational using this definition, but more elaborated results allow to write shorter proofs. All over the article we illustrate the strength of each result by proving p-rationality of some number fields. Many of these number fields are settled to be p-rational or not, the focus is on the method of proof not on the examples.

Examples 1.2.

(1) The imaginary quadratic fields of class number one, i.e. $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, $\mathbb{Q}(\sqrt{-163})$ are p-rational for any primes $p \geq 5$. Indeed, in order to use point (4) of Definition 1.1 let K be any of the above fields and α an element of K which is a p-th power in all the p-adic completions of K and such that the principal ideal generated by α is a p-th power. Since the ring of integers of K is a principal ideal domain α is a p-th power in K, up to multiplication by a unit. Since the unit rank of K is zero and since K has no p-th roots of unity we conclude that α is a p-th power of K. Since $p \geq 5$, $\mathbb{Q}_p$ and its quadratic extensions have no p-th roots of unity so that $\mu(K)_p \to \prod_{\mathfrak{p}\in S_p} \mu(K_\mathfrak{p})_p$ is an isomorphism.

(2) $\mathbb{Q}(i)$ is 2-rational As in the case of $p \geq 5$ we are left with showing that if a unit of $\mathbb{Q}(i)$ is a square in the 2-adic completion then it is a square in $\mathbb{Q}(i)$. Suppose that i is a square in the completion of $\mathbb{Z}[i]$ with respect to $\mathfrak{p} = \langle 1 + i\rangle$. Then there exist two integer a and b such that

$$(a + ib)^2 \equiv i \pmod{\mathfrak{p}^2}.$$

But $\mathfrak{p}^2 = 2\mathbb{Z}[i]$, so $2ab \equiv 1 \pmod 2$, which is a contradiction. Hence the only elements of $\mathbb{Q}(i)$ which are squares in the 2-adic completion of $\mathbb{Q}(i)$ are also squares in $\mathbb{Q}(i)$.

These examples are also treated in [Mov90, Example (c), page 24].

For many properties of p-rational fields we refer the reader to the corresponding chapter of [Gra13, Ch IV.3].

Greenberg's result [Gre16, Prop 6.1] is as follows: if K is abelian and p-rational with the order of $\mathrm{Gal}(K/\mathbb{Q})$ dividing $p - 1$ then, for all $n \in \mathbb{N}$, there exists an explicit continuous representation

$$\rho : \mathrm{Gal}(M/\mathbb{Q}) \to \mathrm{GL}(n, \mathbb{Z}_p)$$

such that $\rho(\Gamma)$ is the pro-p Iwahori subgroup of $\mathrm{SL}(n, \mathbb{Z}_p)$, i.e. the subgroup of $\mathrm{SL}(n, \mathbb{Z}_p)$ whose reduction mod p is the upper unipotent subgroup, under an assumption on the characters of $\mathrm{Gal}(K/\mathbb{Q})$. We recall that M is the compositum of all finite p-extensions of K which are unramified outside the places of K above p. We obtain hence the existence of the morphism ρ above as soon as we can prove the existence of p-rational fields K with an additional property on the characters.

Using the existence of the same p-rational number fields, Cornut and Ray [CR16, Sec 3] showed that the pro-p Iwahori subgroup $I(1)$ of an adjoint simple reductive

group $\mathbf{G}$ appears as a Galois group of an infinite extension of K. More precisely, they have constructed a continuous morphism

$$\rho : \mathrm{Gal}(M/\mathbb{Q}) \to I$$

such that $\rho(\mathrm{Gal}(M/K)) = I(1)$, where I is the Iwahori subgroup of $\mathbf{G}$ (cf. corollary 3.4.4 of [CR16]). This gives the construction of Galois representations with large open images in the $\mathbb{Z}_p$-points of the reductive group $\mathbb{G}$. Note that the assumption on the characters is met if K is the cyclotomic field $\mathbb{Q}(\zeta_p)$ and p is a prime greater than a constant $c_{\mathbf{G}}$ depending on the type of $\mathbf{G}$ (cf. Sec 3.4 of [CR16]).

Greenberg also noted that the hypothesis on the characters are met if K is complex and the Galois group $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^t$ for some t, which raises the question of existence of p-rational fields with such Galois groups. The goal of this work is to investigate the following conjecture:

Conjecture 1.3 (Greenberg [Gre16])**.** *For any odd prime p and for any t, there exist a p-rational field K such that* $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^t$.

In this article we are investigating a generalization of Greenberg's conjecture to other finite groups.

Problem 1.4. Given a finite group G and a prime p, decide the following statements:

(1) Greenberg's conjecture holds for G and p: there exists a number field of Galois group G which is p-rational, in this case we say that $\mathrm{GC}(G,p)$ is true;
(2) the infinite version of Greenberg's conjecture holds for G and p: there exist infinitely many number fields of Galois group G which are p-rational, in this case we say that $\mathrm{GC}_\infty(G,p)$ is true.

Note that this problem is a strengthening of the inverse Galois problem, which is itself open in the non-abelian case (cf [MM13]). Also note that we don't discuss the related conjecture of Gras [Gra14, Conj. 8.11] which states that every number field is p-rational for all but finitely many primes.

Remark 1.5. One should not confound this new conjecture to an older conjecture on Iwasawa invariants (cf [Gre76]). Let $\mathcal{K}$ be the pairs of totally real fields K and primes p which otally splits in K. Due to Remark 2.2 of [Gra16], a particular case of the celebrated conjecture of Greenberg concerning the Iwasawa invariants and a strengthening of the newer p-rationality conjecture of Greenberg can be stated as follows :

invariants conjecture:	$\forall (K,p) \in \mathcal{K}$,	$\lambda = \mu = 0$
p-rationality conjecture:	$\forall t$, $\forall p$, $\exists K$,$(K,p) \in \mathcal{K}$, $\mathrm{Gal}(K) = (\frac{\mathbb{Z}}{2\mathbb{Z}})^t$,	$\lambda = \mu = \nu = 0$,

where $\lambda = \lambda_p(K), \mu = \mu_p(K), \nu = \nu_p(K)$ are the Iwasawa invariants associated to the ideal class group of the cyclotomic $\mathbb{Z}_p$-extension K_∞/K (cf. [Gre76], see also [Was97] for the fact that $\mu = 0$ when K is abelian). The case of totally split p is a particular case of Greenberg's invariants conjecture, but it is an open case. Greenberg's p-rationality conjecture doesn't put conditions on K being totally real but any compositum of quadratic fields has a maximal real subfield whose degree is at least half of the total degree. The condition that p is totally split is not discussed in the rest of the article but numerical experiments show that it is not hard to satisfy this additional constraint.

The main results in this article are summarized by the following theorem. Let Φ_m denote the cyclotomic polynomial associated to m and $\varphi(m)$ its degree.

Theorem 1.6.

(1) *For all odd primes p, $\mathrm{GC}_\infty(\mathbb{Z}/2\mathbb{Z}, p)$ holds.*
(2) *Assume there exist infinitely many odd integers $a \not\equiv 21, 23 \pmod{25}$ so that, for $m = \frac{1}{4}(a^2+27)$, $3 \mid \varphi(m)$, $11 \nmid \varphi(m)$ and Φ_m is irreducible modulo 11 and 2. Then $\mathrm{GC}_\infty(\mathbb{Z}/3\mathbb{Z}, 5)$ holds.*
(3) *Under conjectures based on heuristics and numerical experiments (Conjecture 5.4 and Conjecture 5.2), when $q = 2$ or 3, for any prime p and any integer t such that $p > 5q^t$, $\mathrm{GC}_\infty((\mathbb{Z}/q\mathbb{Z})^t, p)$ holds.*

Roadmap. In Section 2, we relate the notion of p-rationality to that of class number and p-adic regulator, which is enough to prove $\mathrm{GC}_\infty(\mathbb{Z}/2\mathbb{Z}, 3)$, which is point (1) of Theorem 1.6, and to give an example of p-rational field with Galois group $(\mathbb{Z}/2\mathbb{Z})^5$. We also recall the existing conjectures on class number (Cohen-Lenstra-Martinet) and p-adic regulator.

In Section 3, we start by recalling an algorithm to test the divisibility by p of the class number of cyclic cubic fields without computing the class number, due to N.-M. Gras. Furthermore we give a new algorithm to produce units in cyclic cubic fields which are used to test the valuation in p of the p-adic regulator, which is faster then computing a system of fundamental units. Then we recall the algorithm of Pitoun and Varescon to test p-rationality for arbitrary number fields, which allows us to give examples of p-rational number fields of non-abelian Galois groups.

In Section 4, we find a family of cyclic cubic number fields which contains infinitely many 5-rational fields under a list of arithmetic assumptions; this proves point (2) of Theorem 1.6.

In Section 5, we do a numerical experiment to test divisibility by p of the class number of cyclic cubic fields with discriminant up to 10^{14}, which extends the existing calculations [CM87], confirming the Cohen-Lenstra-Martinet conjecture. Then we do a numerical experiment for number fields of Galois group $(\mathbb{Z}/3\mathbb{Z})^2$ and discriminant up to 10^{12} and, thanks to its agreement with the Cohen-Lenstra-Martinet heuristic, we can write down Conjecture 5.2 on the divisibility by p of the class number of such fields. Next we prove a Kuroda-like formula for p-adic regulators of fields of Galois group $(\mathbb{Z}/2\mathbb{Z})^2$, which relates the p-adic regulator of the compositum to those of the quadratic subfields. Based on a heuristic and numerical experiments we write down Conjecture 5.4 which applies to fields of Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ where $q = 2$ or 3. This allows us to prove point (3) of Theorem 1.6.

Acknowledgments

We are very grateful to Ralph Greenberg who encouraged us to study this conjecture.

2. Preliminaries

In the general case, p-rationality is hard to test so that it is important to have a simple criterion in terms of classical invariants as the class number and p-adic regulator (Sec 2.1). This raises the question of the density of number fields whose

class number is not divisible by p (Sec 2.2) and of the valuation in p of the p-adic regulator (Sec 2.3).

In this sequel, p denotes an odd prime and K an abelian number field, $\mathrm{Disc}(K)$ the discriminant of K, $\mathcal{O}_K$ the ring of integers, E_K the unit group, $cl(K)$ the ideal class group of K, $cl_p(K)$ the p-part of the class group $cl(K)$, h_K the class number of K, (r_1, r_2) the signature of K, $r = r_1 + r_2 - 1$ the rank of E_K, S_p the set of primes of K lying above p, $K_\mathfrak{p}$ the completion of K at a prime $\mathfrak{p} \in S_p$. For $c \in \mathbb{N}^*$ we denote ζ_c a primitive c-th root of unity.

2.1. **A simple criterion to prove p-rationality.** Let us call p-primary unit, any unit in K which is a p-th power in $K_\mathfrak{p}$ for any $\mathfrak{p}$ but which is not a p-th power in K.

Lemma 2.1 ([Mov88] Chap II)**.** *Assume K is a number field which satisfies Leopoldt's conjecture, p an odd prime such that $p \nmid h_K$ and K has no p-th roots of unity. Then K is p-rational if and only if K has no p-primary units.*

Proof. If K has a p-primary unit α then $\alpha\mathcal{O}_K = (\mathcal{O}_K)^p$ and this proves that K is not p-rational (point (4) of Definition 1.1).

