A note on p-rational fields and the abc-conjecture

Christian Maire, Marine Rougnant

A NOTE ON p-RATIONAL FIELDS AND THE ABC-CONJECTURE

by

Christian Maire & Marine Rougnant

Abstract. — In this short note we confirm the relation between the generalized abc-conjecture and the p-rationality of number fields. Namely, we prove that given $\mathrm{K}/\mathbb{Q}$ a real quadratic extension or an imaginary S_3-extension, if the generalized abc-conjecture holds in K, then there exist at least $c \log X$ prime numbers $p \leqslant X$ for which K is p-rational, here c is some nonzero constant depending on K. The real quadratic case was recently suggested by Böckle-Guiraud-Kalyanswamy-Khare.

Introduction

Let K be a number field and let p be a prime number. To simplify, we assume p odd. Denote by K_p the maximal pro-p-extension of K unramified outside p; put $G_p := \mathrm{Gal}(\mathrm{K}_p/\mathrm{K})$. By class field theory, the pro-p group G_p is finitely generated and one knows, since Shafarevich and Koch, that moreover G_p is finitely presented (meaning that $H^2(\mathrm{G}_p, \mathbb{F}_p)$ is finite). In fact, G_p may be pro-p free, for example when $\mathrm{K} = \mathbb{Q}$, or when K is an imaginary quadratic field (when $p > 3$) and p doesn't divide the class number of K, or when $\mathrm{K} = \mathbb{Q}(\zeta_p)$ for p regular primes, etc.
A number field K for which G_p is pro-p free is called *p-rational* ([**25**]). Observe that K is p-rational if and only if the Leopoldt conjecture holds for K at p and the torsion $\mathscr{T}_p$ of the abelianization G_p^{ab} of G_p is trivial (see [**28**], or [**27**, Chapter X, §3]).

The study of $\mathscr{T}_p$ and of the p-rationality started in the beginning of the 80's with Gras, Nguyen Quang Do, Movahhedi, Jaulent, and their students. Since the literature is rich: see for example [**24**], [**26**], [**14**], [**21**], [**25**], [**22**], [**31**], [**8**] etc. See also [**13**, Chapitre IV, §3 and §4] for a well-detailed presentation of $\mathscr{T}_p$, of the Leopoldt conjecture and of p-rational fields. In the spirit of our paper, let us mention here the works of Byeon [**5**]

2000 ***Mathematics Subject Classification.*** — 11R37, 11R23.
Key words and phrases. — p-rationals fields, abc-conjecture.

The authors thank Bruno Anglès for pointing them the work of Ichimura. They also thank Georges Gras for constructive observations, Jean-François Jaulent for encouragements, useful comments and the extremely attentive reading, Gebhard Böckle for the exchanges concerning [**4**] and Zakariae Bouazaoui for his interest in this work. They also want to thank the anonymous referees for their careful works and helpful remarks. The authors were partially supported by the ANR project FLAIR (ANR-17-CE40-0012). CM was also supported by the EIPHI Graduate School (ANR-17-EURE-0002).

and Assim-Bouazzaoui [**1**] where they showed the infiniteness of 3 and 5-rational real quadratic fields.
Let us also precise at this level that a recent series of papers in different topics in number theory showed the interest of p-rational fields: Goren [**7**], Greenberg [**16**], Böckle-Guiraud-Kalyanswamy-Khare [**4**], David-Pries [**6**], Hajir-Maire [**17**], Hajir-Maire-Ramakrishna [**18**], etc.

Assuming Leopoldt conjecture (for K at p), the p-rationality of K is therefore equivalent to the nullity of $\mathscr{T}_p$. Observe that $\mathscr{T}_p \simeq H^2(\mathrm{G}_p, \mathbb{Z}_p)^*$ for a cohomological point of view (see [**29**]). When the p-Sylow of the class group of K is trivial, the quantity $\mathscr{T}_p$ is isomorphic to the torsion of the quotient of the units of the p-adic completions K_v of K by the closure of the global units. Moreover, if we assume that no K_v contains the p-roots of the unity (which is always the case when $p > [\mathrm{K} : \mathbb{Q}] + 1$), then the triviality of $\mathscr{T}_p$ is equivalent to the triviality of the *normalized p-adic regulator* defined by Gras [**11**, Definition 5.1]. Recently, Gras [**9**], [**10**], Pitoun-Varescon [**30**], Barbulescu-Ray [**2**] published a series of papers more concentrated on the computations of $\mathscr{T}_p$, and on some heuristics. In [**12**, Conjecture 8.11], Gras proposed the following conjecture:

***Conjecture* (Gras).** — *Let* K *be a number field. Then for large p,* K *is p-rational.*

This conjecture is in the same spirit of the Wieferich prime numbers problem. Indeed, given an odd prime number p, to compute the p-valuation of $2^{p-1} - 1$ is equivalent to compute the normalized p-adic regulator of the 2-units of $\mathbb{Q}$. In particular, in this case the nontriviality of the normalized p-adic regulator is equivalent for p to verify the congruence $2^{p-1} \equiv 1 (\mathrm{mod}\ p^2)$.

