Publ. Math. Debrecen
91/1-2 (2017), 153–170
DOI: 10.5486/PMD.2017.7726

Non-Galois cubic number fields with exceptional units

By STÉPHANE R. LOUBOUTIN (Marseille)

To Catherine H.

Abstract. We consider the family of non-normal totally real cubic number fields $\mathbb{K}_l$ associated with the $\mathbb{Q}$-irreducible cubic polynomials $f_l(X) = X^3 + (l-1)X^2 - lX - 1 \in \mathbb{Z}[X]$, $l \geq 3$. Let ε_l be a root of $f_l(X)$. Then ε_l and $\varepsilon_l - 1$ are units of $\mathbb{K}_l$. Let j_l denote the index of the groups of units generated by -1, ε_l and $\varepsilon_l - 1$ in the group of units $\mathbb{U}_l$ of the ring of algebraic integers of $\mathbb{K}_l$. V. Ennola proved in 1991 (i) that $\gcd(j_l, 2\cdot 3\cdot 5) = 1$ for $l \geq 3$, (ii) that $j_l = 1$ for $3 \leq l \leq 500$, and (iii) he conjectured that $j_l = 1$ for $l \geq 3$. We prove (i) that $\gcd(j_l, 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19) = 1$ for $l \geq 3$, and (ii) that $j_l = 1$ for $3 \leq l \leq 5\cdot 10^7$, thus adding a lot more credit to this conjecture.

1. Introduction and statements of the results

A unit η of an algebraic number field $\mathbb{K}$ is called *exceptional* if $\eta - 1$ is also a unit. In that case, the units η, $1-\eta$, η^{-1}, $(1-\eta)^{-1}$, $1-\eta^{-1}$ and $\eta(\eta-1)^{-1}$ are also exceptional. From now on, we assume that $\mathbb{K}$ is a cubic number field of discriminant $d_{\mathbb{K}}$ and ring of algebraic integers $\mathbb{Z}_{\mathbb{K}}$. One can immediately verify that there are exactly two families of cubic fields containing exceptional units, namely,

$$\begin{aligned} \mathbb{K}_l &= \mathbb{Q}(\varepsilon_l), \quad \mathrm{Irr}(\varepsilon_l, \mathbb{Q}) = f_l(X) = X^3 + (l-1)X^2 - lX - 1, \\ \mathbb{L}_k &= \mathbb{Q}(\tau_k), \quad \mathrm{Irr}(\tau_k, \mathbb{Q}) = g_k(X) = X^3 + kX^2 - (k+3)X + 1, \end{aligned}$$

Mathematics Subject Classification: 11R16, 11R27.
Key words and phrases: units, exceptional units, cubic number fields, unit index.

for some integers l, k. The discriminants are

$$D_l = (l^2+3l-1)^2 - 32, \quad D_k = (k^2+3k+9)^2.$$

Hence, $\mathbb{L}_k/\mathbb{Q}$ is always cyclic, whereas $\mathbb{K}_l/\mathbb{Q}$ is non-Galois for $l \neq 2$.

As in [2], throughout this paper, we focus on the totally real cubic number fields $\mathbb{K}_l$'s with $l \geq 3$ (see [6] for some arithmetical problems related to this family). V. Ennola conjectured that $\{\varepsilon_l, \varepsilon_l - 1\}$ is a fundamental pair of units for the maximal order $\mathbb{Z}_{\mathbb{K}_l}$ of $\mathbb{K}_l$ for $l \geq 3$. He checked numerically that his conjecture holds true for $3 \leq l \leq 500$, and supported it by proving that the unit index

$$j_l := (\mathbb{U}_l : \langle -1, \varepsilon_l, \varepsilon_l - 1\rangle)$$

of the groups of units generated by -1, ε_l and $\varepsilon_l - 1$ in the group of units $\mathbb{U}_l$ of the ring of algebraic integers $\mathbb{Z}_{\mathbb{K}_l}$ of $\mathbb{K}_l$ is always coprime to 2, 3 and 5 for $l \geq 3$. Our aim in the present paper is to add a lot more credit to Ennola's conjecture by greatly improving upon this result:

Theorem 1. *The unit index j_l is coprime to $2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19$ for $l \geq 3$, and $j_l = 1$ for $3 \leq l \leq 5\cdot 10^7$.*

We point out that by extending the range of validity of Proposition 15, thanks to some more easy but time consuming numerical computation, it would be rather easy to improve upon Theorem 1 by taking into account few of the next prime integers $23, 29, \dots$. We also point out that the present development of V. Ennola's method could also be applied to other families of number fields and used to add some credit to [5, Conjecture 3].

By [9, Proposition (3.6)], for $l \geq 3$, the set $\{\varepsilon_l, \varepsilon_l - 1\}$ is a system of fundamental units of the totally real cubic order $\mathbb{Z}[\varepsilon_l]$. Indeed, if $P_n(X) = X^3 - (n-1)X^2 + nX - 1$, as in [9, Proposition (3.6)], then $X^3 P_{l+4}(1-1/X) = X^3 + (l-1)X^2 - lX - 1$. Hence, $\lambda = 1 - 1/\varepsilon_l$ and $\lambda - 1 = -1/\varepsilon_l$ are fundamental units of $\mathbb{Z}[\lambda] = \mathbb{Z}[\varepsilon_l]$, i.e., ε_l and $\varepsilon_l - 1$ are fundamental units of $\mathbb{Z}[\varepsilon_l]$. Using Theorem 1 which enables us to take $\alpha = 2 - 2/\sqrt{23} = 1.58297\cdots$ in Theorem 2, we obtain a much better result:

Theorem 2. *Let $p_0 \geq 5$ be a given prime integer such that $\gcd(p, j_l) = 1$ for $2 \leq p < p_0$ and $l \geq 3$. Set $\alpha = 2 - 2/\sqrt{p_0}$. Let $\mathbb{M}$ be an order of $\mathbb{K}_l$ containing $\mathbb{Z}[\varepsilon_l]$, and such that the index $(\mathbb{M} : \mathbb{Z}[\varepsilon_l])$ is less than or equal to $l^\alpha/2$. Then $\{\varepsilon_l, \varepsilon_l - 1\}$ is a system of fundamental units of $\mathbb{M}$.*

Proof. It is easy to see that for $l \geq 3$ the three conjugates of ε_l satisfy

$$-l < \varepsilon_l < -l + \frac{1}{l^2} < -1 < -\frac{1}{l} < \varepsilon_l' < -\frac{1}{l} + \frac{1}{l^2} < 0 < 1 < \varepsilon_l'' < 1 + \frac{1}{l}. \quad (1)$$

Hence, the regulator

$$\begin{aligned}\operatorname{Reg}(\varepsilon_l, \varepsilon_l - 1) &:= \left|\det\begin{pmatrix}\log|\varepsilon_l| \log|\varepsilon_l - 1| \\ \log|\varepsilon_l'| \log|\varepsilon_l' - 1|\end{pmatrix}\right| \\ &= (\log|\varepsilon_l|)(\log|\varepsilon_l' - 1|) + (-\log|\varepsilon_l'|)(\log|\varepsilon_l - 1|)\end{aligned}$$

is positive, ε_l and ε_l' are multiplicatively independent and

$$\operatorname{Reg}(\varepsilon_l, \varepsilon_l - 1) < f_1(l) := (\log l)\left(\log\left(1 + \frac{1}{l}\right)\right) - \left(\log\left(\frac{1}{l} - \frac{1}{l^2}\right)\right)(\log(l+1)).$$

Set $f_2(l) := \left(\log l + \frac{3}{2l}\right)^2$. We have $f_2(l) - f_1(l) = f_3(1/l)$, where $f_3(x) := u(x)\log x + v(x)$ with $u(x) = 2\log(1+x) - \log(1-x) - 3x$ and $v(x) = \frac{9}{4}x^2 + (\log(1-x))(\log(1+x))$. Now, (i) $u'(x) = x(3x-1)/(1-x^2) \leq 0$ for $0 \leq x \leq 1/3$ yields $u(x) \leq u(0) = 0$ and $u(x)\log(x) \geq 0$ for $0 \leq x \leq 1/3$, and (ii) $0 < -\log(1-x) \leq x + x^2$ for $0 \leq x \leq 1/2$ and $0 \leq \log(1+x) \leq x$ for $x \geq 0$ yield $v(x) \geq \frac{9}{4}x^2 - x(x+x^2) = x^2(5/4 - x) \geq 0$ for $0 \leq x \leq 1/2$. Hence, for $l \geq 3$, we obtain $f_3(1/l) \geq 0$ and $f_1(l) \leq f_2(l)$, i.e.,

$$\operatorname{Reg}(\varepsilon_l, \varepsilon_l - 1) < \left(\log l + \frac{3}{2l}\right)^2. \tag{2}$$

