SOME REMARKS AND EXPERIMENTS ON 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. The object of this article is to discuss a conjecture of Greenberg and its links to the Galois inverse problem. We show that it is related to well established conjectures in algebraic number theory and that some particular cases are corollaries of known results. Finally, we do numerical experiments which allow to formulate new conjectures which imply Greenberg's conjecture.

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 [18] which has been connected to p-rationality [33, Th. 1.1]. In the study of the inverse Galois problem, Greenberg [19] 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 [8, 10] and to the valuation of the p-adic regulator [14, 22].

This classical notion traces back to the work of Gras and Jaulent [16] which was continued by Movahhedi, Nguyen Quang Do and Jaulent [30, 24]. 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 ([30] and [29])**.** 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 [36, 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.

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

Examples 1.2. (1) The imaginary quadratic fields $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, $\mathbb{Q}(\sqrt{-163})$ are p-rational for any odd primes p. Indeed, they have no units other than ± 1 and their rings of integers are principal, so point (4) of the definition is verified.

(2) The field $\mathbb{Q}(i)$ is not 2-rational but is p-rational for every odd prime. Indeed, $\langle 2\rangle = \langle 1+i\rangle^2$ but 2 is not a square in $\mathbb{Q}(i)$, so point (4) is not satisfied.

For many properties of p-rational fields we refer the reader to the corresponding chapter of [13, Ch IV.3]. Greenberg's result [19, 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 $\mathrm{Gal}(K/\mathbb{Q})$. Under the same hypothesis, that there exists a p-rational number field K, Cornut and Ray [11, Sec 3] showed that the pro-p Iwahori subgroup of the adjoint simple reductive group is $\mathrm{Gal}(M/K)$, which solves particular cases of the inverse Galois problem.

Greenberg noted that the hypothesis on the characters are met if 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 [19])**.** *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 strenghtening of the inverse Galois problem, which is itself open in the non-abelian case (cf [27]). Also note that we don't discuss the related conjecture of Gras [14, Conj. 8.11] which states that every number field is p-rational for all but finitely many primes.

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

Theorem 1.5. (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 1.5, 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 1.5.

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 [9], 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 1.5.

2. Preliminaries

In the general case, p-rationality is hard to test so that it is important to have a simple criterium 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 $(\bigcap_{\mathfrak{p}|p} K_\mathfrak{p}^p) - K^p$.

Lemma 2.1 ([19] Rem 3.2)**.** *Assume K is an abelian field, p an odd prime such that $p \nmid h_K$ and K has no pth 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 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 ([19] 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 2.3 ([21])**.** *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 2.4. *For all odd prime p, $\mathrm{GC}_\infty(\mathbb{Z}/2\mathbb{Z}, p)$ holds.*

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 2.5. *(*[19, 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 the previous results to obtain:

Proposition 2.6. 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. Then 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.

Example 2.7. The field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{11}, \sqrt{47}, \sqrt{97})$ is p-rational. Indeed, Table 2.7 lists all the quadratic subfields of K together with their class numbers and normalized 5-adic regulators.

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 [8, 7] 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