In [**32**] Silverman showed how the Wieferich prime numbers are related to the *abc*-conjecture. Let us be more precise. Given an integer $\alpha \in \mathbb{Q}^\times \backslash \{\pm 1\}$, Silverman proved that if the *abc*-conjecture holds then as $X \to \infty$

$$\#\{\text{prime number } p,\ p \leqslant X,\ \alpha^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)\} \geqslant c \log X,$$

where $c > 0$ is some absolute constant. See also [**15**], and [**33**] for a generalization of Wieferich primes in number fields.

Observe now that the generalized *abc*-conjecture has already been used in the context of Iwasawa theory. Indeed in [**19**] Ichimura gave a relationship between the Greenberg conjecture and the *abc*-conjecture. A consequence of his work is that, for example, for any real quadratic field K if the generalized *abc*-conjecture holds in K, then the set of primes p for which K is p-rational, is infinite. See also [**4**].

The goal of our work is to precise the quantity of such primes p, greatly inspired by the computations of Silverman.

Our main result involves the isotypic subspaces $\mathscr{T}_p^\chi$ of $\mathscr{T}_p$. Let us observe here that the authors studied previously in [**23**] such cutting and the arithmetic consequences of the nullity of some $\mathscr{T}_p^\chi$.

Let $\mathrm{K}/\mathbb{Q}$ be a Galois extension of Galois group G. Let us fix an odd prime number $p \nmid \#\mathrm{G}$. For an irreducible $\mathbb{Q}_p$-character ψ of G, let $r_\psi(E_\mathrm{K})$ be the ψ-rank of $\mathbb{Q}_p \otimes E_\mathrm{K}$, where E_K denotes the units of the ring of integers $\mathscr{O}_\mathrm{K}$ of K. Let us also cut $\mathscr{T}_p$ by its isotypic subspaces $\mathscr{T}_p^\psi$, and denote by $r_\psi(\mathscr{T}_p)$ the ψ-rank of $\mathscr{T}_p$. Observe that, assuming Leopoldt conjecture, the number field K is p-rational if and only if $r_\psi(\mathscr{T}_p) = 0$ for all

irreducible $\mathbb{Q}_p$-characters ψ. Moreover we will see that for $p \gg 0$, $r_\psi(\mathscr{T}_p) \leqslant r_\psi(E_{\rm K})$ for all ψ.
We will then focus on some special units u of $E_{\rm K}$: we denote by $\mathbb{S}$ the set of algebraic integers $u \in \overline{\mathbb{Q}}$ having no conjugate on the unit circle.
Here we prove:

Theorem A. — *Let* $\rm K/\mathbb{Q}$ *be a Galois extension of Galois group* $\rm G$ *and let* χ *be an irreducible* $\mathbb{Q}$*-character of* $\rm G$ *such that the* χ*-component of* $\mathbb{Q} \otimes E_{\rm K}$ *contains some unit* $u \in \mathbb{S}$*. If the generalized abc-conjecture holds for* $\rm K$*, then as* $X \to \infty$

$$\#\{\text{prime number } p \leqslant X,\ r_\psi(\mathscr{T}_p) < r_\psi(E_{\rm K}) \text{ for some irred. } \mathbb{Q}_p\text{−char. } \psi|\chi\} \geqslant c \log X,$$

for some constant $c > 0$ *depending on* $\rm K$.

(Of course, in Theorem A one considers only prime numbers $p \nmid \#\rm G$.) As consequence we obtain the following result (the real quadratic case was suggested in [**4**]):

Corollary. — *Let* $\rm K/\mathbb{Q}$ *be a real quadratic field or an imaginary* S_3*-extension. If the generalized abc-conjecture holds for* $\rm K$*, then as* $X \to \infty$

$$\#\{\text{prime number } p \leqslant X,\ \text{K is } p\text{−rational}\} \geqslant c \log X,$$

for some constant $c > 0$ *depending on* $\rm K$.

Remark 1. — *It is well known that Leopoldt conjecture holds in the situations of Corollary, but we don't assume Leopoldt conjecture in Theorem A.*

Let us add one additionnal remark about the units in $\mathbb{S}$.