Let $\mathbb{U}_{\mathbb{M}}$ be the group of units of $\mathbb{M}$. By [1], there exists a unit $\varepsilon \in \mathbb{M}$ such that

$$\operatorname{Reg}(\mathbb{U}_{\mathbb{M}}) \geq \frac{1}{16}\log^2(d_\varepsilon/4) \geq \frac{1}{16}\log^2(d_{\mathbb{M}}/4),$$

where d_ε is the absolute value of the discriminant of the minimal polynomial of ε. Noticing that $d_{\mathbb{M}} = D_l/(\mathbb{M} : \mathbb{Z}[\varepsilon_l])^2 \geq 4D_l/l^{2\alpha}$ and using (2), we have

$$(\mathbb{U}_{\mathbb{M}} : \langle -1, \varepsilon_l, \varepsilon_l - 1\rangle) = \frac{\operatorname{Reg}(\varepsilon_l, \varepsilon_l - 1)}{\operatorname{Reg}(\mathbb{U}_{\mathbb{M}})} \leq \frac{\operatorname{Reg}(\varepsilon_l, \varepsilon_l - 1)}{\frac{1}{16}\log^2(d_{\mathbb{M}}/4)} < \left(\frac{\log l + \frac{3}{2l}}{\frac{1}{4}\log(D_l/l^{2\alpha})}\right)^2,$$

by [10, Lemma 4.15]. Now, it is easy to prove that

$$D_l = (l^2 + 3l - 1)^2 - 32 > l^4 \exp(3/l) > l^4 \exp\left(\frac{6/\sqrt{p_0}}{l}\right) \quad (l \geq 3).$$

Hence,

$$\frac{1}{4}\log(D_l/l^{2\alpha}) > \frac{1}{\sqrt{p_0}}\left(\log l + \frac{3}{2l}\right),$$

and $(\mathbb{U}_{\mathbb{M}} : \langle -1, \varepsilon_l, \varepsilon_l - 1\rangle) < p_0$.

Now, $\mathbb{Z}[\varepsilon_l] \subseteq \mathbb{M} \subseteq \mathbb{Z}_{\mathbb{K}_l}$ yields $\langle -1, \varepsilon_l, \varepsilon_l - 1\rangle \subseteq \mathbb{U}_{\mathbb{M}} \subseteq \mathbb{U}_l$. Hence, the unit index $(\mathbb{U}_{\mathbb{M}} : \langle -1, \varepsilon_l, \varepsilon_l - 1\rangle)$, which divides the unit index j_l, is also coprime to all the prime numbers less than p_0, and is therefore equal to 1. $\square$

In [3, Theorem, page 570], V. Ennola proved that Theorem 2 holds with the weaker bound $l/3$. In [4, Theorem 1.1], using the fact that the unit index j_l is coprime to 30, we proved that it holds true with the better but still weaker bound $l^\alpha/4$, where $\alpha = 2 - 2/\sqrt{7} = 1.244\cdots$.

Remark 3. Roughly speaking, we can reformulate Theorem 2 in the following way (see the proof of Proposition 15): let Δ_l be the square-free part of D_l (i.e., Δ_l is square-free and $D_l = \Delta_l f^2$ for some $f \geq 1$), then $\Delta_l \geq 16 l^{4/\sqrt{p_0}}$ implies that $\{\varepsilon_l, \varepsilon_l - 1\}$ is a system of fundamental units of the maximal order $\mathbb{Z}_{\mathbb{K}_l}$ of $\mathbb{K}_l$. Now, by Siegel's theorem, Δ_l goes to infinity as l goes to infinity. If there existed some explicit $\tau > 0$ such that $\Delta_l \gg l^\tau$, then by extending the validity of Theorem 1 up to a prime p_0 such that $4/\sqrt{p_0} < \tau$, we would obtain that $\{\varepsilon_l, \varepsilon_l - 1\}$ is a system of fundamental units of the maximal order $\mathbb{Z}_{\mathbb{K}_l}$ of $\mathbb{K}_l$ for l explicitly large enough. Of course, we are very far from knowing the existence of such a positive τ (e.g., see [8, (2.10), page 161] which gives only $\Delta_l \gg (\log l)^\tau$ for some explicit $\tau > 0$).

The remaining of this paper is devoted to proving Theorem 1.

Throughout the paper, we will freely use the following facts:

(i) If α, α' and α'' are the three conjugates of an algebraic integer $\alpha \in \mathbb{K}_l$ and $p \geq 3$ is a prime number, then

$$\mathrm{Tr}(\alpha) := \alpha + \alpha' + \alpha'' \in \mathbb{Z} \quad \text{and} \quad \mathrm{Tr}(\alpha^p) \equiv \mathrm{Tr}(\alpha)^p \equiv \mathrm{Tr}(\alpha) \pmod{p}. \tag{3}$$

(ii) If $\mathrm{Irr}(\varepsilon, \mathbb{Q}) = X^3 - sX^2 + tX - 1 \in \mathbb{Z}[X]$ is the minimal polynomial of a cubic algebraic unit of norm $+1$, then $s = \mathrm{Tr}(\varepsilon)$ and $t = \mathrm{Tr}(\varepsilon^{-1})$.

(iii) If $\varepsilon := \varepsilon_l^a(\varepsilon_l - 1)^b = A + B\varepsilon_l + C\varepsilon_l^2$ with $A, B, C \in \mathbb{Z}$, then

$$\mathrm{Irr}(\varepsilon, \mathbb{Q}) = \mathrm{Resultant}(X^3 + (l-1)X^2 - lX - 1, Y - (A + BX + CX^2), X) \tag{4}$$

is easy to compute.

2. The unit index j_l is odd and the units ε_l, $\varepsilon_l - 1$ and $\varepsilon_l^{p-1}(\varepsilon_l - 1)$ are not p-th powers

Using Lemmas 5, 6 and 7 below, the aim of this section is to prove:

Proposition 4. *Assume that $l \geq 3$. The unit index j_l is odd. Moreover, an odd prime number $p \geq 3$ divides j_l if and only if one of the $p-2$ units $\varepsilon_l^k(\varepsilon_l - 1)$ is a p-th power in $\mathbb{K}_l := \mathbb{Q}(\varepsilon_l)$, where $1 \leq k \leq p-2$.*

Lemma 5. *Let $\mathbb{Z}_{\mathbb{K}}^*$ be the group of units of the ring of algebraic integers $\mathbb{Z}_{\mathbb{K}}$ of a totally real cubic number field $\mathbb{K}$. Let ε_1 and ε_2 be two multiplicatively independent units of $\mathbb{Z}_{\mathbb{K}}$. A prime $p \geq 3$ divides the unit index $(\mathbb{Z}_{\mathbb{K}}^* : \langle -1, \varepsilon_1, \varepsilon_2 \rangle)$ if and only if ε_1 or one of the $\varepsilon_1^k \varepsilon_2$, $0 \leq k \leq p-1$, is a p-th power in $\mathbb{Z}_{\mathbb{K}}$. The prime $p = 2$ divides the unit index $(\mathbb{Z}_{\mathbb{K}}^* : \langle -1, \varepsilon_1, \varepsilon_2 \rangle)$ if and only if $\pm\varepsilon_1$, $\pm\varepsilon_2$ or $\pm\varepsilon_1/\varepsilon_2$ is both totally positive and a square in $\mathbb{Z}_{\mathbb{K}}$.*

Proof. Notice that $\varepsilon_1^a \varepsilon_2^b$, with a or b not divisible by p, is a p-th power if and only if $\varepsilon_1^{ka} \varepsilon_2^{kb}$ is a p-th power for any k coprime to p. Hence, we may assume that $b = 0$ and $1 \leq a \leq p-1$, or that $b = 1$ and $0 \leq a \leq p-1$. □

Lemma 6 (see [2, Proof of Proposition 3.3]). *The unit index j_l is odd for $l \geq 3$.*