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

D	$h_{Q(\sqrt{D})}$	$\varepsilon_{\mathbb{Q}(\sqrt{D}}$	$\frac{\varepsilon_{\mathbb{Q}(\sqrt{D}}^{24}-1}{5} \pmod 5$
2	1	$\sqrt{2}+1$	$4\sqrt{2}$
3	1	$\sqrt{3}-2$	$\sqrt{3}$
11	1	$3\sqrt{11}+10$	$\sqrt{11}$
47	1	$7\sqrt{47}-48$	$3\sqrt{47}$
97	1	$569\sqrt{97}+5604$	$2\sqrt{97}$
6	1	$2\sqrt{6}+5$	$2\sqrt{6}$
22	1	$42\sqrt{22}-197$	$3\sqrt{22}$
94	1	$221064\sqrt{94}-2143295$	$4\sqrt{94}$
194	2	$14\sqrt{194}-195$	$4\sqrt{194}$
33	1	$4\sqrt{33}+23$	$4\sqrt{33}$
141	1	$8\sqrt{141}-95$	$3\sqrt{141}$
291	4	$17\sqrt{291}+290$	$\sqrt{291}$
517	1	$465/2\sqrt{517}-10573/2$	$\sqrt{517}$
1067	4	$43\sqrt{1067}+98$	$3\sqrt{1067}$
4559	4	$8728944\sqrt{4559}-589381505$	$\sqrt{4559}$
66	2	$8\sqrt{66}+65$	$4\sqrt{66}$
282	2	$140\sqrt{282}-2351$	$3\sqrt{282}$
582	4	$8\sqrt{582}+193$	$4\sqrt{582}$
1034	2	$494\sqrt{1034}-15885$	$2\sqrt{1034}$
1551	4	$1377/2*a+308365/2$	$\sqrt{1551}$
2134	8	$210\sqrt{2134}-9701$	$2\sqrt{2134}$
3201	8	$168\sqrt{3201}+9505$	$3\sqrt{3201}$
9118	4	$13498005384\sqrt{9118}+1288900496447$	$4\sqrt{9118}$
13677	4	$39/2\sqrt{13677}+4561/2$	$\sqrt{13677}$
50149	12	$1377/2\sqrt{50149}+308365/2$	$4\sqrt{50149}$
3102	4	$19642\sqrt{3102}+1093973$	$2\sqrt{3102}$
6402	8	$80\sqrt{6402}+6401$	$4\sqrt{6402}$
27354	8	$432184\sqrt{27354}-71479105$	$\sqrt{27354}$
100298	8	$22440231983820\sqrt{100298}+7106789938093649$	$4\sqrt{100298}$
150447	32	$8\sqrt{150447}-3103$	$3\sqrt{150447}$
300894	16	$3654497770649690\sqrt{300894}+2004631106498511701$	$2\sqrt{300894}$

TABLE 1. The 31 quadratic subfilds of $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{11},\sqrt{47},\sqrt{97})$.

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 [10, 9] studied the case of fields K of degree 3 and 4, not necessarily cyclic, while more recently Miller [28, Sec 3] studied the case of cyclic extensions:

Conjecture 2.8 ([28] 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 2.9 ([9] 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 [12].

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. For this, we define the normalized p-adic regulator as an element of $\mathbb{Z}_p$ and its divisibility by p will be equivalent to the existence of p-primary units (Def (2.10)).

Let $\mathrm{rad}(p) = \prod_{\mathfrak{p} \mid p} \mathfrak{p}$ be the radical of p in K and

$$\begin{array}{rccc} \tau: & \{x \in K^* \mid \forall \mathfrak{p} \mid p, \mathrm{val}_\mathfrak{p}(x) = 0\} & \to & 1 + \mathrm{rad}(p) \\ & x & \mapsto & x^e, \end{array}$$

where $E = \mathrm{lcm}(\{N(\mathfrak{p}) - 1, \mathfrak{p} \mid p\})$ and $N(\mathfrak{p})$ is the norm of $\mathfrak{p}$. Let $\ell_p(1-x) = \sum_{i=1}^\infty \frac{x^i}{i}$ be the p-adic logarithm defined on $1 + \mathrm{rad}(p)$ with values in $\mathrm{rad}(p)$. Then we finally set $\log_p = \ell_p \circ \tau$, i.e. for any integer x of K whose valuation at $\mathfrak{p}$ is zero for all $\mathfrak{p} \mid p$, we call p-adic logarithm

$$\log_p x = \sum_{i=1}^\infty \frac{(-1)^i}{i} (x^E - 1)^i.$$

Definition 2.10. Let K be totally real of degree n and unit rank $r = n - 1$. Then we call p-adic regulator

$$R_{K,p} = \det\Big(\log_p(\sigma_j(\varepsilon_i))\Big),$$

where σ_j are r embeddings of K in $\overline{\mathbb{Q}_p}$. We then call normalized p-adic regulator

$$R'_{K,p} = \frac{(R_{K,p})^n}{N(\mathrm{rad}(p))^r}.$$

Note that $R'_{K,p} = (R_{K,p}/p^r)^n$ if p is unramified.