Remark 2. — *The following observations will be useful for us:*
- *an unit* $u \neq \pm 1$ *for which all the conjugates are real is in* $\mathbb{S}$*;*
- *every cubic field contains some unit* $u \in \mathbb{S}$*;*
- *Pisot numbers are in* $\mathbb{S}$*.*

See also [**3**] *on the abundance of Pisot units.*

Our work contains two sections. In the first one, we introduce the objects we need. In the second section, we give the proofs of our results.

1. The objects

We start with a Galois extension $\rm K/\mathbb{Q}$ of degree m and Galois group $\rm G$. We denote by $\rm N$ the norm in $\rm K/\mathbb{Q}$.
Let $\mathscr{O}_{\rm K}$ be the ring of integers of $\rm K$, $E_{\rm K}$ be the units of $\mathscr{O}_{\rm K}$, and $\mu_{\rm K}$ be the group of the roots of the unity of $\rm K$.

Let p be an *odd prime* number. In all that will follow, we suppose that:
(*i*) $p \nmid \#\rm G$,
(*ii*) p is unramified in $\rm K/\mathbb{Q}$,
(*iii*) p does not divide the class number $h_{\rm K}$ of $\rm K$.

One excludes this way only a *finite set* of prime numbers p. In particular, there exists an explicit prime number p_0 such that every $p > p_0$ satisfies (*i*), (*ii*) and (*iii*).

1.1. p-rational fields and isotypic components. —

1.1.1. Let S_p be the set of places of K above p. For $v \in S_p$, denote by K_v the completion of K at v, by $\mathscr{O}_v$ the ring of integers of K_v, and by π_v an uniformizer of K_v. Then the p-completion $\mathscr{E}_\mathrm{K} := \mathbb{Z}_p \otimes E_K$ of E_K embeds diagonally, via ι, in $\mathscr{U}_p := \prod_{v \in S_p} \mathscr{U}_v^1$, where $\mathscr{U}_v^1 := 1 + \pi_v \mathscr{O}_v$ is the group of principal units of K_v. Observe that here $\mathscr{U}_p \simeq \mathbb{Z}_p^m$. By p-adic class field theory (and due to the fact that $p \nmid h_\mathrm{K}$), the group G_p^{ab} is isomorphic to $\mathscr{U}_p/\iota(\mathscr{E}_\mathrm{K})$. Then, assuming Leopoldt conjecture for K at p (meaning here that ι is injective), the number field K is p-rational if and only if $\mathscr{U}_p/\iota(\mathscr{E}_\mathrm{K})$ is without torsion.

1.1.2. Observe that as p is unramified in $\mathrm{K}/\mathbb{Q}$, we also get that $p \nmid |\mu_\mathrm{K}|$, and as $p \nmid \#\mathrm{G}$, the character (as G-module) of $\mathscr{E}_\mathrm{K}$ is equal to the character of $\mathbb{Q}_p \otimes (\mathbb{Q} \otimes E_\mathrm{K}) \simeq \mathrm{Ind}_{D_\infty}^{\mathrm{G}} \mathbb{1}$, where D_∞ is the decomposition group of an archimedean place in $\mathrm{K}/\mathbb{Q}$ and where $\mathbb{1}$ is the trivial character. In particular, $\mathscr{E}_\mathrm{K}$ is a submodule of the regular representation.
To be complete, $\mathscr{U}_p$ is isomorphic to the regular representation (here $\mathscr{U}_v^1$ has no nontrivial root of unity).

1.1.3. Let us fix an irreducible $\mathbb{Q}$-character χ of G. Let $\mathbb{Q}[\mathrm{G}]e_\chi \simeq \mathrm{M}_{n_\chi}(D)$ be the simple algebra of $\mathbb{Q}[\mathrm{G}]$ associated to χ, where D is a skew field of degree s_χ^2 over its center (the integer s_χ is the Schur index of χ). Then $\chi = s_\chi \sum_{\psi|\chi} \psi$, where the sum is taken over irreducible $\mathbb{Q}_p$-characters ψ dividing χ (here $p \nmid \#\mathrm{G}$).
Let E_K^χ be the χ-component of the $\mathbb{Q}[\mathrm{G}]$-module $\mathbb{Q} \otimes E_\mathrm{K}$, then the character of E_K^χ is written as $t_\chi \chi$ for some $t_\chi \in \{0, \cdots, n_\chi\}$. Given an irreducible $\mathbb{Q}_p$-character $\psi|\chi$, the integer $s_\chi t_\chi$ is then the ψ-rank $r_\psi(E_\mathrm{K})$ of $\mathbb{Q}_p \otimes E_\mathrm{K}$.