Proof. By (1), the units ε_l and $\varepsilon_l - 1$ are of signature $(-,-,+)$ (two negative conjugates and one positive conjugate), and it remains to prove that $\varepsilon := \varepsilon_l/(\varepsilon_l - 1) = \varepsilon_l^2 + l\varepsilon_l + 1$ is not a square in $\mathbb{K}_l$. Suppose that $\varepsilon = \eta^2$. We may suppose that $N(\eta) = +1$, and hence that $\operatorname{Irr}(\eta, \mathbb{Q}) = X^3 - sX^2 + tX - 1 \in \mathbb{Z}[X]$. We get $X^3 - (l+4)X^2 + (l+3)X - 1 = \operatorname{Irr}(\varepsilon_l^2 + l\varepsilon_l + 1, \mathbb{Q}) = \operatorname{Irr}(\eta^2, \mathbb{Q}) = X^3 - (s^2 - 2t)X^2 + (t^2 - 2s)X - 1$, by (4). Hence, $1 = (l+4) - (l+3) = (s^2 - 2t) - (t^2 - 2s) = (s+t+2)(s-t)$, hence $s + t + 2 = s - t = \pm 1$, hence $t = -1$, $s = -1 \pm 1 = -2, 0$ and $l = s^2 - 2t - 4 = 2, -2$, a contradiction. □

Lemma 7 (see [2, Lemma 4.1 and top of page 111]). *Let $p \geq 3$ be an odd prime number. An exceptional unit in an arbitrary totally real number field $\mathbb{K}$ is never a p-th power in $\mathbb{K}$. In particular, ε_l, $\varepsilon_l - 1$ and $\varepsilon_l^{p-1}(\varepsilon_l - 1)$ are not p-th powers in $\mathbb{K}_l$ for $l \geq 3$.*

Proof. First, $1 - \varepsilon_l$ being exceptional, it is not a p-th power in $\mathbb{K}_l$, hence neither is $\varepsilon_l - 1 = -(1 - \varepsilon_l)$. Second, $\varepsilon_l/(\varepsilon_l - 1)$ being exceptional, it is not a p-th power in $\mathbb{K}_l$, hence neither is $\varepsilon_l^{p-1}(\varepsilon_l - 1) = \varepsilon_l^p(\varepsilon_l - 1)/\varepsilon_l$. □

3. The unit index j_l is coprime to $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ for $3 \leq l \leq 10^5$

We now use Proposition 4 to numerically prove in Proposition 9 that the unit index j_l is coprime to $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ for $3 \leq l \leq 10^5$. For $\pm 1 \neq \varepsilon \in \mathbb{U}_l$, let ε, ε' and ε'' be its three conjugates. We set

$$S_{a,b,p}(l) := \varepsilon^{1/p} + \varepsilon'^{1/p} + \varepsilon''^{1/p}, \qquad \text{where } \varepsilon = \varepsilon_l^a(\varepsilon_l - 1)^b. \tag{5}$$

Letting θ stand for an effective real number such that $0 \le \theta \le 1$, not necessarily the same at different places, the three conjugates of ε_l satisfy

$$\begin{aligned} \varepsilon_l &= -l(1-\theta l^{-2}), & \varepsilon_l - 1 &= -l\left(1+l^{-1}-\theta l^{-2})\right), \\ \varepsilon_l' &= -l^{-1}(1-l^{-1}+3\theta l^{-2}), & \varepsilon_l' - 1 &= -(1+l^{-1}-\theta l^{-2}), \\ \varepsilon_l'' &= 1+l^{-1}-2\theta l^{-2}, & \varepsilon_l'' - 1 &= l^{-1}(1-2l^{-1}+4\theta l^{-2}). \end{aligned}$$

Hence, we obtain:

Lemma 8. *If $p \ge 3$ and $l \ge 3$ vary in such a way that $w := l^{1/p}$ goes to infinity, then with an effective implicit constant we have:*

$$\begin{aligned} S_{a,b,p}(l) = (-1)^{a+b}w^{a+b} + (-1)^{a+b}w^{-a} + w^{-b} + \frac{1}{p}\big((-1)^{a+b}bw^{a+b-p} \\ +(-1)^{a+b}(b-a)w^{-a-p} + (a-2b)w^{-b-p}\big) + O(w^{\max(a+b,-a,-b)-2p}). \end{aligned}$$

Proposition 9. *The unit index j_l is coprime to $2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19$ for $3 \le l \le 10^5$.*

Proof. Set $d(x,\mathbb{Z}) := \min_{n\in\mathbb{Z}} |x-n|$, and

$$m(B) := \min_{3\le l\le B}\ \min_{3\le p\le 19}\ \min_{1\le k\le p-2}\ \min(d(S_{k,1,p}(l),\mathbb{Z}), d(S_{-k,-1,p}(l),\mathbb{Z})).$$

By Proposition 4, if some $p \in \{2,3,\dots,19\}$ divides j_l for some l in the range $3 \le l \le B$, then some $\varepsilon_l^k(\varepsilon_l - 1)$ is a p-th power in $\mathbb{K}_l$ for some $p \in \{3,\dots,19\}$, some $k \in \{1,\dots p-2\}$ and some l in the range $3 \le l \le B$, which implies $S_{k,1,p}(l) \in \mathbb{Z}$, $S_{-k,-1,p}(l) \in \mathbb{Z}$ and $m(B) = 0$. Now, recall that if all the roots of $P(X) = X^3 - aX^2 + bX - c \in \mathbb{R}[X]$ are real, then its discriminant $d_{P(X)}$ is positive, $P(X+a/3) = X^3 - 3BX - C$, where $B = (a^2-3b)/9$ and $C = (2a^3 - 9ab + 27c)/27$, $d_{P(X)} = 27(4B^3 - C^2)$, and the three real roots of $P(X)$ are

$$\frac{a}{3} + 2\frac{C}{|C|}\sqrt{B}\cos\left(\frac{1}{3}\arctan\left(\sqrt{\frac{d_{P(X)}}{27C^2}}\right) - \frac{2k\pi}{3}\right) \quad (0 \le k \le 2). \tag{6}$$

This enables us to efficiently compute numerically $S_{k,1,p}(l)$ and $S_{-k,-1,p}(l)$. Now, an easy numerical computation on a microcomputer yields $m(10^5) = 6.92479(\cdots)\cdot 10^{-12}$ and $m(10^5) \ne 0$ (we did our computation using Maple with a more than enough precision of 70 digits). $\square$

4. The primes 3 and 5 do not divide the unit index j_l

Using Proposition 4 and Lemmas 11, 12 and 14 below, the aim of this section is to prove:

Proposition 10. *Assume that $l \geq 3$. The prime numbers 2 and 3 never divide the unit index j_l, and an odd prime number $p \geq 5$ divides j_l if and only if one of the $p-4$ units $\varepsilon_l^k(\varepsilon_l - 1)$ is a p-th power in $\mathbb{K}_l$, where $2 \leq k \leq p-3$. Moreover, the unit $\varepsilon_l^{(p-1)/2}(\varepsilon_l - 1)$ is not a p-th power in $\mathbb{K}_l$, for p a prime integer in the range $5 \leq p \leq 101$. Hence, the prime numbers 2, 3 and 5 never divide the unit index j_l.*

4.1. The units $\varepsilon_l(\varepsilon_l - 1)$ and $\varepsilon_l^{p-2}(\varepsilon_l - 1)$ are not p-th powers.

Lemma 11 (see [2, top of page 111])**.** *Assume that two of the three conjugates ε, ε' and ε'' of a totally real cubic unit ε are greater than 1, and that $\mathrm{Irr}(\varepsilon, \mathbb{Q}) = X^3 - SX^2 + TX - 1 \in \mathbb{Z}[X]$ with $S^2 - 4T = 1$. Then ε is not a p-th power in $\mathbb{Q}(\varepsilon)$ for any prime number $p \geq 3$.*

In particular, $\varepsilon_l(\varepsilon_l - 1)$ is not a p-th power in $\mathbb{K}_l$ for any prime number $p \geq 3$.