Lemma 2.11. *Let p be a prime and K a totally real number field. If p is ramified we moreover assume that $\deg(K) < p-1$. Then $R'_{K,p}$ is an element of $\mathbb{Z}_p$. Moreover p divides $R'_{K,p}$ if and only if K has p-primary units.*

Proof. The p-adic regulator $R_{K,p}$ belongs a priori to $\overline{\mathbb{Q}_p}$ and since it is stable by any automorphism of K, it belongs to $\mathbb{Q}_p$. As a quotient of $R_{K,p}$ by an element of $\mathbb{Q}_p$, $R'_{K,p}$ is also in $\mathbb{Q}_p$.

Let $\varepsilon_1, \ldots, \varepsilon_{n-1}$ be a system of fundamental units, where $n = \deg K$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of $\mathbb{Q}_p \otimes K$ in $\overline{\mathbb{Q}_p}$. Let $\mathcal{O}_p$ be the ring of integers of $\overline{\mathbb{Q}_p}$. Note that if ε is a unit then $\sum_{j=1}^n \sigma_j(\log_p(\varepsilon)) = \log_p(1) = 0$. Hence, if $\forall j \neq n$ $\sigma_j(\log_p(\varepsilon)) = 0$ then $\sigma_n(\log_p(\varepsilon) = 0$.

If p is unramified, we have $R'_{K,p} = (\det(\frac{\log_p \sigma_j(\varepsilon_i)}{p}))^n$. Suppose now that p is ramified. Let $\mathfrak{p}$ be a prime ideal dividing p and γ be such that $\mathfrak{p} = \langle p, \gamma \rangle$. Then γ belongs to $\mathfrak{p}$ but to none of the other prime ideals dividing p. Then $\forall x \in \mathcal{O}_p$, $\frac{x}{\gamma} \in p\mathcal{O}_p$ if and only if $x \in p\mathrm{rad}(p)$. Also note that $N(\mathrm{rad}(p))$ and $\prod \sigma_j(\gamma)$ are equal up to a factor relatively prime to p.

Note that the ramification index e of $\mathrm{rad}(p)$ is at most n, hence it is less than or equal to $p-1$. Then the following conditions are equivalent:

(1) $\log_p(x) \in p \cdot \mathrm{rad}(p)$
(2) x is a pth power in every completion.

Indeed, let us suppose (1). Then $\mathrm{val}_p(\frac{\log_p(x)}{p}) \geq \mathrm{val}_p(\mathrm{rad}(p)) = \frac{1}{e} > \frac{1}{p-1}$, so $x = \exp(\frac{\log_p x}{p})^p$ so it is a pth power in every completion. Suppose (2), i.e. $x = y^p$ for some y in $\bigcap_{\mathfrak{p}|p} K_{\mathfrak{p}}$, then $\frac{\log_p x}{p} = \log_p y$ and, since $\log_p$ maps into $\mathrm{rad}(p)$, $\log_p x \in p \cdot \mathrm{rad}(p)$.

We have then

$$\begin{aligned}
& p \mid R'_{K,p} \\
\Leftrightarrow\ & p \mid \det\left(\sigma_j(\tfrac{\log_p(\varepsilon_i)}{\gamma})\right) \\
\Leftrightarrow\ & \det\left(\sigma_j(\tfrac{\log_p(\varepsilon_i)}{\gamma})\right) \in p\mathcal{O}_p \\
\Leftrightarrow\ & \exists a_1, \ldots, a_r \in \mathbb{Z}^r - (p\mathbb{Z})^r \qquad \forall j \neq n \qquad \sigma_j(\tfrac{\log_p(\prod_i \varepsilon_i^{a_i})}{\gamma}) \in p\mathcal{O}_p \\
\Leftrightarrow\ & \exists a_1, \ldots, a_r \in \mathbb{Z}^r - (p\mathbb{Z})^r \qquad \forall j \qquad \sigma_j(\tfrac{\log_p(\prod_i \varepsilon_i^{a_i})}{\gamma}) \in p\mathcal{O}_p \\
\Leftrightarrow\ & \exists a_1, \ldots, a_r \in \mathbb{Z}^r - (p\mathbb{Z})^r \qquad \tfrac{\log_p(\prod_i \varepsilon_i^{a_i})}{\gamma} \in p\mathcal{O}_p \\
\Leftrightarrow\ & \exists \varepsilon \in E_K - E_K^p \qquad \log_p(\varepsilon) \in p \cdot \mathrm{rad}(p) \\
\Leftrightarrow\ & \text{K has a } p\text{-primary unit}
\end{aligned}$$