Conversely assume that K has no p-primary units. Let $\alpha \in K^*$ be such that $\alpha\mathcal{O}_K = \mathfrak{a}^p$ and $\forall \mathfrak{p} \mid p$, $\alpha \in (K_\mathfrak{p})^p$. Then $\mathfrak{a}$ is a p-torsion element in the class group, which has order relatively prime to p so $\mathfrak{a}$ is a principal ideal. If β be a generator of $\mathfrak{a}$ then $\alpha\mathcal{O}_K = \beta^p\mathcal{O}_K$ so $\varepsilon := \alpha\beta^{-p}$ is a unit. For all $\mathfrak{p} \mid p$, $\alpha \in (K_\mathfrak{p})^p$ so $\varepsilon \in (K_\mathfrak{p})^p$. Since K is assumed without p-primary units and K has no p-th roots of unity, there exists $\eta \in K$ so that $\alpha\beta^{-p} = \eta^p$, so $\alpha \in K^p$. Hence K is p-rational. □

Lemma 2.2. *For any prime $p \geq 5$ not belonging to $\{\frac{1}{2}a^2 \pm 1 \mid a \in \mathbb{N}\}$ the real quadratic number field $K = \mathbb{Q}(\sqrt{p^2-1})$ is p-rational.*

Proof. First note that $\varepsilon = p + \sqrt{p^2-1}$ is a fundamental unit of K. Indeed, let ε_0 be the fundamental unit of K which is larger than 1 and let n be such that $\varepsilon = \varepsilon_0^n$. If n is even then $\eta := \varepsilon_0^{n/2}$ is such that $\varepsilon = \eta^2$. Then $N_{K/\mathbb{Q}}(\varepsilon) = N_{K/\mathbb{Q}}(\eta)^2 = 1$. Furthermore η^2 cancels the minimal polynomial of ε so η cancels $P(x) := x^4 - 2px^2 + 1 = 0$. Since η is a unit it's minimal polynomial is $\mu_\eta := x^2 - 2ax \pm 1 = 0$, where $a = \mathrm{Tr}(\eta)$. Since $\mu_\eta(x)$ divides $P(x)$ we obtain that $p = \frac{1}{2}a^2 \pm 1$, which contradicts the assumption on p. Therefore n is odd we have

$$(\varepsilon_0^n + \frac{1}{\varepsilon_0^n}) = \omega(\varepsilon_0 + \frac{1}{\varepsilon_0}),$$

where $\omega = \varepsilon_0^{n-1} + \varepsilon_0^{n-3} + \cdots + \frac{1}{\varepsilon_0^{n-3}} + \frac{1}{\varepsilon_0^{n-1}}$. Since $\varepsilon_0 \cdot (\varepsilon_0 - \mathrm{Tr}(\varepsilon_0)) = \pm 1$ we have $\omega \in \mathbb{Z}[\varepsilon_0]$. We also have $\omega = \mathrm{Tr}(\varepsilon)/\mathrm{Tr}(\varepsilon_0) \in \mathbb{Q}$ so ω belongs to $\mathbb{Q} \bigcap \mathbb{Z}[\varepsilon_0] = \mathbb{Z}$. Since $\mathrm{Tr}(\varepsilon) = 2p$ the only possibilities for μ_{ε_0} are $x^2 \pm 2px \pm 1$, $x^2 \pm px \pm 1$, $x^2 \pm 2x \pm 1$ and $x^2 \pm x \pm 1$. The discriminants of these polynomials cannot divide $p^2 - 1$ except for $x^2 \pm 2px \pm 1$, so $\varepsilon_0 \in \{\pm\varepsilon, \pm\frac{1}{\varepsilon_0}\}$. If ε_0 is chose such that it is larger than 1 then $\varepsilon_0 = \varepsilon$.

By a result of Louboutin [LOU98, Theorem 1] we have the effective bound

$$h(K) \leq \sqrt{\mathrm{Disc}(K)} \frac{e \log(\mathrm{Disc}(K))}{4 \log \varepsilon}.$$

Since $\mathrm{Disc}(K) \leq p^2 - 1$, we conclude that $h(K) < p$ and hence $p \nmid h(K)$.

Let us show that ε is not a p-primary unit. We have

$$\begin{aligned}\varepsilon^{p^2-1}-1 &\equiv (p^2-1)^{\frac{p^2-1}{2}}-1+p(p^2-1)^{\frac{p^2-3}{2}}\sqrt{p^2-1} \pmod{p^2\mathbb{Z}[\sqrt{p^2-1}]}\\ &\equiv \pm p\sqrt{p^2-1} \pmod{p^2\mathbb{Z}[\sqrt{p^2-1}]}.\end{aligned}$$

Since $p^2\mathbb{Z}[\sqrt{p^2-1}] \subset p^2\mathcal{O}_K$ this shows that the p-adic logarithm of ε is not a multiple of p^2, so ε is not p-primary. By Lemma 2.1 we conclude that K is p-rational. □

In the sequel the number fields K have no p-th roots of unity.

Lemma 2.3 ([Gre16] Prop 4.1.1(i))**.** *Let p be an odd prime and K a quadratic imaginary number field; if $p = 3$ we additionally assume that it is unramified. If $p \nmid h_K$ then K is p-rational.*

Proof. Case $p = 3$ unramified. The equation $\varphi(n) \leq 2$, where φ is Euler's totient function, has no odd solutions other than 3. If K contains the 3rd primitive root of unity ζ_3 then it also contains $\mathbb{Q}(\zeta_3)$ so 3 is ramified, hence the conditions in the hypothesis rule out the existence of 3rd roots of unity. After Lemma 2.1, K is 3-rational.

Case $p \geq 5$. Since K is imaginary, the unit rank is zero, so it contains no p-primary units. Lemma 2.1 allows to conclude that K is p-rational. □

Hartung proved what it takes to conclude $\mathrm{GC}_\infty(\mathbb{Z}/2\mathbb{Z}, p)$ for $p = 3$ and noted that his method works for any p:

Lemma 2.4 ([Har74])**.** *For any prime odd prime p there exist infinitely many square-free $D < 0$ such that $h_{\mathbb{Q}(\sqrt{D})} \cdot D \not\equiv 0 \pmod{p}$.*

Corollary 2.5. *For all odd prime p, $\mathrm{GC}_\infty(\mathbb{Z}/2\mathbb{Z}, p)$ holds.*

One can ask if it is possible to additionally impose in Problem 1.4 that K is totally real. Almost forty years after Hartung's work on imaginary fields, Byeon proved the corresponding result in the case of real fields.

Lemma 2.6 ([Bye01a] Prop. 3.3, [Bye01b] Thm. 1.1)**.** *For $p \geq 5$, there exists infinitely many integers $D > 0$ so that $h_{\mathbb{Q}(\sqrt{D})} \cdot D \not\equiv 0 \pmod{p}$ and $\mathbb{Q}(\sqrt{D})$ has no p-primary units.*

Corollary 2.7. *For all prime $p \geq 5$ there exist infinitely many real quadratic fields K which are p-rational.*

The study of p-rationality in general case of $G = (\mathbb{Z}/2\mathbb{Z})^t$ with $t \geq 1$ reduces to the case of quadratic fields as proven by a result of Greenberg.

Lemma 2.8. *(*[Gre16, Prop 3.6]*) Let $q \neq p$ be a prime, K be a number field such that its Galois group $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^t$. Then K is p-rational if and only if all the subfields of K of degree q is p-rational.*

We combine Lemmas 2.8 and 2.1 to obtain:

Proposition 2.9. Let K be a number field such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^t$ for some prime q and let $p \geq 5$ be a prime different from q. If for all cyclic subfields of K the class number is not divisible by p and has no p-primary units then K is p-rational.

p	t	$d_1, \ldots, d_t$
5	7	2,3,11,47,97,4691,-178290313
7	7	2,5,11,17,41,619,-816371
11	8	2,3,5,7,37,101,5501,-1193167
13	8	3,5,7,11,19,73,1097,-85279
17	8	2,3,5,11,13,37,277,-203
19	9	2,3,5,7,29,31,59,12461, -7663849
23	9	2,3,5,11,13,19,59,2803,-194377
29	9	2,3,5,7,13,17,59,293,-11
31	9	3,5,7,11,13,17,53,326,-8137
37	9	2,3,5,19,23,31,43,569,-523
41	9	2,3,5,11,13,17,19,241,-1
43	10	2,3,5,13,17,29,31,127,511,-2465249
47	10	2,3,5,7,11,13,17,113,349,-1777
53	10	2,3,5,7,11,13,17,73,181,-1213
59	10	2,3,5,11,13,17,31,257,1392,-185401
61	10	2,3,5,7,13,17,29,83,137, -24383
67	11	2,3,5,7,11,13,17,31,47,5011,-2131
71	10	2,3,5,11,13,17,19,59, 79,-943
73	10	2,3,5,7,13,17,23,37,61,-1
79	10	2,3,5,7,11,23,29,103,107,-1
83	10	2,3,5,7,11,13,17,43,97,-1
89	11	2,3,5,7,11,23,31,41,97,401,-425791
97	11	2,3,5,7,11,13,19,23,43,73,-1

TABLE 1. Examples of p-rational number fields of the form $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_t})$.

Remark 2.10. All over this article we assume that $p \nmid [K : \mathbb{Q}]$ because the p-rational extensions of $\mathbb{Q}$ of degree p are characterized in Example 3.5.1 of Section IV of [Gra13]: Assume L is a p-extension of $\mathbb{Q}$ which satisfies Leopoldt's conjecture at p. Then L is p-rational if and only if the following two conditions are satisfied:

(1) $L/\mathbb{Q}$ is unramified outside p,
(2) $L/\mathbb{Q}$ is unramified outside of $\{p, l\}$, where $l \neq p$ is prime and satisfies $p^2 \nmid (l^{p-1} - 1)$ if $p \geq 3$ or $8 \nmid (l \pm 1)$ if $p = 2$.

See *loc. cit.* for 2-rational abelian 2-extensions of $\mathbb{Q}$ and 3-rational abelian 3-extensions of $\mathbb{Q}$.

Example 2.11. For each prime between 5 and 97, Table 1 gives examples of fields K of the form $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_t})$ which are p-rational.

For each of these fields we applied Proposition 2.9 for which we verified that the $2^{t-1} - 1$ read quadratic subfields have class number non divisible by p and no p-primary units, and that the 2^{t-1} imaginary quadratic subfields have class number non divisible by p.

The examples were found using sage scripts available in the online complement [BR17] by testing the smallest possible value of $d_1 \geq 1$, and recursively for $i = 2, 3, \ldots, t-1$ we found the smallest possible value of $d_i \geq d_{i-1} + 1$ so that $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_i})$ is p-rational. Finally we selected d_t as the negative integer

of smallest absolute value such that the class numbers of all the imaginary real subfields of K are not divisible by p.

Note that $d_1, \ldots, d_{t-2}$ are relatively small showing that it was easy to find examples with small t. However there can be large gaps between d_{t-2} and d_{t-1} showing that this becomes much more difficult as t increases. We give an explanation for this observation in Remark 5.5. The value of $|d_t|$ is not very large showing that it was relatvely easy to go from a totally real to a totally complex example, as required by Greenberg's method to construct Galois representations with open image (cf. discussion before Conjecture 1.3, see also Prop 6.7 and Prop 6.1 of [Gre16]). The search of the negative determinant d_t is fast also due to the Hurwitz-Eichler theorem which to compute recursively class numbers of imaginary quadratic fields [Coh13, Section 5.3.2].

Greenberg and Pollack [Gre16, Sec 4.2, page 99] gave the examples of the fields $\mathbb{Q}(\sqrt{13}, \sqrt{145}, \sqrt{209}, \sqrt{269}, \sqrt{373}, \sqrt{-1})$, which is 3-rational, and of the 5-rational field $\mathbb{Q}(\sqrt{6}, \sqrt{11}, \sqrt{14}, \sqrt{59}, \sqrt{-1})$, for which $t = 5$ is smaller that that of the example on the first row of Table 1.

In order to investigate the existence of p-rational fields it is necessary to discuss the density of fields whose class number is divisible by p.