Proof. We may assume that $\varepsilon, \varepsilon' > 1 > \varepsilon'' > 0$. Suppose that $\varepsilon = \eta^p$ with $\eta \in \mathbb{Q}(\varepsilon)$. Then $\eta, \eta' > 1$ and $\eta'' = 1/(\eta\eta')$. In the range $x > 0$, set

$$\begin{aligned} F(x) &= (\eta^x + \eta'^x + \eta''^x)^2 - 4(\eta^x\eta'^x + \eta^x\eta''^x + \eta'^x\eta''^x) \\ &= \eta^{2x} + \eta'^{2x} + (\eta\eta')^{-2x} - 2(\eta^{-x} + \eta'^{-x} + (\eta\eta')^x), \end{aligned}$$

Hence, $F(n) = \mathrm{Tr}(\eta^n)^2 - 4\,\mathrm{Tr}(\eta^{-n}) \in \mathbb{Z}$ and $F(n) \equiv 0, 1 \pmod 4$ for $n \in \mathbb{Z}$. Set $X = \eta^x > 1$ and $Y = \eta'^x > 1$. Then

$$\frac{x}{2}F'(x) = (X - Y)(X\log X - Y\log Y) + \left(\frac{XY^2 - 1}{X^2Y^2}\right)\log X + \left(\frac{X^2Y - 1}{X^2Y^2}\right)\log Y$$

is positive. Hence, $F(0^+) = -3 < F(1) < F(p) = S^2 - 4T = 1$. Since $F(1) \equiv 0, 1 \pmod 4$, we have $F(1) = 0$ and $0 = F(1) \equiv F(p) \equiv 1 \pmod p$, by (3), which is impossible.

Finally, $\varepsilon := \varepsilon_l^{-1}(\varepsilon_l - 1)^{-1} = \varepsilon_l + l$ satisfies the required conditions for its conjugates verify $0 < \varepsilon < 1 < l - 1 < \varepsilon' < l < \varepsilon'' < l + 2$, by (1). □

The following result, whose proof is simpler than [2, page 112, Case $\eta^5 = \varepsilon(\varepsilon - 1)^2$], generalizes it to any prime $p \geq 5$:

Lemma 12. *For $p \geq 5$ a prime number and $l \geq 3$, the unit $\varepsilon_l^{p-2}(\varepsilon_l - 1)$ is not a p-th power in $\mathbb{K}_l$.*

Proof. To begin with, $\varepsilon_l^{p-2}(\varepsilon_l - 1)$ is a p-th power in $\mathbb{K}_l$ if and only if $\varepsilon := \varepsilon_l^2(\varepsilon_l - 1)^{-1} = \varepsilon_l^2 + (l+1)\varepsilon_l + 1$ is one. We have $\mathrm{Irr}(\varepsilon, \mathbb{Q}) = X^3 - 5X^2 - (l^2 + 3l - 2)X - 1$, by (4), and the conjugates of ε lie in the intervals

$$-l < \varepsilon < -l + 1 < -1 < \varepsilon' < 0 < l + 4 < \varepsilon'' < l + 5.$$

In particular, $\varepsilon'' > -\varepsilon > 1 > -\varepsilon' > 0$.

Suppose that $\varepsilon = \eta^p$ with $\eta \in \mathbb{K}_l$. Then $\eta'' > -\eta > 1 > -\eta' > 0$ and $F(x) := -(-\eta)^x - (-\eta')^x + \eta''^x$ is an increasing function of $x > 0$ such that $F(n) = \mathrm{Tr}(\eta^n) \in \mathbb{Z}$ for $n \in \mathbb{Z}$ odd. Hence, $-1 = F(0^+) < F(1) = \mathrm{Tr}(\eta) < F(p) = \mathrm{Tr}(\varepsilon) = 5$. However, $\mathrm{Tr}(\eta) \equiv \mathrm{Tr}(\eta)^p \equiv \mathrm{Tr}(\eta^p) \equiv \mathrm{Tr}(\varepsilon) \equiv 5 \pmod p$, by (3). Hence, $-1 < \mathrm{Tr}(\eta) < 5$ and $\mathrm{Tr}(\eta) \equiv 5 \pmod p$. It follows that $p = 5$, $\mathrm{Tr}(\eta) = 0$, $\mathrm{Irr}(\eta, \mathbb{Q}) = X^3 + bX - 1 \in \mathbb{Z}[X]$ for some $b \in \mathbb{Z}$ and $\mathrm{Irr}(\varepsilon, \mathbb{Q}) = \mathrm{Irr}(\eta^5, \mathbb{Q}) = X^3 + 5bX^2 + (5b^2 + b^5)X - 1 = X^3 - 5X^2 - (l^2 + 3l - 2)X - 1$, by (4). Therefore, $b = -1$ and $4 = -(l^2 + 3l - 2)$, hence $l = -1$ or $l = -2$, a contradiction. □

4.2. When is the unit $\varepsilon_l^{(p-1)/2}(\varepsilon_l - 1)$ a p-th power? The following result, whose proof is simpler than [2, page 111, Case $\eta^5 = \varepsilon^2(\varepsilon - 1)$], generalizes it to any prime $p \geq 5$:

Lemma 13. *Let $p > 3$ be a given prime number. There are only finitely many $l \geq 3$ for which $\varepsilon_l^{(p-1)/2}(\varepsilon_l - 1)$ is a p-th power in $\mathbb{K}_l$. More precisely, let $S_p(X), T_p(X) \in \mathbb{Z}[X]$ be such that*

$$\begin{aligned} R_p(Y) &:= \mathrm{Resultant}(X^3 - (2S+1)X^2 + (S^2+S)X - 1, Y - X^p, X) \\ &= Y^3 - S_p(S)Y^2 + T_p(S)Y - 1, \end{aligned}$$

and let $L_p(X) \in \mathbb{Z}[X]$ be defined by

$$pL_p(X) = S_p(X)^2 - 4T_p(X) - 1.$$

If $\varepsilon_l^{(p-1)/2}(\varepsilon_l - 1) = \eta^p$ is a p-th power in $\mathbb{K}_l$, then there exists $S \in \mathbb{Z}$ such that $L_p(S) = 0$ and $\mathrm{Irr}(\eta, \mathbb{Q}) = X^3 - (2S+1)X^2 + (S^2+S)X - 1$.

Proof. To begin with, $\varepsilon_l^{(p-1)/2}(\varepsilon_l - 1)$ is a p-th power in $\mathbb{K}_l$ if and only so is $\varepsilon := \varepsilon_l^{-1}(\varepsilon_l - 1)^2 = \varepsilon_l^2 + l\varepsilon_l - l - 2$. Since $\mathrm{Irr}(\varepsilon, \mathbb{Q}) = X^3 + (2l+5)X^2 + (l^2 + 5l + 6)X - 1$, by (4), the conjugates of ε lie in the intervals

$$-l - 3 < \varepsilon' < -l - 3 + 1/l < -l - 2 - 1/l < \varepsilon < -l - 2 < 0 < \varepsilon'' < 1, \tag{7}$$

and $\varepsilon, \varepsilon' < -1$ and $0 < \varepsilon'' < 1$.

Suppose that $\varepsilon = \eta^p$ with $\eta \in \mathbb{K}_l$. Then $\eta, \eta'' < -1$ and $0 < \eta'' < 1$. Set $\rho_1 := -\eta > 1$, $\rho_2 := -\eta' > 1$ and $F(x) := \rho_1^{2x} + \rho_2^{2x} + (\rho_1\rho_2)^{-2x} + 2(\rho_1^{-x} + \rho_2^{-x} - (\rho_1\rho_2)^x)$ with $x > 0$. Hence, $F(n) = \mathrm{Tr}(\eta^n)^2 - 4\,\mathrm{Tr}(\eta^{-n}) \in \mathbb{Z}$ and $F(n) \equiv 0, 1 \pmod 4$ for $n \geq 1$ odd. Moreover, $0 < G(x) < F(x) = G(x) + (\rho_1\rho_2)^{-2x} + 2\rho_1^{-x} + 2\rho_2^{-x} < G(x)+5$, where $G(x) = (\rho_1^x - \rho_2^x)^2$ is an increasing function of $x > 0$. It follows that $0 < F(1) < G(1)+5 < G(p)+5 < F(p)+5 = (2l+5)^2 - 4(l^2+5l+6)+5 = 6$ and $F(1) \equiv 0, 1 \pmod 4$. Hence, $F(1) = 1$, 4 or 5. But $F(1) \equiv F(p) \equiv 1 \pmod p$, by (3), yields $F(1) \neq 4, 5$ for $p > 3$. Hence, $F(1) = 1$ and $\mathrm{Irr}(\eta, \mathbb{Q}) = X^3 - sX^2 + tX - 1$ with $s^2 - 4t = 1$, i.e., $\mathrm{Irr}(\eta, \mathbb{Q}) = X^3 - (2S+1)X^2 + (S^2+S)X - 1$ for some $S \in \mathbb{Z}$. Now, $Y^3 - S_p(S)Y^2 + T_p(S)Y - 1 = R_p(Y) = \mathrm{Irr}(\eta^p, \mathbb{Q}) = \mathrm{Irr}(\varepsilon, \mathbb{Q}) = Y^3 + (2l+5)Y^2 + (l^2+5l+6)Y - 1$ yields $pL_p(S) = (2l+5)^2 - 4(l^2+5l+6) - 1 = 0$. $\square$