□

Very little is known on the probability that the normalized regulator is divisible by p. Schirokauer [34, p. 415] made the heuristic that the matrix which defines $R'_{K,p}$ modulo p is a random matrix with coefficients in $\mathbb{F}_p$ and therefore the probability that $p \mid R'_{K,p}$ 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 2.12 ([22] Conj 1)**.** *For primes $p > 3$ we have*

$$\mathrm{Prob}(p \mid R'_{K,p}) = \begin{cases} \frac{1}{p^2}, & \text{if } p \equiv 2 \pmod 3 \\ \frac{2}{p} - \frac{1}{p^2}, & \text{if } p \equiv 1 \pmod 3. \end{cases}$$

3. Algorithmic tools

Gathering numerical data on the class group, unit group and respectivey 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 [3] 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

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.

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 [3]. 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 surprizing that the algorithm of Cohen et al. [6] has a non-polynomial complexity. It is not clear what is the relevant partial information to associate to the ray class group, but Pitoun and Varescon [32] 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 ([36] 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.

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 ([5] 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 family of cubic cyclic fields we have a closed formula of the minimal polynomial of a unit of infinite order.

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 a unit whose minimal polynomial is

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

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

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

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 ω over $\mathbb{Q}$.

Then

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

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

$$\eta' = \begin{cases} \frac{9-(a+6\alpha)^2}{36}, & \text{if } 3 \nmid a \\ \frac{(a+6\alpha+5)(a+6\alpha-1)}{36}, & \text{otherwise.} \end{cases}$$

which is automatically a unit in K. □

Remark 3.5. Let $\eta_g = \mathbb{N}_{\mathbb{Q}(\zeta_m)/K}\left(\frac{\zeta_m^g-1}{\zeta_m-1}\right)$ for some $g \in \mathbb{N}$. For all odd value of a in $[1, 2000]$ such that m has no square factors other than 9 the minimal polynomial of η_g is

$$\mu_{\eta_g,\mathbb{Q}} = \begin{cases} \mu_a & \text{, if } 3 \nmid a \\ \nu_a & \text{, otherwise.} \end{cases}$$

However, g_a is not necessarily the minimal polynomial of $\omega = \mathbb{N}_{\mathbb{Q}(\zeta_m)/K}(\zeta_m - 1)$. For example, when $m = 313$ the minimal polynomial of ω is $x^3 - 143mx^2 + 122mx - m$.

3.2. **An algorithm to test if p divides h_K.** Nicole-Marie Gras [17] designed an algorithm which allows to test if h_K is divisible by p without computing h_K.

Definition 3.6. 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 3.7 ([15] 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 by van der Linden [35] and Hakkarainen [20] to take a polynomial time instead of exponential.

Lemma 3.8. *Let K be a cyclic number field of degree n and conductor m. Let p and q be two primes such that $q \equiv 1 \pmod{p}$. 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*

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

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

Proof. All $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ induce automorphisms of $k_\mathfrak{q}$ so $\rho_\mathfrak{q}(\tau(\gamma)) = \rho_\mathfrak{q}(\gamma)^{q^c}$ for some $c \in \mathbb{N}$. Since $q \equiv 1 \pmod{p}$, $(\rho_\mathfrak{q}(\gamma)^{q^c})^{\frac{q-1}{p}} = \rho_\mathfrak{q}(\gamma)^{\frac{q-1}{p}}$. We conclude because $\rho_\mathfrak{q}(\mathbb{N}_{\mathbb{Q}(\zeta_m)/K}(\gamma)) = \prod_{\tau\in\mathrm{Stab}(K)} \rho_\mathfrak{q}(\tau(\gamma))$, where $\mathrm{Stab}(K) = \{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \mid \sigma(K) = K\}$. □

The van der Linden algorithm, that we recall in Algorithm 1, consists in trying various primes q and in applying Lemma 3.8.

Algorithm 1 van der Linden

Require: a constant $\mathcal{P}$ 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: false, if $q \nmid h$; true with probability $\mathcal{P}$, if $q \mid h$.