2.2. **Density of fields where $p \mid h$: the Cohen-Lenstra heuristic.** Cohen and Lenstra [CL84b, CL84a] created a heuristic principle which can be used to derive conjectures on the density of class numbers divisible by a given integer. We say that a set $\mathcal{S}$ of number fields has a density δ and write $\mathrm{Prob}(\mathcal{S}) = \delta$ if

$$\lim_{X \to \infty} \frac{\#\{K \in \mathcal{S} \mid \mathrm{Disc}(K) \leq X\}}{\#\{K \mid \mathrm{Disc}(K) \leq X\}} = \delta.$$

Here $\#\{K \mid \mathrm{Disc}(K) \leq X\}$ denotes the number of fields with discriminant less than or equal to X For simplicity we write Prob(property) to designate the density of the set of number fields satisfying the property. Cohen and Lenstra studied the case of quadratic fields, Cohen and Martinet [CM90, CM87] studied the case of fields K of degree 3 and 4, not necessarily cyclic, while more recently Miller [Mil15, Sec 3] studied the case of cyclic extensions:

Conjecture 2.12 ([Mil15] Sec 3)**.** *Let K be a cyclic extension of $\mathbb{Q}$ of odd prime degree q and p a prime not dividing q. Then* $\mathrm{Prob}(p \nmid h_K) = \prod_{k \geq 2}(1 - p^{-k\omega})^{\frac{q-1}{\omega}}$ *where ω is the multiplicative order of p modulo q.*

In the particular case of cubic cyclic fields this conjecture corroborates with the conjecture of Cohen and Martinet:

Conjecture 2.13 ([CM87] Sec 2, Ex 2(b))**.** *Let K be a cyclic cubic number fields and m an integer non divisible by 3. Then we have*

$$\mathrm{Prob}(m \mid h_K) = \prod_{p \mid m, p \equiv 1 \mod 3} \Big(1 - \frac{(p)_\infty^2}{(p)_1^2}\Big) \prod_{p \mid m, p \equiv 2 \mod 3} \Big(1 - \frac{(p^2)_\infty}{(p^2)_1}\Big),$$

where $(p)_\infty = \prod_{k \geq 1}(1 - p^{-k})$ and $(p)_1 = (1 - p^{-1})$.

For an overview on recent progress on the Cohen-Lenstra-Martinet heuristic we refer the reader to a series of recorded lectures of Fouvry [Fou14].

2.3. **Density of fields with p-primary units : valuation of p-adic regulator.** The condition about p-primary units in Lemma 2.1 can be stated in a simpler manner when K is totally real.

Definition 2.14. Let K be a totally real Galois number field and p a prime which is unramified in K. Let $\varepsilon_1, \dots, \varepsilon_r$ be a system of fundamental units and $\sigma_1, \dots, \sigma_{r+1}$ the automorphisms of K. Let $\mathfrak{p}$ be a prime ideal above p and $\log_{\mathfrak{p}}$ the $\mathfrak{p}$-adic logarithm of $K_{\mathfrak{p}}$, $\log_{\mathfrak{p}}(x+1) = \sum_{i\geq 1}(-1)^i \frac{x^i}{i}$. Call $\mathcal{O}_{\mathfrak{p}}$ the ring of integers in $K_{\mathfrak{p}}$. We set $E = \mathrm{lcm}(\{N(\mathfrak{p}')-1, \mathfrak{p}' \mid p\})$ where $N(\mathfrak{p})$ is the norm of $\mathfrak{p}$. By abuse of notations we also denote by $\log_{\mathfrak{p}}$ the following map that we only apply to elements of E_K:

$$\begin{array}{rccc} \log_{\mathfrak{p}} : & \{x \in K^* \mid \ \forall \mathfrak{p}' \mid p, \mathrm{val}_{\mathfrak{p}'}(x) = 0\} & \to & 1+\mathfrak{p}\mathcal{O}_{\mathfrak{p}} \\ & x & \mapsto & \log_{\mathfrak{p}}(x^E). \end{array}$$

We call normalized p-adic regulator the quantity $R_p = \det(\frac{1}{p}\log_{\mathfrak{p}}(\sigma_j(\varepsilon_j)_{1\leq i,j\leq r}))$.

It is classical (see for example [Was97]) that R_p belongs to $\mathbb{Z}_p$ and is independent of the choice of $\mathfrak{p}$ and of the labeling of fundamental units and of the automorphisms. For completion we state a simple and classical property of $R_{K,p}$.

Lemma 2.15. *For all $\gamma \in K$, if K has a p-primary unit then R_p is divisible by p.*

Proof. Let $\varepsilon = \prod_{i=1}^r \varepsilon_i^{a_i}$, $a_1, \dots, a_r \in \mathbb{Z}$ be a p-primary unit. Then $(a_1, \dots, a_r)$ is in the kernel of the matrix which defined $R_{K,p}$ reduced modulo $\mathfrak{p}$. Hence $R_{K,p}$ is divisible by $\mathfrak{p}$ and, since it belongs to $\mathbb{Z}_p$, it is also divisible by p. □

Very little is known on the probability that the normalized regulator is divisible by p. Schirokauer [Sch93, p. 415] made the heuristic that the matrix which defines $R_{K,p}$ modulo p is a random matrix with coefficients in $\mathbb{F}_{p^f}$ for some f and therefore the probability that p divides $R_{K,p}$ is $\mathcal{O}(\frac{1}{p})$. Later Hofman and Zhang studied the case of cyclic cubic fields and gave heuristic arguments and numerical experiments in favor of the following conjecture.

Conjecture 2.16 ([HZ16] Conj 1)**.** *For primes $p > 3$ we have*

$$\mathrm{Prob}(p \textit{ divides } R_{K,p}) = \begin{cases} \frac{1}{p^2}, & \textit{if } p \equiv 2 \pmod 3 \\ \frac{2}{p} - \frac{1}{p^2}, & \textit{if } p \equiv 1 \pmod 3. \end{cases}$$

3. Algorithmic tools

complete information	class group	unit group	ray group
partial information	p divides h_K	p divides $R_{K,p}$	K is p-rational

Table 2. List of invariants associated to a number field K and of partial information associated to a prime p.

Gathering numerical data on the class group, unit group and respectively ray class group of number fields is a hard task despite the important progress done in the design of algorithms. Indeed, the best algorithms to compute class number

are derived from Buchman's algorithm [BW89] and have a non-polynomial complexity. In the context of the Cohen-Lenstra-Martinet heuristic it is not necessary to compute h_K but only to test its divisibility by p. In Section 3.2 we recall an algorithm of polynomial complexity which tests the divisibility of h_K by p without other information on h_K. Similar questions can be studied for the unit and ray class groups.

In the context of the p-adic regulator valuation it is not necessary to compute the regulator to infinite precision, but only to test the divisibility of the normalized p-adic regulator by p. When using the best known algorithms there is no gain in complexity when the precision is reduced because one needs to compute a system of fundamental units, which is done by a variant of Buchman's class number algorithm [BW89]. This motivates us in Section 3.3 to propose a fast method to compute units, which are not necessarily a basis of the unit group but which allow us in general to test the divisibility by p of the normalized p-adic regulator.

Ray class group is related to the cartesian product of the class number and the unit group and from an algorithmic view point, it is similar to these two groups, and it is not surprising that the algorithm of Cohen et al. [CDO98] has a non-polynomial complexity. Pitoun and Varescon [PV15] showed that it allows to test if K is p-rational by an algorithm that we recall in Section 3.4.

3.1. **An algorithm to enumerate abelian number fields.** Numerical computations of densities require to make the list of all the number fields K of a given degree and Galois group such that $|\mathrm{Disc}(K)|$ is less than a given bound X. The task is very much simplified in the case of abelian extensions due the following classical result.

Lemma 3.1 ([Was97] Thm 3.11,The Conductor-discriminant formula)**.** *Let K be an abelian number field and let Ξ be the group of characters $\mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{C}^*$. Then we have*

$$\mathrm{Disc}(K) = (-1)^{r_2} \prod_{\chi \in \Xi} c_\chi,$$

where c_χ is the conductor of χ.

In particular if $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^t$, where q is a prime number, we have a very simple relation between the conductor and the discriminant. Although the result is classical (see for example [Gra75]) we recall the proof because one deduces from it an algorithm to enumerate number fields with Galois group equal to $(\mathbb{Z}/q\mathbb{Z})^t$ and discriminant bounded by a given constant.

Lemma 3.2. *Let K be a number field such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^t$. Then we have,*

1. *the conductor c_K of K can be written as $c_K = p_1 \cdots p_s$ or $c_K = q^2 p_1 \cdots p_{s-1}$ where $p_i \equiv 1 \mod q$ are distinct primes;*
2. $\mathrm{Disc}(K) = c_K^{(q-1)q^{s-1}}$.

Proof. (1) For any abelian group G we call q-rank of G, denoted by $\mathrm{rank}_q G$, the dimension of the $\mathbb{F}_q$ vector space G/G^q. Then one easily checks that for any prime $p_i \not\equiv 1 \mod q$ different than q, $\mathrm{rank}_q(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^* = 0$; for any prime $p_i \equiv 1 \pmod q$ and any $e_i \geq 1$, $\mathrm{rank}_q(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^* = \mathrm{rank}_q(\mathbb{Z}/p_i\mathbb{Z})^*$. Hence $\mathrm{rank}_q(\mathbb{Z}/q\mathbb{Z})^* = 0$ and for any $e \geq 2$, $\mathrm{rank}_q(\mathbb{Z}/q^e\mathbb{Z})^* = 1$. If c is an integer of the form in point (1) and c' is a multiple of c then $(\mathbb{Z}/c\mathbb{Z})^*$ and $(\mathbb{Z}/c'\mathbb{Z})^*$ have the same q-rank. By definition,

the conductor of a number field of Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ is the smallest integer c so that the q-rank of $(\mathbb{Z}/c\mathbb{Z})^*$ is t.

(2) For each prime power a dividing c_K we have to count the number of characters defined on $(\mathbb{Z}/c_K\mathbb{Z})^*$ which are not trivial on $(\mathbb{Z}/a\mathbb{Z})^*$. This is the number of subgroups of $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^t$ whose quotient group is $\mathbb{Z}/q\mathbb{Z}$ and further the number of linear forms from $\mathbb{F}_q^t$ to $\mathbb{F}_q$ which are non-zero on the first component, hence the total number is $(q-1)q^{t-1}$. Due to the conductor-discriminant formula (Lemma 3.1) we obtain the result for $\mathrm{Disc}(K)$. □

In numerical experiments, we enumerate all fields K of Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ with $|\mathrm{Disc}(K)| \leq X$ by enumerating all positive integers c less than $X^{\frac{1}{q^{t-1}(q-1)}}$ of the form given by point (1) of Lemma 3.2. Next we compute all subgroups H of $(\mathbb{Z}/c\mathbb{Z})^*$ such that $(\mathbb{Z}/c\mathbb{Z})^*/H \simeq (\mathbb{Z}/q\mathbb{Z})^t$. Finally we compute the fixed field of H.

In the particular case of cubic cyclic fields one does not need any computations because there exists a canonical polynomial to define every cyclic cubic number fields of conductor m.

Lemma 3.3 ([Coh13] Thm 6.4.6)**.** *Let m be an integer of the form $\prod_{i=1}^t p_i$ or $9\prod_{i=1}^{t-1} p_i$ where $p_i \equiv 1 \pmod 3$. Then there are 2^{t-1} cubic cyclic fields of conductor m. Each of them corresponds to one solution of the equation $m = \frac{a^2+27b^2}{4}$ by the formula*

$$f_a(x) = \begin{cases} x^3 + x^2 + \frac{1-m}{3}x - \frac{m(3+a)-1}{27}, & \text{if } 3 \nmid a \\ x^3 - \frac{m}{3}x - \frac{am}{27}, & \text{otherwise.} \end{cases} \tag{3.1}$$

The subfamily $m = \frac{a^2+27}{4}$ has a pleasant property that deserves our attention.

3.1.1. *A family with explicit units.* For a particular classical family of cubic cyclic fields we have a closed formula of the minimal polynomial of a unit of infinite order. We focus on the existence of the unit, which is not necessarily well explained in the literature.