Lemma 14. *Assume that $l \geq 3$. Then the unit $\varepsilon_l^{(p-1)/2}(\varepsilon_l - 1)$ is not a p-th power in $\mathbb{K}_l$ for p a prime integer in the range $5 \leq p \leq 101$.*

Proof. Using any software for algebraic computation, we compute $L_p(X) \in \mathbb{Z}[X]$ and check that it has no root in $\mathbb{Z}$ (for example, $L_5(X) = 5X^8 + 40X^7 + 110X^6 + 180X^5 + 217X^4 + 188X^3 + 116X^2 + 52X + 11$ and its roots in $\mathbb{Z}$ would divide 11). We would like to point out that for the non-prime odd exponent $p = 9$ it is easy to check that $S = -1$ is an integral root of $L_9(X)$, even though in that case $l = 1$ and $D_\eta = D_{\eta^9} = -23$ is negative. What we mean to say is that this example shows that it might be difficult to prove that $\varepsilon_l^{(p-1)/2}(\varepsilon_l - 1)$ is never a p-th power in $\mathbb{K}_l$, $l \geq 3$. $\square$

5. Ennola's conjecture is true for $3 \leq l \leq 5 \cdot 10^7$

According to Propositions 4 and 10, the unit index j_l is coprime to 30. Notice that our proof is simpler than the one in [2] and does not require l to be explicitly large enough ($l > 500$ in [2]), which imposes to check numerically the result for small l's. Now, using Theorem 2 and Propositions 4 and 10, we are in a position to prove the last assertion of Theorem 1:

Proposition 15. *Set $\alpha_7 = 2 - 2/\sqrt{7} = 1.24407\cdots$. Write $D_l = \Delta_l f^2$, with $\Delta_l > 1$ square-free. If $f \leq l^{\alpha_7}/4$, then $\{\varepsilon_l, \varepsilon_l - 1\}$ is a system of fundamental units of the ring of algebraic integers $\mathbb{Z}_{\mathbb{K}_l}$ of $\mathbb{K}_l$. In particular, $\{\varepsilon_l, \varepsilon_l - 1\}$ is a system of fundamental units of $\mathbb{Z}_{\mathbb{K}_l}$ for all the l's in the range $3 \leq l \leq 5 \cdot 10^7$.*

Proof. Since $D_l = (\mathbb{Z}_{\mathbb{K}_l} : \mathbb{Z}[\varepsilon_l])^2 d_{\mathbb{K}_l}$, it follows that the index $(\mathbb{Z}_{\mathbb{K}_l} : \mathbb{Z}[\varepsilon_l])$ divides f. The first assertion follows from Propositions 4 and 10 and Theorem 2 applied with $p_0 = 7$ and $\mathbb{M} = \mathbb{Z}_{\mathbb{K}_l}$.

For the second assertion, an easy to program numerical computation on a microcomputer yields that there are only nine l's in the range $3 \leq l \leq 5{\cdot}10^7$ for which $f > l/3$ (V. Ennola's bound in [3]): $(l, f) = (9, 7)$, $(16, 7)$, $(163, 119)$, $(436, 161)$, $(1269, 721)$, $(8612, 3409)$, $(1049771, 690319)$, $(2180628, 1661359)$, $(3363845, 8757959)$, $(7335155, 3020857)$ and $(16146757, 7718593)$, four of them $(l, f) = (9, 7)$, $(16, 7)$, $(163, 119)$ and $(1269, 721)$ are such that $f > l^{\alpha_5}/2$ with $\alpha_5 = 2 - 2/\sqrt{5} = 1.10557\cdots$, and only one of them $(l, f) = (9, 7)$ is such that $f > l^{\alpha_7}/2$ with $\alpha_7 = 2 - 2/\sqrt{7} = 1.24407\cdots$. (This clearly shows the effect of the choice of p_0 in Theorem 2.)

Finally, for $l = 9$, since $\mathrm{Irr}(\varepsilon_l - 2, \mathbb{Q}) = X^3 + 14X^2 + 35X + 21$ is 7-Eisenstein, 7 does not divide the index $(\mathbb{Z}_{\mathbb{K}_l} : \mathbb{Z}[\varepsilon_l])$ (e.g., see [7, Lemma 2.3]). Since $7^2 \cdot 233 = D_9 = (\mathbb{Z}_{\mathbb{K}_9} : \mathbb{Z}[\varepsilon_9])^2 d_{\mathbb{K}_9}$, for $l = 9$ we have $\mathbb{Z}_{\mathbb{K}_l} = \mathbb{Z}[\varepsilon_l]$, and the conclusion holds true for $l = 9$, by Theorem 2. $\square$

6. The primes 7, 11, 13, 17 and 19 do not divide the unit index j_l

In the previous sections, following V. Ennola, we proved that the unit ε_l and the four units $\varepsilon_l^k(\varepsilon_l - 1)$'s with $k \in \{0, 1, p-2, p-1\}$ are never p-th powers in $\mathbb{K}_l$. For a given p, we also devised a simple method to find the l's for which the unit $\varepsilon_l^{(p-1)/2}(\varepsilon_l - 1)$ is a p-th power in $\mathbb{K}_l$ (Lemma 13). Since we could not prove similar results for other values of k, now our strategy will be different.

Let us explain how we can prove that not only a given $\varepsilon_l^k(\varepsilon_l - 1)$ but any given $\varepsilon_l^a(\varepsilon_l - 1)^b$ is not a p-th power in $\mathbb{K}_l$ for $l \geq l_p$ explicitly large enough. Recalling (5), we set

$$s = S_{a,b,p}(l), \ t = S_{-a,-b,p}(l) \quad \text{and} \quad w = l^{1/p} \tag{8}$$

and notice that if $\varepsilon_l^a(\varepsilon_l - 1)^b$ is a p-th power in $\mathbb{K}_l$, then $s \in \mathbb{Z}$ and $t = \mathbb{Z}$. For given a, b and p, V. Ennola's strategy was to arrive at a contradiction by constructing some $F_{a,b}(X, Y) \in \mathbb{Z}[X, Y]$ such that $0 < f(w) < 1$ (for l large enough), where

$$f(w) = F_{a,b}(s, t) = F_{a,b}(S_{a,b,p}(w^p), S_{-a,-b,p}(w^p)). \tag{9}$$

However, to build such polynomials in [2, Pages 111–112], he used the fact that he was working with a specific prime, namely, $p = 5$, which enabled him to use the relation $w^5 = l$ to cancel out the exponent w^5 in the expansion of $f(w)$. For example, taking $F_{2,1}(X, Y) = Y^2 + XY + Y - 2X - l - 3$, he could prove that $\varepsilon_l^2(\varepsilon_l - 1)$ is not a 5-th power in $\mathbb{K}_l$, but he did not prove that it was not, say, a 7-th power. Our approach is different. For given a and b, we construct a polynomial $F_{a,b}(X,Y) \in \mathbb{Z}[X,Y]$ that for any given prime integer p explicitly large enough works for $l \geq l_p$ explicitly large enough. The small values $l < l_p$ are then dealt with by using Propositions 9 and 15. For example, taking $F_{2,1}(X,Y) = X^2 + Y^3 - 3XY + X - 2Y + 3$, we will be able to prove that $\varepsilon_l^2(\varepsilon_l - 1)$ is not a p-th power for $p \in \{7, 11, 13, 17, 19\}$. By Lemma 8, our strategy to find such polynomials is to find some $0 \neq F_{a,b}(X,Y) \in \mathbb{Z}[X,Y]$ such that the non-negative powers of w cancel out in the expansion of

$$F_{a,b}\left((-1)^{a+b}w^{a+b} + (-1)^{a+b}w^{-a} + w^{-b}, (-1)^{a+b}w^{-a-b} + (-1)^{a+b}w^{a} + w^{b}\right).$$

Since $\varepsilon_l^k(\varepsilon_l - 1)$ is a p-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l^a(\varepsilon_l - 1)^b$, where b is not divisible by p and $a \equiv kb \pmod{p}$, for a given k we will choose b not divisible by p and a with $a \equiv kb \pmod{p}$ such that $\max(|a+b|, |a|, |b|)$ is as small as possible. This makes the construction of the $F_{a,b}(X,Y)$'s easier than that of the $F_{k,1}(X,Y)$'s. For example, $\varepsilon_l^{(p+1)/2}(\varepsilon_l - 1)$ is a p-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l(\varepsilon_l - 1)^2$ (see Lemma 16).