If M is a $\mathbb{Z}_p[\mathrm{G}]$-module of finite type, the ψ-rank $r_\psi(M)$ of M is defined as $r_\psi(M) := \dfrac{1}{\deg(\psi)} \dim_{\mathbb{F}_p}(M^\psi/(M^\psi)^p)$.
As seen before $r_\psi(E_\mathrm{K}) = r_\psi(\mathscr{E}_\mathrm{K})$, obviously $r_\psi(\mathscr{E}_\mathrm{K}) \geqslant r_\psi(\iota(\mathscr{E}_\mathrm{K}))$, and Leopoldt conjecture is equivalent to the equality $r_\psi(\mathscr{E}_\mathrm{K}) = r_\psi(\iota(\mathscr{E}_\mathrm{K}))$ for every χ and ψ. Observe that one knows that $r_\psi(\iota(\mathscr{E}_\mathrm{K})) \geqslant 1$ when $r_\psi(\mathscr{E}_\mathrm{K}) \neq 0$ (see [**20**]).

Remark 1.1. — When G is abelian, one has $r_\psi(\mathscr{E}_\mathrm{K}) \leqslant 1$.

As seen before, with all the assumptions, the torsion of $\mathscr{U}_p/\iota(\mathscr{E}_\mathrm{K})$ is isomorphic to $\mathscr{T}_p$. Thus, $r_\psi(\mathscr{T}_p) \leqslant r_\psi(\mathscr{E}_\mathrm{K})$. If for every $\psi|\chi$ the ψ-rank of $\mathscr{U}_p/\iota(\mathscr{E}_\mathrm{K})$ is maximal, meaning $r_\psi(\mathscr{T}_p) = r_\psi(\mathscr{E}_\mathrm{K})$, then necessarily, for every unit $x \in E_\mathrm{K}^\chi$ such that $x \equiv 1 (\mathrm{mod}\ \mathfrak{p})$ for all $\mathfrak{p}|p$, one must have $x \equiv 1 (\mathrm{mod}\ \mathfrak{p}^2)$ for all $\mathfrak{p}|p$.

Lemma 1.2. — *If there exists an unit $u \in E_\mathrm{K}^\chi$ such that $u \equiv 1 (\mathrm{mod}\ \mathfrak{p}_0)$ but $u \not\equiv 1 (\mathrm{mod}\ \mathfrak{p}_0^2)$ for some $\mathfrak{p}_0|p$, then $r_\psi(\mathscr{T}_p) < r_\psi(\mathscr{E}_\mathrm{K})$ for some $\psi|\chi$.*

Proof. — Put $x = u^{\mathrm{N}(\mathfrak{p}_0)-1} \in E_\mathrm{K}^\chi$, where $\mathrm{N}(\mathfrak{p}) = \#\mathscr{O}_\mathrm{K}/\mathfrak{p}$. Observe that $x \equiv 1 (\mathrm{mod}\ \mathfrak{p})$ for every $\mathfrak{p}|p$ (the extension $\mathrm{K}/\mathbb{Q}$ is Galois) but, easily, one also has $x \not\equiv 1 (\mathrm{mod}\ \mathfrak{p}_0^2)$. We conclude with the small discussion above. ☐

1.2. The generalized *abc*-conjecture. — See [**34**]. If $I \subset \mathscr{O}_\mathrm{K}$ is an integral ideal, let us denote by $\mathrm{Rad}(I)$ the following ideal:

$$\mathrm{Rad}(I) = \prod_{\mathfrak{p}|I} \mathrm{N}(\mathfrak{p}),$$

where the product is taken over prime ideal $\mathfrak{p}$ dividing I and where as usual $\mathrm{N}(\mathfrak{p}) = \#\mathcal{O}_K/\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$.
The generalized *abc*-conjecture for K states that for any $\varepsilon > 0$, there exists a constant $C_{K,\varepsilon} > 0$ such that the inequality :

$$\prod_v \max\{|a|_v, |b|_v, |c|_v\} \leqslant C_{K,\varepsilon}\,(\mathrm{Rad}(abc))^{1+\varepsilon}$$

holds for all nonzero $a, b, c \in \mathcal{O}_K$ verifying $a + b = c$, $(a, b) = 1$, where the product is taken over all absolute values of K and where $|\cdot|_v$ denotes the normalized norm of K_v (such that $\prod_v |x|_v = 1$ for all $x \in \mathrm{K}^\times$).
Here we use it in the case where $b = u_2$ and $c = u_1$ are two distinct units of K and $a = u_1 - u_2$: for every $\varepsilon > 0$, there exists a constant $C_{\mathrm{K},\varepsilon}$ such that for all $u_1 \neq u_2 \in E_{\mathrm{K}}$, one has

$$|\mathrm{N}(u_1 - u_2)| \leqslant C_{\mathrm{K},\varepsilon}\mathrm{Rad}((u_1 - u_2))^{1+\varepsilon}.$$

2. Proofs

2.1. As explained in Introduction, some part of the proof is greatly inspired by [**32**].
Let $\mathrm{K}/\mathbb{Q}$ be a Galois extension of degree m. Consider the number field $\mathrm{L} := \mathrm{K}(\zeta)$ where ζ is a primitive nth-root of 1. The extension $\mathrm{L}/\mathbb{Q}$ is Galois of degree $O(\varphi(n))$.