Lemma 3.4. *Let a be an odd integer, $m = \frac{1}{4}(a^2+27)$ and let K be the number field defined by Equation* (3.1)*. Then K contains an integer ω whose minimal polynomial is*

$$g_a(x) = x^3 - mx^2 + 2mx - m$$

and $\eta := \sigma(\omega)/\omega$ is a unit whose minimal polynomial is

$$\mu_a(x) = x^3 - \frac{2m-3-a}{2}x^2 + \frac{2m-3+a}{2}x - 1,$$

where $\mathrm{Gal}(K/\mathbb{Q})$ is generated by the automorphism σ. Additionally, K contains a unit whose minimal polynomial is

$$\nu_a(x) = x^3 + (m-3)x^2 + 3x - 1.$$

Proof. Let α be a root of f_a in K. One can plug in g_a the element

$$\omega = \begin{cases} \frac{a^2}{36} + \frac{\alpha a}{3} + \alpha^2 + \frac{3}{4}, & \text{if } 3 \nmid a \\ \frac{a^2}{36} + \frac{a\alpha}{3} + \alpha^2 + \frac{a}{9} + \frac{2}{3}\alpha + \frac{31}{36}, & \text{otherwise.} \end{cases}$$

and note that $g_a(\omega) = 0$, so g_a has a root in K for any a. We set $\eta = \frac{\sigma(\omega)}{\omega}$ and, for $i \in \mathbb{N}$, $\omega_i = \sigma^i(\omega)$. Let $x^3 - Ax^2 + Bx - 1$ be the minimal polynomial of η over $\mathbb{Q}$. Then, equating $x^3 - Ax^2 + Bx - 1 = (x - \eta)(x - \sigma(\eta))(x - \sigma^2(\eta))$, we obtain

$$\begin{aligned} A + B &= \sum_{i=0}^{2} \frac{\omega_{i+1}}{\omega_i} + \frac{\omega_i}{\omega_{i+1}} = \frac{1}{m}(\sum_{i=0}^{2} \omega_{i+1}^2\omega_i + \omega_{i+1}\omega_i^2) \\ &= \frac{1}{m}\left((\sum_{i=0}^{2} \omega_i\omega_{i+1})(\sum_{i=0}^{2} \omega_i) - 3\prod_{i=0}^{2} \omega_i\right) = 2m - 3. \end{aligned}$$

Note that $g_a(x)$ is the minimal polynomial of ω which links m with ω_i's giving us the second equality above. We also have

$$AB = (\sum_{i=0}^{2} \frac{\omega_{i+1}}{\omega_i})(\sum_{i=0}^{2} \frac{\omega_i}{\omega_{i+1}}) = m^2 - 4m + 9.$$

Hence A and B are such that the minimal polynomial of $\eta = \sigma(\omega)/\omega$ is μ_a.

Finally, we test by direct computations that ν_a has a root

$$\eta' = \begin{cases} \alpha^2 + \frac{a-1}{3}\alpha + \frac{a^2}{36} - \frac{a}{18} + \frac{1}{36}, & \text{if } 3 \nmid a \\ \alpha^2 + \frac{(a-3)\alpha}{3} + \frac{a^2}{36} - \frac{a}{6} + \frac{1}{4}, & \text{otherwise.} \end{cases}$$

which is automatically a unit in K. □

The computations in the proof can be found in the online complement [BR17].

3.2. **An algorithm to test if p divides h_K.** Marie-Nicole Gras [Gra75] designed an algorithm which allows to test if h_K is divisible by p without computing h_K.

Definition 3.5. Let K be an abelian number field. We call cyclotomic units of Leopoldt the set C_K of units of K which are of the form $\pm\eta_a := N_{\mathbb{Q}(\zeta_c)/K}(\frac{\zeta_c^a - 1}{\zeta_c - 1})$ where c is the conductor of K and a runs through all elements of $\mathbb{Z}/c\mathbb{Z}$.

The main ingredient of Gras' algorithm is a result due to Leopoldt:

Lemma 3.6 ([GG77] section III 3)**.** *Let K be a cyclic number field of odd prime degree. Then*

$$h_K = [E_K : C_K],$$

where C_K is the group of cyclotomic units of Leopoldt.

For every a in $(\mathbb{Z}/c\mathbb{Z})^*$ we denote by σ_a the automorphism of $\mathbb{Q}(\zeta_c)$ given by $\zeta_c \mapsto \zeta_c^a$. One starts the algorithm by computing η_a for every a in a system of representatives of

$$(\mathbb{Z}/c\mathbb{Z})^*/\{a \in (\mathbb{Z}/c\mathbb{Z})^* \mid \sigma_{a|K} = id\},$$

where id is the identity map. Then one tests if one can form a product of η_a's which is an p-th power. This step was improved to take a polynomial time instead of exponential. Indeed, the following result is attributed by Hakkarainen to van der Linden and replaces a product of an exponential number of terms to a power elevation, which can be done by a fast exponentiation algorithm.

Lemma 3.7 ([Hak09] Eq (5.1))**.** *Let K be a cyclic number field of degree n and conductor m. Let p and q be two primes and let f be the order of q modulo p. Let $\mathfrak{q}$ be a prime ideal of $\mathbb{Q}(\zeta_m)$ above of q and let $\rho_{\mathfrak{q}} : \mathbb{Z}[\zeta_m] \to k_{\mathfrak{q}}$ be the canonical projection on $k_{\mathfrak{q}} = \mathbb{Z}[\zeta_m]/\mathfrak{q}$ which is the residual field of $\mathfrak{q}$. Then for any $\gamma \in \mathbb{Z}[\zeta_m]$ we have*

$$\rho_{\mathfrak{q}}(N_{\mathbb{Q}(\zeta_m)/K}(\gamma)) = \rho_{\mathfrak{q}}(\gamma)^{\frac{\varphi(m)}{nf}\frac{q^f-1}{p}}.$$

Consequently, if there exists $\mathfrak{q}$ such that $\rho_{\mathfrak{q}}(\gamma)^{\frac{\varphi(m)}{nf}\frac{(q^f-1)^2}{p(q-1)}} \neq 1$ then γ is not a p-th power in K.

Proof. Recall that the morphism

$$\begin{array}{rccc} \_: & \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) & \to & \mathrm{Gal}(k_{\mathfrak{q}}/\mathbb{F}_q) \\ & \tau & \mapsto & \overline{\tau}, \end{array}$$

where $\forall a \in k_{\mathfrak{q}}, \overline{\tau}(a) = \rho_{\mathfrak{q}}(\tau(\gamma))$ where γ is a lift of a in $\mathbb{Q}(\zeta_m)$, is surjective. Hence, for all $i = 0, \ldots, f-1$, $\#\{\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K) \mid \overline{\tau}(\rho_{\mathfrak{q}}(\gamma)) = \rho_{\mathfrak{q}}(\gamma)^{q^i}\} = \frac{\varphi(m)}{nf}$.

We have then

$$\rho_{\mathfrak{q}}(N_{\mathbb{Q}(\zeta_m)/K}(\gamma)) = \prod_{\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K)} \overline{\tau}(\rho_{\mathfrak{q}}(\gamma)) = \Big(\prod_{i=0}^{f-1} \rho_{\mathfrak{q}}(\gamma)^{q^i}\Big)^{\frac{\varphi(m)}{nf}} = \rho_{\mathfrak{q}}(\gamma)^{\frac{q^f-1}{q-1}\frac{\varphi(m)}{nf}}.$$

Consequently, since $k_{\mathfrak{q}}^*$ is cyclic, an element is a p-th power if and only if its $(\#k_{\mathfrak{q}} - 1)/p$ power is 1. This completes the proof because $\#k_{\mathfrak{q}} = q^f$. □

The Gras-van der Linden algorithm, that we recall in Algorithm 1, consists in trying various primes q and in applying Lemma 3.7. The implementation of SAGE code for Algorithm 1 is in Appendix B, and can be downloaded from the online complement [BR17].

Algorithm 1 Gras-van der Linden

Require: an integer N and a cyclic cubic number field K given by a conductor m and an element g of $(\mathbb{Z}/m\mathbb{Z})^*$ such that $\zeta_m \mapsto \zeta_m^g$ doesn't fix K

Ensure: The algorithm returns 'false', if $q \nmid h_K$
The algorithm returns 'non-certified true', if $q \mid h_K$.

$i \leftarrow 0$
repeat
  $q \leftarrow$ next prime congruent to 1 mod p,
  we increment i and continue
until i>N or the polynomial $\frac{x^g-1}{x-1}^{\frac{\varphi(m)}{3}\frac{q-1}{p}} \not\equiv 1 \mod \langle q, f(x)\rangle$

3.3. **An algorithm to test if p divides the normalised p-adic regulator.** The relevant notion in this section is the p-adic logarithm but for computational issues we focus on a truncation of it that deserves its own name.

Definition 3.8 ([Sch93], Sec 3.)**.** Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial and let p be a prime which does not divide the index of f, i.e. $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ where

$\mathcal{O}_K$ is the ring of integers in the number field K of f and α is a root of f in its number field. The Schirokauer map associated to f and p is

$$\begin{array}{rccc} \lambda_{f,p}: & \{\frac{a_1(x)}{a_2(x)} \mid a_1, a_2 \in \mathbb{Z}[x], p \nmid \mathrm{Res}(a_1 a_2, f)\} & \to & \mathbb{F}_p[x]/\langle f(x)\rangle \simeq \mathbb{F}_p^{\deg f} \\ & a_1/a_2 \in \mathbb{Q}(x) & \mapsto & \frac{(a_1^{p^e-1}-1)-(a_2^{p^e-1}-1)}{p} \mod \langle p, f\rangle, \end{array}$$

where $e = \mathrm{lcm}(\{\deg f_i \mid f_i \text{ divides } f \text{ in } \mathbb{F}_p[x]\}$ and Res denotes the resultant.

Also note that we can identify $\mathbb{Q}[x]/\langle f(x)\rangle$ and K so that every element of K is represented by a polynomial. In this language the condition $p \nmid \mathrm{Res}(a_1 a_2, f)$ states that $\forall \mathfrak{p} \mid p$, $\mathrm{val}_{\mathfrak{p}}(\frac{a_1}{a_2}) = 0$.

When p is non-ramified $R'_{K,p}$ is not divisible by p if and only if the matrix formed with $\lambda_{f,p}(\varepsilon_1) \ldots, \lambda_{f,p}(\varepsilon_r)$ has full rank. This implies that the result of the computations is independent on the choice of f.

The remaining question is that of computing a system of generators for E_K/E_K^p. In the case of the family of Section 3.1.1, this is easily done using an explicit formula. However in the general case of cyclic cubic fields we propose a new technique.

Lemma 3.9. *Let K be a number field of odd prime degree q and of cyclic Galois group and call m its conductor. Then we have:*

1. *for any prime factor ℓ of m there exists an ideal $\mathfrak{l}$ so that $\mathfrak{l}^q = \ell\mathcal{O}_K$;*
2. *If $\mathfrak{l}$ is principal, for any generator $\omega \in \mathcal{O}_K$ of $\mathfrak{l}$ and any generator σ of $\mathrm{Gal}(K/\mathbb{Q})$, $\frac{\sigma(\omega)}{\omega}$ is a unit.*

Proof. (i) Let ℓ be a prime factor of m other than q. Then ℓ is ramified in K and, since $\deg K = q$ is prime, there exists a prime ideal $\mathfrak{l}$ so that $\ell = \mathfrak{l}^q$.

(ii) The ideal generated by $\frac{\sigma(\omega)}{\omega}$ is $\sigma(\mathfrak{l})\mathfrak{l}^{-1}$. Since σ induces an automorphism on K, $\sigma(\mathfrak{l})$ is a prime ideal above ℓ. But ℓ is totally ramified in K so $\sigma(\mathfrak{l}) = \mathfrak{l}$. So $\frac{\sigma(\omega)}{\omega}$ is a unit. □

Remark 3.10. The ideal $\mathfrak{l}$ is not necessarily principal and even if it is, the computation of a generator ω is not fast in the worst case. Indeed, since $\ell\mathbb{Z}[\zeta_\ell] = ((\zeta_\ell - 1)\mathbb{Z}[\zeta_\ell])^{(\ell-1)}$, $\ell\mathbb{Z}[\zeta_m] = ((\zeta_\ell - 1)\mathbb{Z}[\zeta_m])^{(\ell-1)}$ so that in $\mathbb{Z}[\zeta_m]$ we have

$$\mathfrak{l}^q = \langle \zeta_\ell - 1\rangle^{\ell-1}.$$

By unique factorization we deduce that $\mathfrak{l}\mathbb{Z}[\zeta_m] = \langle \zeta_m - 1\rangle^{\frac{\ell-1}{q}}$. We consider the norms and obtain that $N_{\mathbb{Q}(\zeta_m)/K}(\mathfrak{l}\mathbb{Z}[\zeta_m]) = \langle N_{\mathbb{Q}(\zeta_m)/K}(\zeta_\ell - 1)^{\frac{\ell-1}{q}}\rangle$ is principal, but this is not necessarily equal to $\mathfrak{l}$.