We wanted to extend as far as we thought it reasonable Ennola's approach who dealt only with the primes 2, 3 and 5, while we go up to 19. We decided to stop there because in the process we could not find a nice method for constructing the polynomials $F_{a,b}(X,Y)$ but wanted to show that it is reasonable to suspect that it is always possible to find one. We wanted to give enough of them in the present paper to show that there are not hideous polynomials, and that maybe some reader could guess an elegant method for constructing them instead of finding them by trial and error, as we did.

6.1. The prime 7 does not divide the unit index j_l. Recall that for the remainder of this paper, for given exponents a and b, we try to prove that $\varepsilon := \varepsilon_l^a(\varepsilon - 1)^b$ is not a p-th power in $\mathbb{K}_l$ for $l \geq l_p$ large enough. In all the following Lemmas, s and t are as in (8), hence depend on w and p. We have the following result, whose proof is simpler than [2, Case $\eta^5 = \varepsilon^2(\varepsilon - 1)$] and generalizes it to other prime numbers $p \geq 5$.

Lemma 16. *Fix a prime number $p \geq 7$, and assume that $l \geq 3$.*

(1) *We have $F_{2,1}(s,t) := s^2 + t^3 - 3st + s - 2t + 3 = c_p w^{-1} + O(w^{-2})$, where $c_7 = 6/7$ and $c_p = 1$ for $p > 7$. Hence, for $l \geq l_p$ large enough, we have $0 < F_{2,1}(s,t) < 1$, and $\varepsilon_l^2(\varepsilon_l - 1)$ is not a p-th power in $\mathbb{K}_l$.*

(2) *We have $F_{1,2}(s,t) := -s^2 + t^3 - 3st - s + 2t + 3 = c_p w^{-1} + O(w^{-2})$, where $c_7 = 12/7$ and $c_p = 1$ for $p > 7$. Hence, for $l \geq l_p$ large enough, we have $0 < F_{1,2}(s,t) < 1$, and $\varepsilon_l(\varepsilon_l - 1)^2$ is not a p-th power in $\mathbb{K}_l$.*

(3) *The units* $\varepsilon_l^2(\varepsilon_l - 1)$ *and* $\varepsilon_l^{(p+1)/2}(\varepsilon_l - 1)$ *are not p-th powers in* $\mathbb{K}_l$ *for* $p \in \{7, 11, 13, 17, 19\}$. *Hence, 7 does not divide the unit index* j_l, *by Proposition 10.*

Proof. Assume that $p \geq 7$. In the first case, by Lemma 8 we have

$$s = S_{2,1,p}(l) = -w^3 + w^{-1} - w^{-2} - \frac{1}{p}w^{3-p} + O(w^{-2-p}),$$
$$t = S_{-2,-1,p}(l) = -w^2 + w - w^{-3} - \frac{1}{p}w^{2-p} + O(w^{-3-p}).$$

In the second case, by Lemma 8 we have

$$s = S_{1,2,p}(l) = -w^3 - w^{-1} + w^{-2} - \frac{2}{p}w^{3-p} + O(w^{-1-p}),$$
$$t = S_{-1,-2,p}(l) = w^2 - w - w^{-3} + \frac{3}{p}w^{2-p} + O(w^{1-p}).$$

Finally, numerical computation shows that in the first case $l_7 = 7$, $l_{11} = 19$, $l_{13} = 35$, $l_{17} = 114$ and $l_{19} = 204$, and in the second case $l_7 = 5$, $l_{11} = 4977$, $l_{13} = 28629$, $l_{17} = 708155$ and $l_{19} = 3459663$. Hence, noticing that $\varepsilon_l^{(p+1)/2}(\varepsilon_l - 1)$ is a p-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l(\varepsilon_l - 1)^2$, the last assertion follows from Propositions 9 and 15.

An easy but maybe not rigorous enough way to obtain these results is to use (6) and any software for computation (we used Maple) to draw the graph of $f(w)$ defined in (9) for $(a, b) = (2, 1)$ and $(a, b) = (1, 2)$.

Let us give some details on the involved computation for a rigorous justification of these results, i.e., let us make the implicit constants in the error terms fully explicit, for example, in the second case, with $p \geq 7$.

The minimal polynomial of $\varepsilon := \varepsilon_l(\varepsilon_l - 1)^2 = -(l+1)\varepsilon_l^2 + (l+1)\varepsilon_l + 1$ is $\mathrm{Irr}(\varepsilon, \mathbb{Q}) = X^3 + (l^3 + 2l^2 + l - 3)X^2 + (l^2 + 2l + 4)X - 1$, by (4). It follows that for $l \geq 4$ we have (with $0 \leq \theta \leq 1$, not necessarily the same at different places):

$$\varepsilon = -l^3(1 + 2l^{-1} + \theta l^{-2}),$$
$$\varepsilon' = -l^{-1}(1 + l^{-1} + 3\theta l^{-3}) = -l^{-1}(1 + l^{-1} + \theta l^{-2}),$$
$$\varepsilon'' = l^{-2}(1 - 3l^{-1} + 6\theta l^{-2}).$$

Hence, noticing that $w := l^{1/p} \geq 1$, by Lemma 17 below, for $l \geq 8$ we have

$$s = -w^3\left(1 + \frac{2}{pl} + \frac{14\theta_1}{pl^2}\right) - w^{-1}\left(1 + \frac{1}{pl} + \frac{8\theta_3}{pl^2}\right) + w^{-2}\left(1 - \frac{3}{pl} + \frac{54\theta_2}{pl^2}\right)$$
$$= -w^3 - w^{-1} + w^{-2} - \frac{2w^{3-p} + w^{-1-p} + 3w^{-2-p}}{p} + \frac{76\theta}{p}w^{3-2p} \quad (|\theta| \leq 1).$$

In the same way, $\mathrm{Irr}(1/\varepsilon,\mathbb{Q}) = X^3-(l^2+2l+4)X^2-(l^3+2l^2+l-3)X-1$ yields $1/\varepsilon = -l^{-3}(1-2l^{-1}+3\theta l^{-2})$, $1/\varepsilon' = -l(1-l^{-1}+\theta l^{-2})$, $1/\varepsilon'' = l^2(1+3l^{-1}+4\theta l^{-2})$, and, by Lemma 17, for $l\geq 8$ we have

$$\begin{aligned} t &= -w^{-3}\left(1-\frac{2}{pl}+\frac{26\theta_1}{pl^2}\right)-w\left(1-\frac{1}{pl}+\frac{8\theta_3}{pl^2}\right)+w^2\left(1+\frac{3}{pl}+\frac{42\theta_2}{pl^2}\right)\\ &= w^2-w-w^{-3}+\frac{3w^{2-p}+w^{1-p}+2w^{-3-p}}{p}+\frac{76\theta}{p}w^{2-2p}\quad(|\theta|\leq 1). \end{aligned}$$

Finally, let us give all the details in the case that $p=19$, i.e., let us compute l_{19}. Let s_+ and t_+ denote the expressions above for s and t for $\theta=+1$, and s_- and t_- those for $\theta=-1$. Hence, $s_-\leq s\leq s_+$ and $t_-\leq t\leq t_+$. For $l\geq 3$ we have $s\leq s_+<0$, and for $l\geq 208$ we have $t\geq t_-\geq 0$, which implies $M_-(w)\leq F_{1,2}(s,t) = -s^2+t^3-3st-s+2t+3\leq M_+(w)$, where $M_-(w) := -s_-^2+t_-^3-3s_+t_--s_++2t_-+3$, and $M_+(w) := -s_+^2+t_+^3-3s_-t_+-s_-+2t_++3$ are polynomials in w^{-1}, i.e., in $l^{-1/p}$, whose signs are easy to study. It follows that $F_{1,2}(s,t)\geq M_-(w)>0$ for $l\geq 3459663$, $F_{1,2}(s,t)\leq M_+(w)<1$ for $l\geq 4$, and $F_{1,2}(s,t)\leq M_+(w)<0$ for $6\leq l\leq 3459662$. $\square$