Let T_n be the set of integers $j \in \{1, \cdots, n-1\}$ coprime to n. We denote by Φ_n the nth cyclotomic polynomial: $\Phi_n(u) = \prod_{j \in T_n}(u - \zeta^j)$. The polynomial Φ_n is of degree $\varphi(n)$.
Thereafter, we will focus on integer n such that $\varphi(n) \geqslant \frac{1}{2}n$. Recall Lemma 6 of [**32**]:

$$\#\{n \leqslant X, \varphi(n) \geqslant \frac{1}{2}n\} \geqslant (\frac{6}{\pi^2} - \frac{1}{2})\ X + O(\log X).$$

We start with the key lemma extending Lemma 5 of [**32**].

Lemma 2.1. — *Let $u \in E_{\mathrm{K}} \cap \mathbb{S}$. Then there exists some $k \in \mathbb{Z}_{>0}$ such that*

$$|\mathrm{N}(\Phi_n(u^k))| \geqslant \exp(cn),$$

for n such that $\varphi(n) \geqslant \frac{1}{2}n$, where $c > 0$ is a constant depending on u and k.

Proof. — As $u \in \mathbb{S}$, there exists an embedding $\sigma : \mathrm{K} \hookrightarrow \mathbb{C}$ such that $|\sigma(u)| \geqslant a > 1$, for some real a. Hence, for $k \in \mathbb{Z}_{>0}$, we get $|\sigma(u^k)| \geqslant a^k$, and then $|\sigma(u^k) - \zeta^j| \geqslant a^k - 1$.
Let us choose an another embedding τ. We want to give some "good" lower bound for $|\tau(u^k) - \zeta^j|$. As $u \in \mathbb{S}$ there is only two situations.

• If $|\tau(u)| < 1$, then clearly for sufficiently large k, we get

$$|\tau(u^k) - \zeta^j| \geqslant 1 - |\tau(u^k)| \geqslant \frac{1}{2}.$$

• If $|\tau(u)| > 1$, for sufficiently large k, we get $|\tau(u^k) - \zeta^j| \geqslant 1$.

Putting all of this together, we obtain

$$\mathrm{N}(\Phi_n(u^k)) = \prod_{i=1}^{m}\prod_{j \in T_n} |\sigma_i(u^k) - \zeta^j| \geqslant \left((a^k - 1)2^{-m+1}\right)^{\varphi(n)},$$

Consequently, by taking sufficiently large k, we get that for every n with $\varphi(n) \geqslant \frac{1}{2}n$

$$\mathrm{N}(\Phi_n(u^k)) \geqslant \exp(cn),$$

where the σ_i's are the embeddings of K in $\mathbb{C}$ and where $c > 0$ is some constant (depending on u, k and m). □

Suppose now that $u \in E_{\mathrm{K}}$ is such that

$$|\mathrm{N}(\Phi_n(u))| \geqslant \exp(cn),$$

for every n such that $\varphi(n) \geqslant \frac{1}{2}n$ (which is always possible by Lemma 2.1).
Let us write $(u^n - 1) = I_n J_n$, with I_n and J_n relatively prime and where if $\mathfrak{p}|I_n$, then $\mathfrak{p}^2 \nmid I_n$, and if $\mathfrak{p}|J_n$ then $\mathfrak{p}^2|J_n$. Then, if we write $u^n - 1 + 1 = u^n$, the generalized *abc*-conjecture implies that

$$|\mathrm{N}(u^n - 1)| \ll_{\mathrm{K},\varepsilon} \mathrm{Rad}(I_n J_n)^{1+\varepsilon} \ll_{\mathrm{K},\varepsilon} \left(\mathrm{N}(I_n)\mathrm{N}(J_n)^{1/2}\right)^{1+\varepsilon}.$$