$N \leftarrow \lceil \log_p \frac{1}{1-\mathcal{P}} \rceil$

repeat

$q \leftarrow$ next prime congruent to 1 mod p

increment i

until i>N or $\frac{x^g-1}{x-1}^{\frac{\varphi(m)}{3}\frac{q-1}{p}} \not\equiv 1 \mod \langle q, f(x)\rangle$

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 3.9 ([34])**.** 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

$$\begin{array}{rccc} \lambda_{f,p}: & \{\frac{a_1(x)}{a_2(x)} \mid a_1, a_2 \in \mathbb{Z}[x], p \nmid \mathrm{Res}(a_1a_2, f)\} & \to & \mathbb{F}_p[x]/\langle f(x)\rangle \simeq \mathbb{F}_p^{\deg f} \\ & a_1/a_2 \in \mathbb{Q}(x) & \mapsto & \frac{(a_1^{p^e-1}-1)-(a_2^{p^e-1}-1)}{p} \mod \langle p, f\rangle, \end{array}$$

where $e = \mathrm{lcm}(\{\deg f_i \mid f_i \text{ divides } f \text{ in } \mathbb{F}_p[x]\}$ and Res denotes the resultant. Note that the definition is well defined because, for all $a, b \in \mathbb{Z}[x]$, $\lambda_{f,p}(ab) = \lambda_{f,p}(a) + \lambda_{f,p}(b)$.

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 $p \nmid \mathrm{Res}(a_1a_2, f)$ 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 3.10. *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 a principal ideal $\mathfrak{l}$ so that $\mathfrak{l}^q = \ell\mathcal{O}_K$;*
2. *Let $\omega \in \mathcal{O}_K$ be a generator of $\mathfrak{l}$ and let σ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$. Then $\frac{\sigma(\omega)}{\omega}$ 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 $\ell = \mathfrak{l}^q$. Also, 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

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

By unique factorization we deduce that $\mathfrak{l}\mathbb{Z}[\zeta_m] = \langle\zeta_m - 1\rangle^{\frac{\ell-1}{q}}$ and, since the exponent is an integer, we conclude that $\mathfrak{l}$ is principal.

(ii) Since $\omega\mathcal{O}_K = \mathfrak{l}$, $\sigma(\omega)\mathcal{O}_K = \sigma(\mathfrak{l})$. But $\sigma(\mathfrak{l}) = \mathfrak{l}$ because $\mathfrak{m}^q = \ell\mathcal{O}_K = \sigma(\ell)\mathcal{O}_K = \sigma(\mathfrak{l})^q$ and the factorization into prime ideals is unique. Then $\omega\mathcal{O}_K = \sigma(\omega)\mathcal{O}_K$, hence their quotient is a unit. □

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 [5, Sec 4.8.2]
3: compute a generator ω_ℓ of the ideal $\mathfrak{l}$ using [4].
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. Note that Schirokauer's function is an application with image in $\langle p^2, f\rangle$ where f is a defining polynomial of K. Hence we call λ_0, λ_1, λ_2 the coefficients of 1, x and x^2 of the image of each element.

3.4. **An algorithm to determine p-rationality.** For any n let $\mathcal{A}_{p^n}$ denote the p-part of the ray class group ([13] 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 $[d_1,\ldots,d_k]$ 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 [6] and implemented in PARI [1].

Lemma 3.11 ([32] Thm 3.7 and Cor 4.1)**.** *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 $FI(\mathcal{A}_{p^n}) = [b_1,\ldots,b_s,a_1,\ldots,a_{r_2+1}]$ such that*

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 [37] to factor a defining polynomial of K in $K[x]$ and obtain a non-trivial automorphism σ
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
Compute a truncation of the normalized p-adic regulator using algorithms in [31] and return the result of the test whether this rank is 2
end if
end for

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

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

Example 3.12. The algorithm does not restrict to abelian number fields so that we could construct a examples of p-rational fields for each Galois group of quartic polynomials. 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.

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 Lemma 2.1 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.