Lemma 17. *For $|X|\geq X_0 := |A|+\sqrt{A^2+2|B|}$ and $p>1$, it holds that*

$$\left(1+AX^{-1}+BX^{-2}\right)^{1/p} = 1+\frac{A}{p}X^{-1}+2\theta\frac{A^2+3|B|}{p}X^{-2}\ \textit{with}\ |\theta|\leq 1.$$

Proof. Set $x=1/X$, with $|x|\leq x_0 := 1/X_0$. By Taylor's formula, $f(x) := (1+Ax+Bx^2)^{1/p} = 1+\frac{Ax}{p}+\frac{x^2}{2}f''(C)$ for some C between 0 and x. Now,

$$pf''(C) = \frac{2B}{(1+AC+BC^2)^{1-1/p}}-\frac{(1-1/p)(A+2BC)^2}{(1+AC+BC^2)^{2-1/p}}.$$

Using $|C|\leq|x|\leq x_0$, $|A|x_0+|B|x_0^2 = 1/2$ and $(|A|+2|B|x_0)^2 = A^2+2|B|$, we obtain that the denominators satisfy $|(1+AC+BC^2)^{k-1/p}|\geq 1/2^{k-1/p}\geq 1/2^k$, $k=1,2$, and the desired result follows. $\square$

Remark 18. (This remark holds also true for the forthcoming Lemmas). By the first point of Lemma 16, for any given prime number $p\geq 7$, there are only finitely many l's for which $\varepsilon_l^2(\varepsilon_l-1)$ can be a p-th power in $\mathbb{K}_l$, Ennola's conjecture implying that no such l exists. However, our procedure for finding these l's is less neat and satisfactory than the one in Lemma 13: we have to make the error in the asymptotic expansion $f(w) = F_{2,1}(s,t) = F_{2,1}(s_{2,1,p}(l),t_{2,1,p}(l)) = c_pw^{-1}+O(w^{-2})$ explicit to find an explicit l_p such that $0<f(w)<1$ for $l\geq l_p$, and then deal with the l's less than l_p.

6.2. The prime 11 does not divide the unit index j_l. By Proposition 10 and Lemma 16, the prime 11 divides j_l if and only if one of the four units $\varepsilon_l^k(\varepsilon_l - 1)$ is an 11-th power in $\mathbb{K}_l$, $k \in \{3, 4, 7, 8\}$. Moreover,

(i) $\varepsilon_l^3(\varepsilon_l - 1)$ is an 11-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l^2(\varepsilon_l - 1)^{-3}$,

(ii) $\varepsilon_l^4(\varepsilon_l - 1)$ is an 11-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l^{-3}(\varepsilon_l - 1)^2$,

(iii) $\varepsilon_l^7(\varepsilon_l - 1)$ is an 11-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l(\varepsilon_l - 1)^{-3}$,

(iv) $\varepsilon_l^8(\varepsilon_l - 1)$ is an 11-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l^{-3}(\varepsilon_l - 1)$.

Lemma 19. *Fix a prime number $p \geq 11$, and assume that $l \geq 3$.*

(1) *We have $F_{2,-3}(s,t) := -s^2 - t^3 + 3st - s + 2t - 3 = w^{-1} + O(w^{-2})$. Hence, for $l \geq l_p$ large enough we have $0 < F_{2,-3}(s,t)) < 1$, and $\varepsilon_l^2(\varepsilon_l - 1)^{-3}$ is not a p-th power in $\mathbb{K}_l$.*

(2) *We have $F_{-3,2}(s,t) := -s^2 + t^3 - 3st - s + 2t + 3 = w^{-1} + O(w^{-2})$. Hence, for $l \geq l_p$ large enough we have $0 < F_{-3,2}(s,t) < 1$, and $\varepsilon_l^{-3}(\varepsilon_l - 1)^2$ is not a p-th power in $\mathbb{K}_l$.*

(3) *We have $F_{1,-3}(s,t) := s^2 - t^3 + 3st + s - 2t - 3 = w^{-1} + O(w^{-2})$. Hence, for $l \geq l_p$ large enough we have $0 < F_{1,-3}(s,t) < 1$, and $\varepsilon_l(\varepsilon_l - 1)^{-3}$ is not a p-th power in $\mathbb{K}_l$.*

(4) *We have $F_{-3,1}(s,t) := s^2 - t^3 + 3st + s - 2t - 3 = w^{-1} + O(w^{-2})$. Hence, for $l \geq l_p$ large enough we have $0 < F_{-3,1}(s,t) < 1$, and $\varepsilon_l^{-3}(\varepsilon_l - 1)$ is not a p-th power in $\mathbb{K}_l$.*

(5) *The units $\varepsilon_l^2(\varepsilon_l - 1)^{-3}$, $\varepsilon_l^{-3}(\varepsilon_l - 1)^2$, $\varepsilon_l(\varepsilon_l - 1)^{-3}$ and $\varepsilon_l^{-3}(\varepsilon_l - 1)$ are not 11-th, 13-th, 17-th or 19-th powers in $\mathbb{K}_l$. Hence, 11 does not divide the unit index j_l, by Proposition 10 and the last point of Lemma 16.*

Proof. Assume that $p \geq 11$. By Lemma 8 we have

$$\begin{aligned}
S_{2,-3,p}(l) &= w^3 - w^{-1} - w^{-2} + O(w^{3-p}),\\
S_{-2,3,p}(l) &= -w^2 - w + w^{-3} + O(w^{2-p}),\\
S_{-3,2,,p}(l) &= -w^3 - w^{-1} + w^{-2} + O(w^{3-p}),\\
S_{3,-2,p}(l) &= w^2 - w - w^{-3} + O(w^{2-p}),\\
S_{1,-3,p}(l) &= w^3 + w^{-1} + w^{-2} + O(w^{3-p}),\\
S_{-1,3,p}(l) &= w^2 + w + w^{-3} + O(w^{2-p}),\\
S_{-3,1,p}(l) &= w^3 + w^{-1} + w^{-2} + O(w^{3-p}),\\
S_{3,-1,,p}(l) &= w^2 + w + w^{-3} + O(w^{2-p}).
\end{aligned}$$

Finally, numerical computation shows that in the first case $l_{11} = 3$, $l_{13} = 4$, $l_{17} = 8$ and $l_{19} = 11$, in the second case $l_{11} = 3727$, $l_{13} = 27237$, $l_{17} = 706748$ and $l_{19} = 3458256$, in the third case $l_{11} = 3268$, $l_{13} = 13328$, $l_{17} = 242669$ and $l_{19} = 1042804$, and in the fourth case $l_{11} = 3540$, $l_{13} = 13591$, $l_{17} = 242931$ and $l_{19} = 1043067$. Hence, the last assertion follows from Propositions 9 and 15. $\square$

6.3. The prime 13 does not divide the unit index j_l. By Proposition 10 and Lemma 16, the prime 13 divides j_l if and only if one of the six units $\varepsilon_l^k(\varepsilon_l - 1)$ is a 13-th power in $\mathbb{K}_l$, $k \in \{3, 4, 5, 8, 9, 10\}$. Moreover,

(i) $\varepsilon_l^4(\varepsilon_l - 1)$ is a 13-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l(\varepsilon_l - 1)^{-3}$,

(ii) $\varepsilon_l^5(\varepsilon_l - 1)$ is a 13-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l^{-3}(\varepsilon_l - 1)^2$,

(iii) $\varepsilon_l^8(\varepsilon_l - 1)$ is a 13-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l^2(\varepsilon_l - 1)^{-3}$,

(iv) $\varepsilon_l^{10}(\varepsilon_l - 1)$ is a 13-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l^{-3}(\varepsilon_l - 1)$.

Hence, by Lemma 19, the prime 13 divides j_l if and only if $\varepsilon_l^3(\varepsilon_l - 1)$ or $\varepsilon_l^9(\varepsilon_l - 1)$ is a 13-th power in $\mathbb{K}_l$. Moreover, $\varepsilon_l^9(\varepsilon_l - 1)$ is a 13-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l(\varepsilon_l - 1)^3$.