Among the 2217 cyclic cubic number fields with conductor between 7 and 10000 we have:

$\mathfrak{l}$ is principal and Algorithm 2 succeeds	1237	55.8%	$x^3 + x^2 - 2x - 1$
Algorithm 2 succeeds but $\mathfrak{l}$ is not principal	258	11.64%	$x^3 - 21x^2 + 35$
$\mathfrak{l}$ is principal but Algorithm 2 fails	402	18.13%	$x^3 - x^2 - 30x - 27$.

Here we write that $\mathfrak{l}$ is principal when there exists a prime ℓ above the conductor m of the number field of f such that $\mathfrak{l}$ is principal. The case in which $\mathfrak{l}$ is principal and Algorithm 2 fails is due to the usage of the LLL algorithm [LLL82]. Indeed, given a lattice L of dimension n the algorithm finds in polynomial time an element

of the lattice whose euclidean norm is less than $c_n|\det(L)|^{\frac{1}{n}}$. If $\omega_1, \dots, \omega_n$ is an integer basis of $\mathcal{O}_K$ and LLL is applied to the lattice

$$L = \{(a_0, \dots, a_{n-1}) \in \mathbb{Z}^n \mid \sum_{i=0}^{n} a_i\omega_i \in \mathfrak{l}\}$$

computes an element $(\gamma_0, \dots, \gamma_n) \in \mathbb{Z}^n$ such that $\gamma = \sum_{i=0}^{n} \gamma_i\omega_i$ is such that $N_{K,\mathbb{Q}}(\gamma) \leq CN(\mathfrak{l})$ for some constant C independent on $\mathfrak{l}$. Since $C > 1$, it is not always true that LLL finds a generator. Generic algorithms to replace LLL exist but they are much slower.

In the following we present Algorithm 2 which is used for fast computation of a unit in cyclic cubic fields. The implementation using SAGE is in Appendix C, and the program can be downloaded from the online complement [BR17].

Algorithm 2 Fast computation of a unit of cyclic cubic K.

Require: a cubic cyclic field K and a factorization of its conductor m
Ensure: a unit of K
1: **for** $\ell \equiv 1 \mod q$ factor of m **do**
2: factor ℓ in $\mathcal{O}_K$ to obtain $\mathfrak{l}$ using [Coh13, Sec 4.8.2]
3: search a generator ω_ℓ of the ideal $\mathfrak{l}$ using LLL [LLL82].
4: **end for**
5: **return** a product of the units $\eta_\ell := \sigma(\omega_\ell)/\omega_\ell$

In order to do statistics about the p-adic regulator we proceed as in Algorithm 3. The implementation of SAGE code for the Algorithm is in Appendix D, and the program can be downloaded from the online complement [BR17]. Note that Schirokauer's map $\lambda_{f,p}$ (Definition 3.8) has image in the $\mathbb{F}_p$-vector space $\mathbb{F}_p[x]/\langle f(x)\rangle$ which has the basis $(1, x, x^2)$ when f is cubic. Hence we call λ_0, λ_1, λ_2 the components of $\lambda_{f,p}$ corresponding to the projections on the line of 1, x and respectively x^2.

3.4. **An algorithm to decide p-rationality.** For any n let $\mathcal{A}_{p^n}$ denote the p-part of the ray class group ([Gra13] Ch I.4) of K with respect to the ideal p^n. For any finite abelian group G we denote by $FI(G)$ the invariant factors of G i.e. the integers $[d_1, \dots, d_k]$ so that $G \simeq \oplus_{i=1}^{k} \mathbb{Z}/d_i\mathbb{Z}$ and $d_1 \mid d_2 \mid \cdots \mid d_k$. The following result reduces the problem of testing p-rationality to that of computing the ray class group, which is studied for example in [CDO98] and implemented in PARI [BBB+98].

Lemma 3.11 ([PV15] Thm 3.7 and Cor 4.1, see also Prop. 1.13 of [HM16])**.** *Let K be a number field which satisfies Leopoldt's conjecture. Let e be the ramification index of p in K. Then there exists $n \geq 2+e$ so that the invariant factors of $FI(\mathcal{A}_{p^n})$ can be divided into two sets $FI(\mathcal{A}_{p^n}) = [b_1, \dots, b_s, a_1, \dots, a_{r_2+1}]$ such that*

(1) $\min(\mathrm{val}_p(a_i)) > \max(\mathrm{val}_p(b_i)) + 1$;
(2) $FI(\mathcal{A}_{p^{n+1}}) = [b_1, \dots, b_s, pa_1, \dots, pa_{r_2+1}]$.

Moreover, K is p-rational if and only if $\mathrm{val}_p(b_1) = \mathrm{val}_p(b_2) = \cdots = \mathrm{val}_p(b_s) = 0$.

The algorithm of Pitoun and Varescon was implemented in PARI [BBB+98] by Bill Allombert on a large number of imaginary quadratic fields. The algorithm applies to all number fields satisfying Leopoldt's conjecture not only to abelian

Algorithm 3 Test if $p \mid R'_{K,p}$ for a list of random cyclic cubic fields

Require: a list of cyclic cubic fields
Ensure: a certificate on the divisibility of $R'_{K,p}$ by p
for K in list of cyclic cubic fields **do**
Apply Algorithm 2 to compute a unit η
Apply algorithms in [WR76] to factor a defining polynomial of K in $K[x]$ and obtain a non-trivial automorphism σ of K
Compute the rank r of the matrix

$$\begin{pmatrix} \lambda_0(\varepsilon_1) & \lambda_1(\varepsilon_1) & \lambda_2(\varepsilon_1) \\ \lambda_0(\varepsilon_2) & \lambda_1(\varepsilon_2) & \lambda_2(\varepsilon_2) \end{pmatrix},$$

where $\lambda_0, \lambda_1, \lambda_2$ are the Schirokauer maps of a polynomial defining K
if r=2 **then**
return $p \nmid R_{K,p}$
else
we compute a truncation of the normalized p-adic regulator using algorithms in [Pan95] and return the result of the test whether this rank is 2
end if
end for

fields. Indeed, the problem is not the answer which is always correct, but the fact that the algorithm doen't terminate when Leopoldt's conjecture doesn't hold for K. To illustrate that the algorithm works also for non-abelian number fields we construct examples of p-rational fields for all possible Galois groups of quartic polynomials.

Example 3.12. In Table 3.12 we list the set of primes less than 100 where the number fields of the listed polynomials are not p-rational. The case for the polynomial $x^4 + x^3 + x^2 + x + 1$ is already discussed by Greenberg [Gre16, Sec. 4.4], thanks to the computations of Robert Pollack. The SAGE code for the programme to verify p-rationality using Lemma 3.11 is in Appendix A, and the programme can be downloaded fromthe online complement [BR17].

Galois group	$\forall p \leq 100,\ p-$ rational	non 7-rational
$\mathbb{Z}/4\mathbb{Z}$	$x^4 + x^3 + x^2 + x + 1$	$x^4 - 23x^3 - 6x^2 + 23x + 1$
V_4	$x^4 - x^2 + 1$	$x^4 + 10x^2 + 1$
D_4	$x^4 - 3$	$x^4 - 6$
A_4	$x^4 + 8x + 12$	$x^4 - x^3 - 16x^2 - 7x + 27$
S_4	$x^4 + x + 1$	$x^4 + 35x + 1$

TABLE 3. p-rationality of a list of number fields.

To sum up we have a fast criterion for p-rationality given by Proposition 2.9 and a slow condition which works in the general case which is given by Lemma 3.11. For efficiency reasons we implemented a combination of the two as given by Algorithm 4. An implementation of this algorithm is available in the online complement [BR17].

Algorithm 4 test p-rationality of a list of cyclic cubic fields

Require: a prime p and a list of cyclic cubic fields
Ensure: for each number field the information whether it is p-rationality
for K in list of cyclic cubic fields **do**
Apply Algorithm 1 to certify that p does divides h_K when it is possible
Apply Algorithm 3 to certify that p does not divides $R'_{K,p}$ when it is possible
if we have certificates that $p \nmid h_K R'_{K,p}$ **then**
return True and certificates
else
Apply the algorithm of Pitoun and Varescon in Appendix A, based on Lemma 3.11 to decide if K is p-rational
Return answer and certificate
end if
end for

In an experiment, using Algorithm 4, we tested p-rationality the 158542 cyclic cubic fields of conductor less than 10^6. The proportion of fields where $5 \mid h_K$ is expected to be $0,000016$ (Conjecture 2.13) and the proportion of fields where $5 \mid R'_{K,5}$ is expected to be 0.04 (Conjecture 2.16), which is matched very well by the experiments: 5351 fields found for an expected number of $0.04 \cdot 158542 \approx 6127$. It turns out that in all the 5351 cases where we couldn't apply the criterion in Lemma 2.1 the field was actually non 5-rational. The data can be found in the online complement [BR17]. The total time used by the 153191 number fields where the fast criterion could be applied was negligible with respect to the total time used for the 5351 number fields where the algorithm of Pitoun and Varescon was applied. Hence we had a speed-up of approximatively $158542/5351 \approx 5^2$. In the general case, for a prime p, we expect a speed-up of $p/2$ when $p \equiv 1 \pmod 3$ and of p^2 when $p \equiv 2 \pmod 3$.

4. Some families of p-rational fields

Recall that, when given a cyclic cubic field K, in Algorithm 1 one searches for a prime q where Lemma 3.7 applies, and hence certifies that the class number is not divisible by p. The idea of this section is to fix $q = 11$ and to search for cyclic cubic fields where Lemma 3.7 applies for $p = 5$. Under some arithmetic assumptions this allows to construct an infinite family of fields of class number non-divisible by 5. We can also find a family of number fields where the 5-adic regulator is not divisible by 5 thanks to the explicit formula in Section 3.1.1. Under the assumption that the two families intersect we obtain an infinite family of 5-rational cyclic cubic fields.

Lemma 4.1. *Let m be a prime such that $3 \mid \varphi(m)$, $11 \nmid \varphi(m)$ and Φ_m is irreducible modulo 11. Then the number field of f_a defined in Equation (3.1) has class number not divisible by 5.*

Proof. Let $\eta := N_{\mathbb{Q}(\zeta_m)/K}(\frac{\zeta_m^2-1}{\zeta_m-1})$ be a unit not necessarily cyclotomic. By Lemma 3.6 the class number cannot be divisible by 5 if η is not a 5th power. We will prove that $\rho_{\mathfrak{q}}(\eta)^2 \neq 1$, which shows that $\rho_{\mathfrak{q}}(\eta)$ is not a 5th power and therefore η is not a 5th power.

We apply Lemma 3.7 to $\gamma = \frac{\zeta_m^2-1}{\zeta_m-1}$, $n = 3$, $p = 5$ and $q = 11$, so $\rho_{\mathfrak{q}}(\eta) = (\rho_{\mathfrak{q}}(\zeta_m)+1)^{\frac{2\varphi(m)}{3}}$. We have to test if $\rho_{\mathfrak{q}}(\eta) = \pm 1$. Since 11 is a generator of $(\mathbb{Z}/m\mathbb{Z})^*$, Φ_m is irreducible modulo 11, so $\rho_{\mathfrak{q}}(\zeta_m+1) = (x+1) \pmod{\Phi_m}$ where Φ_m is seen as an irreducible polynomial in $\mathbb{F}_{11}[x]$. The finite field $\mathbb{F}_{11}[x]/\langle\Phi_m(x)$ admits the basis $(1, x, x^2, \ldots, x^{\varphi(m)-1})$. Since $\frac{2\varphi(m)}{3} < \varphi(m)$ the coordinates of $(x+1)^{\frac{2\varphi(m)}{3}} \bmod \Phi_m$ on the basis of $\mathbb{F}_{11}[x]/\langle\Phi_m(x)$ are the same as the coefficients of the polynomial $(x+1)^{\frac{2\varphi(m)}{3}}$.