Hence, as $|\mathrm{N}(u^n - 1)| = \mathrm{N}(I_n)N(J_n)$, we get

$$\mathrm{N}(J_n)^{1/2} \ll_{\mathrm{K},\varepsilon} \mathrm{N}(I_n)^{\varepsilon}\mathrm{N}(J_n)^{\varepsilon/2} \ll_{\mathrm{K},\varepsilon} |\mathrm{N}(u^n - 1)|^{\varepsilon},$$

and then

$$\mathrm{N}(J_n) \ll_{\mathrm{K},\varepsilon} |\mathrm{N}(u^n - 1)|^{2\varepsilon}.$$

Now let us also write $(\Phi_n(u)) = A_n B_n$, with A_n and B_n relatively prime and where if $\mathfrak{p}|A_n$, then $\mathfrak{p}^2 \nmid A_n$, and if $\mathfrak{p}|B_n$ then $\mathfrak{p}^2|B_n$. Of course, $B_n|J_n$, and then

$$\mathrm{N}(B_n) \ll_{\mathrm{K},\varepsilon} |\mathrm{N}(u^n - 1)|^{2\varepsilon}.$$

Choose $\beta > 1$ such that $|\sigma_i(u)| \leqslant \beta$ for all i. Then

$$|\mathrm{N}(u^n - 1)| \leqslant \prod_{i=1}^{m}(|\sigma_i(u)|^n + 1) \leqslant 2^m(\beta^m)^n,$$

which implies

$$\mathrm{N}(B_n) \ll_{\mathrm{K},\varepsilon} 2^{2m\varepsilon}(\beta^m)^{2n\varepsilon}.$$

Hence,

$$\mathrm{N}(A_n) = \mathrm{N}(\Phi_n(u))/\mathrm{N}(B_n) \gg_{\mathrm{K},\varepsilon} \exp(n(c - 2m\varepsilon\log\beta)).$$

We finally obtain:

Proposition 2.2. — *If the generalized abc-conjecture holds then for all $\varepsilon > 0$, one has*

$$\mathrm{N}(A_n) \gg_{\mathrm{K},\varepsilon} \exp(n(c - 2m\varepsilon\log\beta)),$$

for every n such that $\varphi(n) \geqslant \frac{1}{2}n$.

Take now $\varepsilon > 0$ such that $\varepsilon < \dfrac{c}{2m\log(\beta)}$. Thanks to Proposition 2.2, there exists $n_0 \in \mathbb{Z}_{>0}$ such that for all $n \geqslant n_0$, with $\varphi(n) \geqslant \frac{1}{2}n$, then $\mathrm{N}(A_n) > n^m$, where we recall that $m = [\mathrm{K} : \mathbb{Q}]$. Then, for each such n, there exists a prime ideal $\mathfrak{p}_n \subset \mathscr{O}_K$, dividing A_n but not n: indeed if it was not the case then as A_n is square free, A_n would divide n, which contradicts $\mathrm{N}(A_n) > n^m$. Observe that $\mathfrak{p}_n|(u^n - 1)$ implies $\mathrm{N}(\mathfrak{p}_n) \leqslant 2^m\beta^{mn}$.
As $\mathfrak{p}_n \nmid n$, the polynomial $X^n - 1$ is separable over $\mathscr{O}_K/\mathfrak{p}_n$. Thus u is a simple root of $X^n - 1 = \prod_{d|n}\Phi_d(X)$ modulo $\mathfrak{p}_n$ and, as $\mathfrak{p}_n$ divides $\Phi_n(u)$, its order in $(\mathscr{O}_{\mathrm{K}}/\mathfrak{p}_n)^{\times}$ is

exactly n. Furthermore, $\mathfrak{p}_n$ is a divisor of A_n, so $\mathfrak{p}_n^2$ does not divide $u^n - 1$ (in other words $\mathfrak{p}_n | I_n$).
Let p_n be the prime number such that $p_n\mathbb{Z} = \mathfrak{p}_n \cap \mathbb{Z}$.
In conclusion, we obtain:

Proposition 2.3. — *Take $u \in E_{\mathrm{K}}$ as before. For each $n \geqslant n_0$ such that $\varphi(n) \geqslant \frac{1}{2}n$, there exists a prime ideal $\mathfrak{p}_n \subset \mathscr{O}_{\mathrm{K}}$ such that*

(*i*) $\mathfrak{p}_n | \Phi_n(u)$ *and* $u^n \not\equiv 1 (\mathrm{mod}\ \mathfrak{p}_n^2)$,
(*ii*) *u is of order n in* $(\mathscr{O}_{\mathrm{K}}/\mathfrak{p}_n)^{\times}$,
(*iii*) $\mathrm{N}(\mathfrak{p}_n) \leqslant \gamma^n$, *for some γ depending only on* K.