In an experiment 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 $0,000016$ and the proportion of fields where $5 \mid R'_{K,5}$ is expected to be 0.04, 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

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 Lemma 3.11 to decide if K is p-rational
      Return answer and certificate
    end if
  end for

apply the criterion in Lemma 2.1 the field was actually non 5-rational. In terms of speed the criterion is much faster making the application of the criterion for 158542 fields negligible with respect to the application of Lemma 3.11 for the 5351 fields where the criterion couldn't be applied. Hence we had a speed-up of 5^2 and, 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 3.8 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 3.8 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 an integer such that $3 \mid \varphi(m)$, $11 \nmid \varphi(m)$ and Φ_m is irreducible modulo 11 and modulo 2. Then the number field of f_a defined in Equation (3.1) has class number not divisible by 5.*

Proof. Since 2 is a generator of $(\mathbb{Z}/m\mathbb{Z})^*$, $\eta := N_{\mathbb{Q}(\zeta_m)/K}(\frac{\zeta_m^2-1}{\zeta_m-1})$ is a generator of the group of cyclotomic units. By Lemma 3.7 the class number is divisible by 5 if and only if η is 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 3.8 to $\gamma = \frac{\zeta_m^2-1}{\zeta_m-1}$, $n = 3$, $p = 5$ and $q = 11$, so $\rho_{\mathfrak{q}}(\eta)^2 = (\rho_{\mathfrak{q}}(\zeta_m)+1)^{\frac{2\varphi(m)}{3}}$. 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 $(x+1)^{\frac{2\varphi(m)}{3}} \not\equiv 1 \mod \Phi_m \in \mathbb{F}_{11}[x]$, 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 proves that there are infinitely many primes m such that Φ_m is irreducible modulo 11 (resp 2). Hooley [23] 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. One verifies that in each case the normalized 5-adic regulator is not divisible by 5. Hence, for any integer $a \not\equiv 21, 23 \pmod 2 5$, 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 1.5.

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 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 1.5) 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 quadratc 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 10^4, i.e. discriminant less than 10^8, which

was the bound for the computations of that time (e.g. [17] considered the fields of conductor less than 4000). In the midwhile 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 10^4 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.

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	$\frac{45}{1269} \approx 0.0355$	24.5%	$\frac{78063}{1714450} \approx 0.0456$	3%
11	0.0000689	0	100%	$\frac{133}{1714450} \approx 0.0000775$	12.5%
13	0.00584	$\frac{6}{1269} \approx 0.00472$	19%	$\frac{21938}{1714450} \approx 0.00128$	0.2%
19	0.0128	$\frac{11}{1269} \approx 0.0086$	48.55%	$\frac{10232}{1714450} \approx 0.00584$	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 ([26] Sec 3 and [25] 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 [9])**.**

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

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

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

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

The conjecture is supported by the numerical evidence in Table 5.

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. [2]) 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 $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$ 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 $1 - (1 - \frac{1}{p})^7$.

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 2.7. 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, which corroborates with experimental values:

i	3	4	5	6	7
d_i	3	11	47	97	1567
$2^{-i}\log_2(d_i)$	0.20	0.21	0.17	0.10	0.08

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 2.12 and 2.9 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 2.9 and Conjecture 2.12, 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 composita 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 theoryi, 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 [19, 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.

References

1. 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.
2. Lyliane Bouvier and Jean-Jacques Payan, *Sur la structure galoisienne du groupe des unités d'un corps abélien de type* (p, p), Annales de l'institut Fourier, vol. 29, 1979, pp. 171–187.
3. Johannes Buchmann and Hugh Williams, *On the computation of the class number of an algebraic number field*, Mathematics of Computation **53** (1989), no. 188, 679–688.
4. Johannes Buchmann and Hugh C. Williams, *On principal ideal testing in algebraic number fields*, Journal of Symbolic Computation **4** (1987), no. 1, 11–19.
5. Henri Cohen, *A course in computational algebraic number theory*, Graduate texts in mathematics, vol. 138, Springer Science & Business Media, 2013.
6. Henri Cohen, Francisco Diaz Y Diaz, and Michel Olivier, *Computing ray class groups, conductors and discriminants*, Mathematics of Computation **67** (1998), no. 222, 773–795.
7. Henri. Cohen and Hendrik Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62. MR 756082
8. Henri Cohen and Hendrik W Lenstra, Jr., *Heuristics on class groups*, Number theory (New York, 1982), Lecture Notes in Math., vol. 1052, Springer, Berlin, 1984, pp. 26–36. MR 750661
9. Henri Cohen and Jacques Martinet, *Class groups of number fields: numerical heuristics*, Math. Comp. **48** (1987), no. 177, 123–137. MR 866103
10. ———, *étude heuristique des groupes de classes des corps de nombres*, J. Reine Angew. Math. **404** (1990), 39–76. MR 1037430
11. Christophe Cornut and Jishnu Ray, *Generators of the pro-p iwahori and galois representations*, arXiv preprint arXiv:1611.06084 (2016).