The coefficient of x in $(x+1)^{\frac{2\varphi(m)}{3}}$ is $\frac{2\varphi(m)}{3}$ which is not 0 modulo 11 by the assumptions on m. Hence $(x+1)^{\frac{2\varphi(m)}{3}} \not\equiv \pm 1 \mod \Phi_m \in \mathbb{F}_{11}[x]$, so the class number is not divisible by 5. □

Remark 4.2. Artin's conjecture states that if a is a non-square integer other than -1 then the set of primes m such that a is primitive in $(\mathbb{Z}/m\mathbb{Z})^*$ has a positive density. In particular this implies that there are infinitely many primes m such that Φ_m is irreducible modulo 11 (resp 2). Hooley [Hoo67] proved the conjecture under a generalization of Riemann's Hypothesis

Lemma 4.3. *For all integers $a \neq 21, 23 \pmod{25}$ the number field defined by f_a as defined in Equation (3.1) has no $R_{K,5} \not\equiv 0 \pmod 5$.*

Proof. We have $\mathrm{Disc}(f_a) = \mathrm{Disc}(\mathbb{Q}(\alpha))[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]^2$ where α is a root of f_a in its number field. Since

$$\mathrm{Disc}(a) = a^4 + 6a^3 + 27a^2 + 54a + 81,$$

5 is not ramified and doesn't divide the index $[\mathcal{O}_{\mathbb{Q}(\alpha)} : \mathbb{Z}[\alpha]]$. The definition of Schirokauer maps implies that if $f \equiv g \pmod{p^2\mathbb{Z}[x]}$ are two polynomials then they have the same Schirokauer maps.

For each a in the interval $[1, 5^2]$ other than 21 and 23 we compute the matrix

$$\begin{pmatrix} \lambda_0(\alpha) & \lambda_1(\alpha) & \lambda_2(\alpha) \\ \lambda_0(-\frac{\alpha+1}{\alpha}) & \lambda_1(-\frac{\alpha+1}{\alpha}) & \lambda_2(-\frac{\alpha+1}{\alpha}) \end{pmatrix},$$

where α is a root of f_a in its number field. Here the λ_i's are defined as in Algorithm 3. Note that $\frac{\alpha+1}{\alpha}$ is the image of α by an automorphism of f_a. One verifies that in each case the normalized 5-adic regulator is not divisible by 5. Hence, for any integer $a \not\equiv 21, 23 \pmod{25}$, the 5-adic regulator of $\{\alpha, -\frac{\alpha+1}{\alpha}\}$ divided by 25 is not divisible by 5. Finally, the normalized 5-adic regulator of f_a is not divisible by 5. □

When combining Lemma 4.1 and Lemma 4.3 one obtains point (2) of Theorem 1.6.

5. Numerical investigation of the density of p-rational fields

The Cohen-Lenstra-Martinet heuristic predicts very simple formulae for the density of number fields with class number prime to p and with Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ for every prime q and integer t. However, the authors of the heuristic conjectured only those heuristic statements which corroborate with numerical experiments. We bring new evidence in favor of the conjecture for cubic cyclic fields in Section 5.1. Then in Section 5.2 we bring evidence in many cases $(\mathbb{Z}/2\mathbb{Z})^t$ and $(\mathbb{Z}/3\mathbb{Z})^t$ for $t = 2, 3, 4$ and are able to state the corresponding conjectures. In Section 5.3, we

extend the results of Hofmann and Zhang to the case of Galois groups $(\mathbb{Z}/3\mathbb{Z})^t$ and $(\mathbb{Z}/2\mathbb{Z})^t$ with $t = 2, 3, 4$ and conclude by proving point (3) of the main theorem (Th 1.6) in Section 5.4.

5.1. **Numeric verification of the Cohen-Lenstra heuristics.** One of the most interesting facts about the Cohen-Lenstra heuristic is how well it is supported by statistical data. Encouraged by the case of quadratic fields one would expect a similar situation for the case of cyclic cubic fields, but in 1989 Cohen and Martinet wrote that "we believe that the poor agreement [with the tables] is due to the fact that the discriminants are not sufficiently large".

Puzzled by this assertion we repeated their computations and made statistics on the fields of conductor less than 8000, i.e. discriminant less than 6410^6, which was the bound for the computations of that time (e.g. [Gra75] considered the fields of conductor less than 4000). Since then computers' capabilities have increased by more than a factor 1000 so that we could compute the statistics for fields of conductor less than 10^7, i.e. discriminant less than 10^{14}, in roughly one calendar month, in parallel on several 30 cores and summed up to roughly 2.5 CPU years.

Looking at the data in Table 4 we understand what happened: the convergence speed to the mean density is very slow and the statistics to 8000 have a relative error between 19% and 100% which didn't allow Cohen and Martinet to conclude. However statistics to 10^7 have only a relative error between 0.2% and 15.5%, so we can conclude that the numerical data confirms their conjecture. More details are available in the online complement [BR17].

p	theoretic density	stat. density cond. ≤ 8000	relative error	stat. density cond. $\leq 10^7$	relative error
5	0.00167	$\frac{3}{1269} \approx 0.0236$	46%	$\frac{3316}{1714450} \approx 0.00193$	15.5%
7	0.0469	$\frac{45}{1269} \approx 0.0355$	24%	$\frac{78063}{1714450} \approx 0.0456$	3%
11	0.0000689	0	100%	$\frac{133}{1714450} \approx 0.0000775$	12.5%
13	0.00584	$\frac{6}{1269} \approx 0.00472$	19%	$\frac{10232}{1714450} \approx 0.00584$	2%
19	0.0128	$\frac{11}{1269} \approx 0.0086$	48%	$\frac{21938}{1714450} \approx 0.0128$	0.2%

TABLE 4. Statistics on the density of cyclic cubic fields whose class number is divisible by $p = 5$, 7, 11, 13 and respectively 19.

5.2. **Cohen-Lenstra-Martinet for Galois group $(\mathbb{Z}/3\mathbb{Z})^t$ and $(\mathbb{Z}/2\mathbb{Z})^t$.**

Lemma 5.1 (Kuroda's class number formula ([Lem94] Sec 3 and [Kur50] Sec 10))**.** *Let q be a prime and K a totally real Galois extension such that* $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/q\mathbb{Z})^t$*. Then K contains $\frac{q^t-1}{q-1}$ subfields of degree q and there exists an integer A such that*

$$h_K = q^A \prod_{k_i \text{ subfield of degree } q} h_{k_i}.$$

The Cohen-Lenstra-Martinet heuristic implies that that the class groups of the intermediate cyclic fields of prime k_i behave independently, and they obtain the following heuristic statement.

Conjecture 5.2 (reformulation of statements in [CM87])**.**

(1) *If $K = \mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_t})$, and p an odd prime, then*

$$\text{Prob}(p \nmid h_K) = \frac{(p)_\infty}{(p)_1}^{2^t - 1}.$$

(2) *If K has degree 3^t and is the compositum of t cyclic cubic fields and $p \geq 5$ is a prime then*

$$\text{Prob}(p \nmid h_K) = \begin{cases} (\frac{(p)_\infty}{(p)_1})^{2\frac{3^t-1}{2}}, & \text{if } p \equiv 1 \pmod 3; \\ \frac{(p^2)_\infty}{(p^2)_1}^{\frac{3^t-1}{2}}, & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

The conjecture is supported by the numerical evidence in Table 5. The data is available in the online complement [BR17].

p	theoretic density	stat. density cond. $\leq 10^6$	relative error
5	0.00334	$\frac{933}{203559} \approx 0.00458$	37%
7	0.0916	$\frac{23912}{203559} \approx 0.0354$	28%
11	0.000138	$\frac{26}{203559} \approx 0.000128$	7.5%
13	0.0116	$\frac{6432}{203559} \approx 0.0316$	72%
17	0.0000140	$\frac{4}{203559} \approx 0.0000197$	40.5%
19	0.0254	$\frac{3536}{203559} \approx 0.0173$	31.5%

TABLE 5. Statistics on the density of fields of Galois group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ whose class number is divisible by $p = 5$, 7, 11, 13, 17 and respectively 19.

5.3. **On the p-adic regulator for Galois groups $(\mathbb{Z}/2\mathbb{Z})^t$ and $(\mathbb{Z}/3\mathbb{Z})^t$.** We are interested in the probability that all the cyclic subfields of number field of Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ are without p-primary unity, or equivalently we want to investigate the relations between the normalized p-adic regulators of a compositum and of its subfields. We have here a similar result to Kuroda's formula.

Lemma 5.3. *Let p be an odd prime and $K = \mathbb{Q}(\sqrt{a}, \sqrt{b}))$ with a, b and ab positive rational numbers which are not squares. Let R denote the normalized p-adic regulator of K, then R_1, R_2 and R_3 the p-adic regulators of $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ and $\mathbb{Q}(\sqrt{ab})$. Then there exists an integer α such that*

$$R = 2^\alpha R_1 R_2 R_3.$$

Proof. A simple regulator calculation (e.g. [BP79]) implies that there exists β such that

$$[E : E_1E_2E_3] = 2^\beta \frac{h}{h_1h_2h_3},$$

where E and h are the unit group and the class number of $\mathbb{Q}(\sqrt{a},\sqrt{b})$, and E_i and h_i are the unit groups and class numbers of the quadratic subfields.

By Kuroda's formula (Lemma 5.1), $h/(h_1, h_2h_3)$ is a power of 2 so

$$[E : E_1E_2E_3] = 2^\gamma$$

for some integer γ. Hence the p-adic regulator of E is equal to the p-adic regulator of $E_1E_2E_3$ up to multiplication by a power of 2.

Let $\{\sigma_0 = \mathbf{id}, (\sigma_1 : \sqrt{a} \mapsto -\sqrt{a}, \sqrt{b} \mapsto \sqrt{b}), (\sigma_2 : \sqrt{a} \mapsto \sqrt{a}, \sqrt{b} \mapsto -\sqrt{b})$ and $(\sigma_3 : \sqrt{a} \mapsto -\sqrt{a}, \sqrt{b} \mapsto -\sqrt{b})\}$ be the automorphisms of K.

If ε_1 is a fundamental unit of $\mathbb{Q}(\sqrt{a})$ then $\varepsilon_1\sigma_1(\varepsilon_1) = N_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(\varepsilon_1) = \pm 1$ so that

$$\log_p(\sigma_1(\varepsilon_1)) = -\log_p(\varepsilon_1).$$

Since $\sigma_2(\varepsilon_1) = \varepsilon_1$ we have

$$\log_p(\sigma_2(\varepsilon_1)) = \log_p(\sigma_3(\varepsilon_1)) = \log_p(\varepsilon_1).$$

Similar equations hold for the fundamental units ε_2 and ε_3 of $\mathbb{Q}(\sqrt{b})$ and $\mathbb{Q}(\sqrt{ab})$. Hence the p-adic regulator of the subgroup generated by $\varepsilon_1, \varepsilon_2$ and ε_3 is

$$\begin{vmatrix} \log_p(\varepsilon_1) & \log_p(\sigma_1(\varepsilon_1)) & \log_p(\sigma_2(\varepsilon_1)) \\ \log_p(\varepsilon_2) & \log_p(\sigma_1(\varepsilon_2)) & \log_p(\sigma_2(\varepsilon_2)) \\ \log_p(\varepsilon_3) & \log_p(\sigma_1(\varepsilon_3)) & \log_p(\sigma_2(\varepsilon_3)) \end{vmatrix} = \begin{vmatrix} \log_p(\varepsilon_1) & -\log_p(\varepsilon_1) & \log_p(\varepsilon_1) \\ \log_p(\varepsilon_2) & \log_p(\varepsilon_2) & -\log_p(\varepsilon_2) \\ \log_p(\varepsilon_3) & -\log_p(\varepsilon_3) & -\log_p(\varepsilon_3) \end{vmatrix}.$$

The latter determinant is equal to $(-4)\log_p\varepsilon_1\log_p\varepsilon_2\log_p\varepsilon_3$, which completes the proof. □

Our heuristic is to assume that the factors R_1, R_2 and R_3 in Lemma 5.3 are independent.