By (*ii*) of Proposition 2.3, it follows that $\mathfrak{p}_n = \mathfrak{p}_{n'}$ if and only if $n = n'$. Observe that a set of primes $\mathfrak{p}_n$ of size Y gives at least Y/m primes p_n.
Now given $X \geqslant 1$, let n_1 be the largest integer such that $\gamma^{n_1} \leqslant X$. Assume X sufficiently large to ensure $n_0 \leqslant n_1$. Then, for each $n \in [n_0, n_1]$ such that $\varphi(n) \geqslant \frac{1}{2}n$, there exists a prime ideal $\mathfrak{p}_n \subset \mathscr{O}_{\mathrm{K}}$ for which $u^n \equiv 1 (\mathrm{mod}\ \mathfrak{p}_n)$ and $u^n \not\equiv 1 (\mathrm{mod}\ \mathfrak{p}_n^2)$. Note that $p_n \leqslant \mathrm{N}(\mathfrak{p}_n) \leqslant \gamma^n \leqslant \gamma^{n_1} \leqslant X$. Thereby:

$$\frac{1}{m}\#\{n,\ n_0 \leqslant n \leqslant n_1,\ \varphi(n) \geqslant \frac{1}{2}n\}$$
$$\leqslant \#\{p_n \leqslant X, p_n \text{ prime} \mid \exists\ \mathfrak{p}_n \in \mathscr{O}_k, \mathfrak{p}_n | p_n, u^n \equiv 1 (\mathrm{mod}\ \mathfrak{p}_n) \text{ and } u^n \not\equiv 1 (\mathrm{mod}\ \mathfrak{p}_n^2)\}.$$

In conclusion, one has found at least $c\ \log X$ prime numbers $p_n \leqslant X$ satisfying (*i*) of Proposition 2.3 for some $\mathfrak{p}_n | p_n$.

2.2. *Proof of Theorem A.* Let χ be an irreducible $\mathbb{Q}$-character of G such that there exists some $u \in E_{\mathrm{K}}^{\chi} \cap \mathbb{S}$. By the previous section, there exists $k \geqslant 1$ such that $u^{kn} \equiv 1 (\mathrm{mod}\ \mathfrak{p}_n)$ and $u^{kn} \not\equiv 1 (\mathrm{mod}\ \mathfrak{p}_n^2)$ for at least $c\ \log X$ prime numbers $p_n \leqslant X$ (where $\mathfrak{p}_n | p_n$). We conclude with Lemma 1.2 (after forgetting the prime numbers smaller than p_0).

Proof of the Corollary.
Observe first that, in the two cases, the Leopoldt conjecture holds and the field K contains some unit in $\mathbb{S}$ (see Remark 2). Take $p > p_0$. The choice of the character is the following : if K is real quadratic, let $\chi = \psi$ be the nontrivial character of G ; if $\mathrm{K}/\mathbb{Q}$ is an imaginary S_3-extension, let χ be the irreducible $\mathbb{Q}$-character of G of degree 2 (observe that $\chi = \psi$ is also $\mathbb{Q}_p$-irreducible). Then $\mathbb{Q} \otimes E_{\mathrm{K}} = E_{\mathrm{K}}^{\chi}$, $r_{\psi}(E_{\mathrm{K}}) = 1$, and $\mathscr{T}_p = \mathscr{T}_p^{\psi}$. Therefore by Theorem A, $\mathscr{T}_p = \{1\}$ for at least $c\ \log X$ prime numbers $p \leqslant X$.

References

[1] J. Assim, Z. Bouazzaoui, *Half-integral weight modular forms and real quadratic p-rational fields*, 2018, arXiv:1906.03344.

[2] R. Barbulescu and J. Ray, *Some remarks and experiments on Greenberg's p-rationality conjecture*, 2017, arXiv:1706.04847.

[3] M.-J. Bertin, T. Zaïmi, *Complex Pisot numbers in algebraic number fields*, C. R. Acad. Sci. Paris, Ser. I **353** (2015), 965-967.

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

[5] D. Byeon, *Indivisibility of special values of Dedekind zeta functions of real quadratic fields*, Acta Arithmetica **109** (2003), no. 3, 231-235.

[6] R. David, R. Pries, *Cohomology groups of Fermat curves via ray class fields of cyclotomic fields*, 2018, arXiv:1806.08352.

[7] E. Z. Goren, *Hasse invariants for Hilbert modular varieties*, Israel Journal of Mathematics **122** (2001), 157-174.

[8] G. Gras, *Practice of incomplete p-ramification over a number field – History of abelian p-ramification*, 2019, arXiv:1904.10707.

[9] G. Gras, *Heuristics in direction of a p-adic Brauer–Siegel theorem*, Mathematics of Computation **88** (2019), no. 318, 1929-1965.