12. Etienne Fouvry, *Analytic aspects of cohen-lenstra heuristics*, recorder lectures of the IHES summer school on analytic number theory, IHES, 2014.
13. Georges Gras, *Class field theory: from theory to practice*, Springer Science & Business Media, 2013.
14. ———, *Les θ-régulateurs locaux d'un nombre algébrique. conjectures p-adiques*, (2014).
15. Georges Gras and Marie-Nicole Gras, *Calcul du nombre de classes et des unités des extensions abéliennes réelles de q*, Bull. Sci. Math **2** (1977), no. 101, 2.
16. Georges Gras and Jean-François Jaulent, *Sur les corps de nombres réguliers*, Mathematische Zeitschrift **202** (1989), no. 3, 343–365.
17. 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** (1975), no. 89, 116.
18. Ralph Greenberg, *On the iwasawa invariants of totally real number fields*, American Journal of Mathematics **98** (1976), no. 1, 263–284.
19. ———, *Galois representations with open image*, Ann. Math. Qué. **40** (2016), no. 1, 83–119. MR 3512524
20. Tuomas Hakkarainen, *On the computation of class numbers of real abelian fields*, Mathematics of Computation **78** (2009), no. 265, 555–573.
21. 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** (1974), no. 4, 276–278.
22. Tommy Hofmann and Yinan Zhang, *Valuations of p-adic regulators of cyclic cubic fields*, Journal of Number Theory **169** (2016), 86–102.
23. Christopher Hooley, *On artin's conjecture.*, Journal für die reine und angewandte Mathematik **225** (1967), 209–220.
24. 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** (1993), no. 2, 343–363.
25. Sigekatu Kuroda, *über die Klassenzahlen algebraischer Zahlkörper*, Nagoya Math. J. **1** (1950), 1–10. MR 0039759
26. Franz Lemmermeyer, *Kuroda's class number formula*, Acta Arith. **66** (1994), no. 3, 245–260. MR 1276992
27. Gunter Malle and Bernd Heinrich Matzat, *Inverse galois theory*, Springer Science & Business Media, 2013.
28. John C. Miller, *Class numbers in cyclotomic $\mathbb{Z}_p$-extensions*, J. Number Theory **150** (2015), 47–73. MR 3304606
29. Abbas Movahhedi, *Sur les p-extensions des corps p-rationnels*, Math. Nachr. **149** (1990), 163–176. MR 1124802
30. Abbas Movahhedi and Thong Nguyen-Quang-Do, *Sur l'arithmétique des corps de nombres p-rationnels*, Séminaire de Théorie des Nombres, Paris 1987–88, Progr. Math., vol. 81, Birkhäuser Boston, Boston, MA, 1990, pp. 155–200. MR 1042770
31. Peter N Panayi, *Computation of leopoldt's p-adic regulator.*, Ph.D. thesis, University of East Anglia, 1995.
32. Frédéric Pitoun and Firmin Varescon, *Computing the torsion of the p-ramified module of a number field*, Math. Comp. **84** (2015), no. 291, 371–383. MR 3266966
33. Odile Sauzet, *Theorie d'iwasawa des corps p-rationnels et p-birationnels*, manuscripta mathematica **96** (1998), no. 3, 263–273.
34. Oliver Schirokauer, *Discrete logarithms and local units*, Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences **345** (1993), no. 1676, 409–423.
35. Franciscus Jozef Van der Linden, *Class number computations of real abelian number fields*, Mathematics of Computation **39** (1982), no. 160, 693–707.
36. Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575
37. Peter J. Weinberger and Linda Preiss Rothschild, *Factoring polynomials over algebraic number fields*, ACM Transactions on Mathematical Software (TOMS) **2** (1976), no. 4, 335–350.

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