Conjecture 5.4. *Let $q = 2$ or 3, $p > q$ a prime and t an integer. Then the density of totally real number fields K such that $\mathrm{Gal}(K) = (\mathbb{Z}/q\mathbb{Z})^t$ for which the normalized p-adic regulator is divisible by p for at least one of the cyclic subgroups is*

(1) $\mathrm{Prob}\left(\exists F \subset K, R'_{F,p} \equiv 0[p] | \mathrm{Gal}(K) = (\mathbb{Z}/2\mathbb{Z})^t \text{ tot. real}\right) = 1 - (1 - \frac{1}{p})^{2^t-1}$

(2) $\mathrm{Prob}\left(\exists F \subset K, R'_{F,p} \equiv 0[p] \mid \mathrm{Gal}(K) = (\mathbb{Z}/3\mathbb{Z})^t\right) = 1 - (1-\mathcal{P})^{\frac{3^t-1}{2}}$, *where*

$$\mathcal{P} = \begin{cases} \frac{2}{p} - \frac{1}{p^2}, & \text{if } p \equiv 1 \pmod 3 \\ \frac{1}{p^2}, & \text{otherwise.} \end{cases}$$

In a numerical experiment, we considered all number fields to verify Conjecture 5.4 of the form $\mathbb{Q}(\sqrt{d_1},\sqrt{d_2},\sqrt{d_3})$ with $d_1, d_2 \in [2, 300]$ squarefree and distinct, then the fields of Galois group $(\mathbb{Z}/3\mathbb{Z})^3$ and conductor less than 10^5, i.e. discriminant less than 10^{30}. In Table 6 we compare the statistical density with $1 - (1 - \frac{1}{p})^7$. The numerical computations use Algorithm 3 with SAGE code in Appendix D. The programme can be downloaded from the online complement [BR17].

p	experimental density	Conj 5.4 density	relative error
5	$\frac{29301}{37820} \approx 0.775$	0.790	2%
7	$\frac{19538}{37820} \approx 0.517$	0.660	22%
11	$\frac{17872}{37820} \approx 0.473$	0.487	3%

TABLE 6. Numerical verification of Conjecture 5.4 in the case where $\mathrm{Gal}(K) = (\mathbb{Z}/2\mathbb{Z})^3$. The sample consists of number fields which can be written as $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$ with $2 \leq d_1, d_2, d_3 \leq 300$ squarefree and distinct.

Remark 5.5. Conjecture 5.4 describes well the computations required to find Example 2.11. With notations as in Example 2.11 we set $d_1 = -1$ and $d_2 = 2$ and, for $i \geq 3$ we define d_i as the smallest integer larger than d_{i-1} such that, for all subfield $F \subset \mathbb{Q}(d_1, \ldots, d_i)$, $R'_{F,p}$ is not divisible by p. Then the conjecture predicts $\log_2 d_i \approx c2^i$ for some constant c since the expectancy of d_i is the inverse of the probability of $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_{i-1}}, \sqrt{d})$ has normalized p-regulator non divisible by p when d is a random integer, which corroborates with experimental values:

i	3	4	5	6	7
d_i	3	11	47	97	4691
$2^{-i}\log_2(d_i)$	0.20	0.21	0.17	0.10	0.19

One can expect $d_9 \approx 2^{0.2 \cdot 2^9} \approx 2 \cdot 10^{15}$, which is out of reach of nowadays computers. Moreover, once the condition on p-adic regulators is satisfied, one has to also test the condition on class numbers. It seems to indicate that one needs new theoretical results before finding examples of the Greenberg's conjecture for $p = 5$ and Galois groups $(\mathbb{Z}/2\mathbb{Z})^t$ with t larger than 10.

5.4. **Greenberg's conjecture as a consequence of previous conjectures.** Since the Conjectures 2.16 and 2.13 predated Greenberg's conjecture and are supported by strong numerical evidence it is interesting to note that they imply that $\mathrm{GC}_\infty(\mathbb{Z}/3\mathbb{Z}, p)$ holds.

Theorem 5.6. *Under Conjecture 2.13 and Conjecture 2.16, for all prime $p > 3$, $\mathrm{GC}_\infty(\mathbb{Z}/3\mathbb{Z}, p)$ holds.*

Proof. For any D let $K(D)$ be the set of cubic cyclic number fields with conductor less than D. Then we have

$$\begin{aligned}\limsup_{D\to\infty} \frac{\#\{K \in K(D) \text{ non } p\text{-rational}\}}{\#K(D)} &\leq \limsup_{D\to\infty} \frac{\#\{K \in K(D),\ p \mid h_K R'_{K,p}\}}{\#K(D)} \\ &\leq \mathrm{Prob}(p \mid h_K) + \mathrm{Prob}(p \mid R'_{K,p}) \\ &\leq \frac{2}{p} + 1 - \prod_{i=1}^{\infty}(1 - p^{-i}) < \frac{1}{2}.\end{aligned}$$

Hence, there exist cyclic cubic fields K with arbitrarily large conductors such that p doesn't divide $h_K R'_{K,p}$, and which by Lemma 2.1 are p-rational. □

Thanks to Conjecture 5.4 we can prove a similar result in the case of composite of quadratic and respectively cubic cyclic real fields.

Theorem 5.7. *Let t be an integer, $q = 2$ or 3 and p a prime such that $p > 5q^t$. Under Conjecture 5.4 and Conjecture 5.2, there exist infinitely many p-rational number fields of Galois group $(\mathbb{Z}/q\mathbb{Z})^t$, or equivalently $\mathrm{GC}_\infty((\mathbb{Z}/2\mathbb{Z})^t, p)$ and $\mathrm{GC}_\infty((\mathbb{Z}/3\mathbb{Z})^t, p)$ hold.*

Proof. Let $K(D)$ denote the set of totally real number fields of Galois group $(\mathbb{Z}/q\mathbb{Z})^t$ of conductor less than D. Then we have

$$\begin{aligned}
\limsup_{D\to\infty} \frac{\#\{K \in K(D) \text{ non } p\text{-rational})}{\#K(D)} &\leq \limsup_{D\to\infty} \frac{\#\{K \mid K(D)\ \exists F \subset K\ p \mid h_F R'_{F,p}\}}{\#K(D)} \\
&\leq \mathrm{Prob}(p \mid h_K) + \mathrm{Prob}(\exists F \subset K, p \mid R'_{F,p}) \\
&\leq 2 - (1 - \frac{2}{p})^{\frac{q^t-1}{q-1}} - (1 - \sum_{i=1}^{\infty} p^{-i})^{\frac{q^t-1}{q-1}} \\
&\leq \frac{2q^t}{q-1}(\frac{2}{p} + \frac{1}{p(p-1)}) \\
&\leq \frac{5q^t}{p}(\frac{4}{5} + \frac{2}{5(p-1)}) < 1.
\end{aligned}$$

□

Note that Theorem 5.7 has a conclusion which encompass the one of Theorem 5.6, but the difference in assumptions justifies to separate the two results. Also note that the condition $p > 5q^t$ is artificial and it could be improved if one proved

$$\mathrm{Prob}(p \mid h_K R'_{K,p}) < \mathrm{Prob}(p \mid h_K) + \mathrm{Prob}(p \mid R'_{K,p}).$$

If these two divisibility properties were orthogonal then Greenberg's conjecture for groups $(\mathbb{Z}/q\mathbb{Z})^t$, $q = 2$ or 3, would hold without any condition on p and t.

Conclusion and open questions

To sum up, Greenberg's conjecture is solved in the particular case of $G = \mathbb{Z}/2\mathbb{Z}$ and it is well supported by heuristics and numerical experiments for $G = (\mathbb{Z}/q\mathbb{Z})^t$ when $q = 2$ or 3. In the general case of non-abelian Galois groups however our results are limited to a list of examples.

The problem raises new questions about the independence of class numbers and of p-adic regulators, which could be tackled by techniques of analytic number theory, similar to the recent progress on the Cohen-Lenstra-Martinet heuristic. It is interesting to create new algorithms to test divisibility of p-regulator and of the class number by p with a better complexity than computing a system of fundamental units and respectively the class number.

Greenbergs' p-rationality conjecture corresponding to the case $G = (\mathbb{Z}/2\mathbb{Z})^t$ offers a new technique to construct Galois representations with open image in $\mathrm{GL}_n(\mathbb{Z}_p)$ with $4 \leq n \leq 2^{t-1} - 3$ (cf [Gre16, Prop 6.7], solving new cases of the inverse Galois problem. The previous results were restricted to $n = 2$ and $n = 3$, so that the known examples with $G = (\mathbb{Z}/2\mathbb{Z})^5$ are enough to improve on previous results.

Appendix A. The algorithm of Pitoun and Varescon

```
"""

Compute the invariant factors as in Corollary 4.1 in the reference article.
"""
def FI(K,p,n):
    f=K.defining_polynomial()
    r1,r2=K.signature()
    ab=pari(' K = bnfinit(' + str(f) + ',1);   '+\
           ' bnfcertify(K);               '+\
           ' Kr = bnrinit(K, ' + str(p^n)+ '); '+\
           ' Kr.clgp.cyc ')
    # Kr is the Ray class group.
    return ab
    # return val(ai) and val(bj)
    # where A_{p^{n}}(K) = Z/a1 x ... x Z/a_r2+1 x Z/b1 x ... x Z/bt
    # and val_p(a1) >= ... >=val_p(a_r2+1) >= val_p(b1) >= ...


"""
Test is the number field of f is p-rational.
If this number field doesn't verify Leopoldt's conjecture
 then the programme doesn't terminate.

"""
def is_p_rational(f,p):
    Zx=f.parent()
    K.<a>=NumberField(f)
    r1,r2=K.signature()
    OK=K.ring_of_integers()
    factorization_p=factor(p*OK) # pairs (pi,vi)
    e=max([pivi[1] for pivi in factorization_p]) # second component of (pi,vi)
    s=valuation(e,p)
    n=2+s
    old_ab=FI(K,p,n)
    old_a=FI(K,p,n)[:r2+1]  # first r2+1 components returned by FI
    #                         old_a=[val_p(a1),val_p(a2),...,val_p(a_r2+1)]
    old_b=FI(K,p,n)[r2+1:]  # old_b=[val_p(b1),val_p(b2),...,val_p(bt)]
    n+=1
    found=false
    while not found:
        new_ab=FI(K,p,n)
        new_a=FI(K,p,n)[:r2+1] # similar to old_a, corresponds to n+1
        new_b=list(FI(K,p,n)[r2+1:]) # similar to old_b, corresponds to n+1
        if new_a ==  [p*ai for ai in old_a] and min(new_a) > p*max(new_b+[1]):
            #  if new_b is empty we replace max(new_b) by 1
            found=true
            if new_b == len(new_b)*[1]: # the elements of new_b are non-negative
                answer=true       # their sum is 0 if they are all zero
            else:
                answer=false
        old_ab=new_ab             # increase n by 1
```

```
        old_a=new_a
        n+=1
    return answer
```

Appendix B. Implementation of Algorithm 1

```
"""
Given a cyclic cubic field K=Q(z) and an integer R, the function searches
 a certificate that (z^R-1)/(x-1) is not a p-th power in K.

R,p = two integers
f = a polynomial defining a cyclic cubic field
m = conductor f
factm = factorization of m
OK = ring of integers of the number field of f
required_trials = number of failures before we give up
"""
def is_cyclo_p_th_power(R,p,m,factm,OK,f,required_trials):
    euler_phi_m = prod([qe[0]^qe[1]-qe[0]^(qe[1]-1) for qe in factm])
    #  Euler totient of m
    m1 = euler_phi_m // 3  # constant used in Lemma 3.8
    q = next_prime(p)
    trials = 0
    while true:
        # q runs through primes = 1 mod (p) larger than p
        # next 4 lines generate next q
        q = next_prime(q+1)
        if q % p != 1:
            q=next_prime(q+1)
            continue
        trials += 1                    # increase number of trials
        gq = (q*OK).factor()[0][0]     # gq (gothic q) is a prime ideal above q
        k_gq = gq.residue_field()      # k_gq is the residue field of gq
        abar = f.roots(k_gq)[0][0]     # abar is a root of f in k_gq
        e = m1*(norm(gq)-1)//p         # expression used in Lemma 3.8
        epsbar = (abar^R-1)/(abar-1)  # image in k_gq of (z^R-1)/(z-1)
        if epsbar^e != 1:              # if (z^R-1)/(z-1) is not  1 (mod gq)
            #                            then gq is a certificate
            return False
        else:
            if trials >= required_trials:
                return True
```