[10] G. Gras, *On p-rationality of number fields. Applications – PARI/GP programs*, Publ. Math. Besançon (Théorie des Nombres), Années 2017/2018, to appear, arXiv:1709.06388.

[11] G. Gras, *The p-adic Kummer-Leopoldt Constant - Normalized p-adic Regulator*, International Journal of Number Theory **14** (2018), no. 2, 329-337.

[12] G. Gras, *Les Θ-régulateurs locaux d'un nombre algébrique : Conjectures p-adiques*, Canadian Journal of Mathematics **68** (2016), 571-624.

[13] G. Gras, Class Field Theory, From Theory to practice, corr. 2nd ed., Springer Monographs in Mathematics, Springer (2005), xiii+507 pages.

[14] G. Gras and J.-F. Jaulent, *Sur les corps de nombres réguliers*, Mathematische Zeitschrift **202** (1989), 343- 365.

[15] H. Graves, R. Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions*, Journal of Number Theory **133** (2013), no. 6, 1809–1813.

[16] R. Greenberg, *Galois representations with open image*, Annales Mathématiques du Québec **40** (2016), no. 1, 83-119.

[17] F. Hajir, C. Maire, *Prime decomposition and the Iwasawa mu-invariant*, Mathematical Proceedings of the Cambridge Philosophical Society, to appear.

[18] F. Hajir, C. Maire, R. Ramakrishna, *Cutting towers of number fields*, 2019, arXiv:1901.04354.

[19] H. Ichimura, *A note on Greenberg's conjecture and the abc conjecture*, Proceedings of the American Math. Society **126** (1998), no. 5, 1315-1320.

[20] J.-F. Jaulent, *Sur l'indépendance ℓ-adique de nombres algébriques*, Journal of Number Theory **20** (1985), 149-158.

[21] J.-F. Jaulent and T. Nguyen Quang Do, *Corps p-réguliers, corps p-rationnels et ramification restreinte*, Journal de Théorie des Nombres de Bordeaux **5** (1993), 343-363.

[22] J.-F. Jaulent, O. Sauzet, *Pro-ℓ-extensions de corps de nombres ℓ-rationnels*, Journal of Number Theory **65** (1997), 240-267.

[23] C. Maire, M. Rougnant, *Composantes isotypiques de pro-p-extensions de corps de nombres et p-rationalité*, Publicationes Mathematicae Debrecen **94** 1/2 (2019), 123-155.

[24] A. Movahhedi and T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p-rationnels*, Séminaire de Théorie des Nombres, Paris 1987–88, 155–200, Progr. Math., 81, Birkhäuser Boston, Boston, MA, 1990.

[25] A. Movahhedi, *Sur les p-extensions des corps p-rationnels*, PhD Université Paris VII, 1988.

[26] A. Movahhedi, *Sur les p-extensions des corps p-rationnels*, Mathematische Nachrichten **149** (1990), 163–176.

[27] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of Number Fields, GMW 323, Springer-Verlag Berlin Heidelberg, 2000.

[28] T. Nguyen Quang Do, *Sur la structure galoisienne des corps locaux et de la théorie d'Iwasawa*, Compositio Mathematica **46** (1982), no. 1, 85-119.

[29] T. Nguyen Quang Do, *Sur la $\mathbb{Z}_p$-torsion de certains modules galoisiens*, Annales Institut Fourier **36** (1986), no. 2, 27-46.

[30] F. Pitoun and F. Varescon, *Computing the torsion of the p-ramified module of a number field*, Mathematics of Computation **84** (2015), no. 291, 371-383.

[31] O. Sauzet, *Théorie d'Iwasawa des corps p-rationnels et p-birationnels*, Manuscripta Math. **96** (1998), no. 3, 263–27.

[32] J.H. Silverman, *Wieferich's Criterion and the abc-Conjecture*, Journal of Number Theory **30** (1988), 226-237.

[33] K. Sirinas, M. Subramani, *Non-Wieferich primes in number fields and abc-conjecture*, Czechoslovak Mathematical Journal **68** no 2 (2018), 445-453.

[34] P. Vojta, *A more general ABC conjecture*, International Math. Research Notices **21** (1998), 1103–1116.

June 22, 2019

Christian Maire, FEMTO-ST Institute, Université Bourgogne Franche-Comté, 15B Avenue des Montboucons, 25030 Besançon Cedex, France • *E-mail :* `christian.maire@univ-fcomte.fr`

Marine Rougnant, Laboratoire de Mathématiques de Besançon, Université Bourgogne Franche-Comté, UFR Sciences et Techniques, 16 route de Gray, 25030 Besançon Cedex, France
E-mail : `marine.rougnant@univ-fcomte.fr`