Appendix C. Implementation of Algorithm 2

```
"""
This function takes as parameter a polynomial f whose number field K is cyclic cubic.
The output is a unit u, which is not necessarily of infinite order.
If ord(u) is infinite and p is a prime which doesn't divide the p-adic regulator of K,
then u is used to rapidly certify it.
"""
def fast_units(f):
    K.<a>=NumberField(f)
    OK=K.ring_of_integers()
```

```
    m=K.disc().sqrt()    # m is the conductor of K because it is cyclic cubic
    # the following 5 lines compute gm, an ideal such that gm^3=(m)
    gm=OK
    for p in m.prime_factors():
       pfact=(p*OK).factor()
       gp=prod([pe[0]^(pe[1]//3) for pe in pfact])
       #                 # gp prime ideal such that gp^3=(p)
       gm=gm*gp
    if not gm.is_principal(): # is_principal uses LLL and \
                              # is not certified to find a generator\
                              #  even if gm is principal
        return K(1),K(1)
    omega=gm.gens_reduced()[0] # (omega)=gm. Uses LLL.
    sigma=K.automorphisms()[1] # sigma is a non-trivial automorphism of K
    eps=sigma(omega)/omega     # a unit of K, according to Remark 3.10
    return eps,sigma(eps)
```

Appendix D. Implementation of Algorithm 3

```
"""
Schirokauer map associated to z and p. Parameter E doesn't depend on z so it is pre-computed.
"""
def Schirokauer(z,p,E,gamma=None):
    v = exp_mod_pk(z,E,p,k=2)-1                    # Definition 3.9
    unramified = not (z.parent().disc() % p == 0) # p divides Disc(K) ?
    if unramified and gamma == None:
        gamma=p                                    # if NO we are done
    elif gamma == None:                            # if YES and we have a
        #                                            uniformizer we are done
        #                                       otherwise compute a uniformizer
        # next 6 lines compute a uniformizer gamma
        K = z.parent()                  # deduce K from z
        OK = K.ring_of_integers()       # ring of integers
        n=K.degree()                    # degree of K
        rad=prod([gp_[0]^(gp_[1]//n) for gp_ in  (p*OK).factor()] )
        # rad = product of prime ideals above p
        _,gamma=rad.gens_two()
        # gamma is such that <p,gamma> == rad
        Pcoeffs = (v/gamma).vector()
        # Compute a polynomial P such that P(a) = v/gamma
        # where a is such that K=Q(a).
        # Call Pcoeffs the coefficients of P.
    return [GF(p)(e) for e in Pcoeffs]
    #  Reduce the coefficients of P modulo p.

"""
Given a polynomial f and a prime p tries to find a certificate that
the p-adic regulator is not divisible by p.
"""
def criterium_p_not_divides_pRegulator(f,p):
    K.<a>=NumberField(f)            # K=Q(a) is the number field of f
    OK=K.ring_of_integers()         # ring of integers
```

```
    m = K.disc().sqrt()             # since K is cyclic cubic, m=cond(K)
    eps0,eps1=fast_units(f)         # try to find unit using Algorithm 2.
    if eps0 == 1:                   # in case of failure
        return "Maybe"              # we do not have a basis of subgroup
        #                             of finite index
        if (f.disc() // K.disc()) % p^2 == 0: # if p divides [OK:Z[a]]
            return "Maybe"                    # we answer "Maybe"
        # Compute E denoted e in Definition 3.9
        E=ZZ(lcm([ee[0].norm()-1 for ee in (p*OK).factor()]))
        # The next 9 lines compute gamma, a uniformizer of p
        if K.disc() % p == 0:
            OK=K.ring_of_integers()
            n=K.degree()
            rad=prod([gp_[0]^(gp_[1]//n) for gp_ in  (p*OK).factor()] )
            _,gamma=rad.gens_two()
            if gamma == p:
                gamma=p
        else:
            gamma=p
        # compute the rank of the matrix in Algorithm 3.
        Srank=Matrix(GF(p),2,3,[Schirokauer(eps0,p,E,gamma),Schirokauer(eps1,p,E,gamma)]).rank()
        if Srank == 2:
            return True
# Main enumeration.
Qx.<x>=QQ['x']
line=fd.readline()                      # line = next line of file fd
cond=0                                  # cond = conductor of previous field
while line != "":                       # until end f file
    if not line[0] == "x":              # skip comment lines
        cond=int(line)
    else:
        f=Qx(line.strip())              # f = polynomial read in file
        K.<a>=NumberField(f)            # K=Q(a) is the number field of f
        OK=K.ring_of_integers()         # ring of integers
        m = K.disc().sqrt()             # since K is cyclic cubic, m=cond(K)
        if m < cond:                    # skip f if its conductor is smaller
            line=fd.readline()          # than previous conductor because
            continue                    # it has been already treated
        for p in ps:
            bool = criterium_p_not_divides_pRegulator(f,p)
            if bool == "True":
                bools = bools + ",False"
            else:
                bools = bools + ",Maybe"
        gd.write(str(f)+":"+bools+"\n")
        gd.flush()
    line=fd.readline()
```

References

[BBB+98] Christian Batut, Karim Belabas, Dominique Bernardi, Henri Cohen, and Michel Olivier. *User's Guide to PARI-GP*. ftp://megrez.math.u-bordeaux.fr/pub/pari, 1998. see also http://pari.home.ml.org.

[BP79] Lyliane Bouvier and Jean-Jacques Payan. Sur la structure galoisienne du groupe des unités d'un corps abélien de type (p, p). In *Annales de l'institut Fourier*, volume 29, pages 171–187, 1979.

[BR17] Razvan Barbulescu and Jishnu Ray. Electronic manuscript of computations of "Some remarks and experiments on Greenberg's p-rationality conjecture", 2017. available online at `https://webusers.imj-prg.fr/~razvan.barbaud/pRational.html`.

[BW89] Johannes Buchmann and Hugh Williams. On the computation of the class number of an algebraic number field. *Mathematics of Computation*, 53(188):679–688, 1989.

[Bye01a] Dongho Byeon. Divisibility properties of class numbers. *Trends in mathematics, Information Center for Mathematical Sciences*, 4(1):26–30, 2001.

[Bye01b] Dongho Byeon. Indivisibility of class numbers and Iwasawa λ-invariants of real quadratic fields. *Compositio Mathematica*, 126(3):249–256, 2001.

[CDO98] Henri Cohen, Francisco Diaz Y Diaz, and Michel Olivier. Computing ray class groups, conductors and discriminants. *Mathematics of Computation*, 67(222):773–795, 1998.

[CL84a] Henri. Cohen and Hendrik Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[CL84b] Henri Cohen and Hendrik W Lenstra, Jr. Heuristics on class groups. In *Number theory (New York, 1982)*, volume 1052 of *Lecture Notes in Math.*, pages 26–36. Springer, Berlin, 1984.

[CM87] Henri Cohen and Jacques Martinet. Class groups of number fields: numerical heuristics. *Math. Comp.*, 48(177):123–137, 1987.

[CM90] Henri Cohen and Jacques Martinet. étude heuristique des groupes de classes des corps de nombres. *J. Reine Angew. Math.*, 404:39–76, 1990.

[Coh13] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate texts in mathematics*. Springer Science & Business Media, 2013.

[CR16] Christophe Cornut and Jishnu Ray. Generators of the pro-p iwahori and galois representations, 2016. arXiv preprint arXiv:1611.06084, to appear in International Journal of Number Theory.

[Fou14] Etienne Fouvry. Analytic aspects of cohen-lenstra heuristics, 2014. recorder lectures of the IHES summer school on analytic number theory, IHES.

[GG77] Georges Gras and Marie-Nicole Gras. Calcul du nombre de classes et des unités des extensions abéliennes réelles de q. *Bull. Sci. Math*, 2(101):2, 1977.

[GJ89] Georges Gras and Jean-François Jaulent. Sur les corps de nombres réguliers. *Mathematische Zeitschrift*, 202(3):343–365, 1989.

[Gra75] Marie Nicole Gras. Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de q. *J. reine angew. Math*, 277(89):116, 1975.

[Gra13] Georges Gras. *Class Field Theory: from theory to practice*. Springer monographs of mathematics. Springer Science & Business Media, 2013.

[Gra14] Georges Gras. Les θ-régulateurs locaux d'un nombre algébrique. conjectures p-adiques. *HAL Id: hal-00936889*, 2014.

[Gra16] Georges Gras. Approche p-adique de la conjecture de Greenberg (cas galoisien réel p-décomposé). *Prépublication, arXiv:1611.09592*, 2016.

[Gre76] Ralph Greenberg. On the Iwasawa invariants of totally real number fields. *American Journal of Mathematics*, 98(1):263–284, 1976.

[Gre16] Ralph Greenberg. Galois representations with open image. *Ann. Math. Qué.*, 40(1):83–119, 2016.

[Hak09] Tuomas Hakkarainen. On the computation of class numbers of real abelian fields. *Mathematics of Computation*, 78(265):555–573, 2009.

[Har74] Paul Hartung. Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3. *Journal of Number Theory*, 6(4):276–278, 1974.

[HM16] Farshid Hajir and Christian Maire. Prime decomposition and the Iwasawa mu-invariant. *arXiv preprint arXiv:1601.04195*, 2016.

[Hoo67] Christopher Hooley. On artin's conjecture. *Journal für die reine und angewandte Mathematik*, 225:209–220, 1967.

[HZ16] Tommy Hofmann and Yinan Zhang. Valuations of p-adic regulators of cyclic cubic fields. *Journal of Number Theory*, 169:86–102, 2016.

[JNQD93] Jean-François Jaulent and Thong Nguyen Quang Do. Corps p-rationnels, corps p-réguliers, et ramification restreinte. *Journal de théorie des nombres de Bordeaux*, 5(2):343–363, 1993.

[Kur50] Sigekatu Kuroda. Über die Klassenzahlen algebraischer Zahlkörper. *Nagoya Math. J.*, 1:1–10, 1950.

[Lem94] Franz Lemmermeyer. Kuroda's class number formula. *Acta Arith.*, 66(3):245–260, 1994.

[LLL82] Arjen Klaas Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[LOU98] Stéphane LOUBOUTIN. Majorations explicites du résidu au point 1 des fonctions zêta de certains corps de nombres. *J. Math. Soc. Japan*, 50(1):57–69, 01 1998.

[Mil15] John C. Miller. Class numbers in cyclotomic $\mathbb{Z}_p$-extensions. *J. Number Theory*, 150:47–73, 2015.

[MM13] Gunter Malle and Bernd Heinrich Matzat. *Inverse Galois Theory*. Springer Science & Business Media, 2013.

[MNQD90] Abbas Movahhedi and Thong Nguyen Quang Do. Sur l'arithmétique des corps de nombres p-rationnels. In *Séminaire de Théorie des Nombres, Paris 1987–88*, volume 81 of *Progr. Math.*, pages 155–200. Birkhäuser Boston, Boston, MA, 1990.

[Mov88] Abbas Movahhedi. *Sur les p-extensions des corps p-rationnels*. PhD thesis, Université Paris VII, 1988.

[Mov90] Abbas Movahhedi. Sur les p-extensions des corps p-rationnels. *Math. Nachr.*, 149:163–176, 1990.

[Pan95] Peter N Panayi. *Computation of Leopoldt's p-adic regulator*. PhD thesis, University of East Anglia, 1995.

[PV15] Frédéric Pitoun and Firmin Varescon. Computing the torsion of the p-ramified module of a number field. *Math. Comp.*, 84(291):371–383, 2015.

[Sau98] Odile Sauzet. Theorie d'Iwasawa des corps p-rationnels et p-birationnels. *Manuscripta mathematica*, 96(3):263–273, 1998.

[Sch93] Oliver Schirokauer. Discrete logarithms and local units. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 345(1676):409–423, 1993.

[Sha66] Igor Shafarevich. Extensions with given points of ramification. *Americal mathematical society translations*, 2.59:128–149, 1966.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[WR76] Peter J. Weinberger and Linda Preiss Rothschild. Factoring polynomials over algebraic number fields. *ACM Transactions on Mathematical Software (TOMS)*, 2(4):335–350, 1976.

UMR 7586, CNRS, Université Paris 6 and Université Paris 7
Current address: 4, place Jussieu, 75005, Paris, France
E-mail address: razvan.barbulescu@imj-prg.fr

Département de Mathématiques, Université Paris-Sud 11
Current address: bât. 425, 91405 Orsay Cedex, France
E-mail address: jishnu.ray@u-psud.fr