Lemma 20. *Fix a prime number $p \geq 13$, and assume that $l \geq 3$.*

(1) *We have $0 < F_{3,1}(s,t) := s^3 - t^4 + 4st^2 - 2s^2 - 3st + s - 4t + 3 = c_p w^{-1} + O(w^{-2})$, where $c_{13} = 8/13$ and $c_p = 1$ for $p > 13$. Hence, for $l \geq l_p$ large enough we have $0 < F_{3,1}(s,t) < 1$, and $\varepsilon_l^3(\varepsilon_l - 1)$ is not a p-th power in $\mathbb{K}_l$.*

(2) *We have $F_{1,3}(s,t) := s^3 - t^4 + 4st^2 - 2s^2 - 3st + s - 4t + 3 = c_p w^{-1} + O(w^{-2})$, where $c_{13} = 2/13$ and $c_p = 1$ for $p > 13$. Hence, for $l \geq l_p$ large enough we have $0 < F_{1,3}(s,t) < 1$, and $\varepsilon_l(\varepsilon_l - 1)^3$ is not a p-th power in $\mathbb{K}_l$.*

(3) *The units $\varepsilon_l^3(\varepsilon_l - 1)$ and $\varepsilon_l(\varepsilon_l - 1)^3$ are not 13-th, 17-th or 19-th powers in $\mathbb{K}_l$. Hence, 13 does not divide the unit index j_l, by Proposition 10 and the last points of Lemmas 16 and 19.*

Proof. Assume that $p \geq 13$. By Lemma 8 we have

$$\begin{aligned}
S_{3,1,p}(l) &= w^4 + w^{-1} + w^{-3} + \frac{1}{p} w^{4-p} + O(w^{-1-p}), \\
S_{-3,-1,p}(l) &= w^3 + w + w^{-4} + \frac{2}{p} w^{3-p} + O(w^{1-p}), \\
S_{1,3,p}(l) &= w^4 + w^{-1} + w^{-3} + \frac{3}{p} w^{4-p} + O(w^{-1-p}), \\
S_{-1,-3,p}(l) &= w^3 + w + w^{-4} + \frac{5}{p} w^{3-p} + O(w^{1-p}).
\end{aligned}$$

Finally, numerical computation shows that in the first case $l_{13} = 244$, $l_{17} = 7058$ and $l_{19} = 23234$, and in the second case $l_{13} = 58$, $l_{17} = 5485$ and $l_{19} = 21430$. Hence, the last assertion follows from Propositions 9 and 15. $\square$

6.4. The prime 17 does not divide the unit index j_l. By Proposition 10 and Lemma 16, the prime 17 divides j_l if and only if one of the ten units $\varepsilon_l^k(\varepsilon_l - 1)$ is a 17-th power in $\mathbb{K}_l$, $k \in \{3, 4, 5, 6, 7, 10, 11, 12, 13, 14\}$. Moreover,

(i) $\varepsilon_l^5(\varepsilon_l - 1)$ is a 17-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l^2(\varepsilon_l - 1)^{-3}$,

(ii) $\varepsilon_l^6(\varepsilon_l - 1)$ is a 17-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l(\varepsilon_l - 1)^3$,

(iii) $\varepsilon_l^7(\varepsilon_l - 1)$ is a 17-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l^{-3}(\varepsilon_l - 1)^2$,

(iv) $\varepsilon_l^{11}(\varepsilon_l - 1)$ is a 17-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l(\varepsilon_l - 1)^{-3}$,

(v) $\varepsilon_l^{14}(\varepsilon_l - 1)$ is a 17-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l^{-3}(\varepsilon_l - 1)$.

Hence, by Lemmas 19, and 20 the prime 17 divides j_l if and only if one of the four units $\varepsilon_l^k(\varepsilon_l - 1)$ is a 17-th power in $\mathbb{K}_l$, $k \in \{4, 10, 12, 13\}$, hence if and only if one of the four units $\varepsilon_l(\varepsilon_l - 1)^{-4}$, $\varepsilon_l^{-4}(\varepsilon_l - 1)^3$, $\varepsilon_l^3(\varepsilon_l - 1)^{-4}$ or $\varepsilon_l^{-4}(\varepsilon_l - 1)$ is a 17-th power in $\mathbb{K}_l$.

Lemma 21. *Fix a prime number $p \geq 17$, and assume that $l \geq 3$.*

(1) *We have $F_{1,-4}(s,t) := -s^3 + t^4 - 4st^2 + 2s^2 + 3st - s + 4t - 3 = w^{-1} + O(w^{-2})$. Hence, for $l \geq l_p$ large enough we have $0 < F_{1,-4}(s,t) < 1$, and $\varepsilon_l(\varepsilon_l - 1)^{-4}$ is not a p-th power in $\mathbb{K}_l$.*

(2) *We have $F_{-4,1}(s,t) := s^3 + t^4 - 4st^2 + 2s^2 - 3st + s + 4t + 3 = w^{-1} + O(w^{-2})$. Hence, for $l \geq l_p$ large enough we have $0 < F_{-4,1}(s,t) < 1$, and $\varepsilon_l^{-4}(\varepsilon_l - 1)$ is not a p-th power in $\mathbb{K}_l$.*

(3) *We have $F_{3,-4}(s,t) := -s^3 + t^4 - 4st^2 + 2s^2 + 3st - s + 4t - 3 = w^{-1} + O(w^{-2})$. Hence, for $l \geq l_p$ large enough we have $0 < F_{3,4}(s,t) < 1$, and $\varepsilon_l^3(\varepsilon_l - 1)^{-4}$ is not a p-th power in $\mathbb{K}_l$.*

(4) *We have $F_{-4,3}(s,t) := -s^3 - t^4 + 4st^2 - 2s^2 + 3st - s - 4t - 3 = w^{-1} + O(w^{-2})$. Hence, for $l \geq l_p$ large enough we have $0 < F_{-4,3}(s,t) < 1$, and $\varepsilon_l^{-4}(\varepsilon_l - 1)^3$ is not a p-th power in $\mathbb{K}_l$.*

(5) *The units $\varepsilon_l(\varepsilon_l - 1)^{-4}$, $\varepsilon_l^{-4}(\varepsilon_l - 1)^3$, $\varepsilon_l^3(\varepsilon_l - 1)^{-4}$ and $\varepsilon_l^{-4}(\varepsilon_l - 1)$ are not 17-th or 19-th powers in $\mathbb{K}_l$. Hence, 17 does not divide the unit index j_l, by Proposition 10 and the last points of Lemmas 16, 19 and 20.*

Proof. Assume that $p \geq 17$. By Lemma 8 we have

$$S_{1,-4,p}(l) = w^4 - w^{-1} - w^{-3} + O(w^{4-p}),$$
$$S_{-1,4,p}(l) = -w^3 - w + w^{-4} + O(w^{3-p}),$$

$$
\begin{aligned}
S_{-4,1,p}(l) &= -w^4 + w^{-1} - w^{-3} + O(w^{4-p}),\\
S_{4,-1,p}(l) &= -w^3 + w - w^{-4} + O(w^{3-p}),\\
S_{3,-4,p}(l) &= w^4 - w^{-1} - w^{-3} + O(w^{4-p}),\\
S_{-3,4,p}(l) &= -w^3 - w + w^{-4} + O(w^{3-p}),\\
S_{-4,3,p}(l) &= -w^4 - w^{-1} + w^{-3} + O(w^{4-p}),\\
S_{4,-3,p}(l) &= w^3 - w - w^{-4} + O(w^{3-p}).
\end{aligned}
$$

Finally, numerical computation shows that in the first case $l_{17} = 5512$ and $l_{19} = 21527$, in the second case $l_{17} = 3$ and $l_{19} = 3$, in the third case $l_{17} = 7084$ and $l_{19} = 23330$, and in the fourth case $l_{17} = 3$ and $l_{19} = 3$. Hence, the last assertion follows from Propositions 9 and 15. □

6.5. The prime 19 does not divide the unit index j_l. According to Proposition 4 and Lemmas 16, 19, 20 and 21, as in the beginning of the previous section, we have that the prime 19 divides j_l if and only if $\varepsilon_l^7(\varepsilon_l - 1)$ or $\varepsilon_l^{11}(\varepsilon_l - 1)$ is a 17-th power in $\mathbb{K}_l$, $k \in \{7, 11\}$. Moreover,

(i) $\varepsilon_l^7(\varepsilon_l - 1)$ is a 19-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l^2(\varepsilon_l - 1)^3$,

(ii) $\varepsilon_l^{11}(\varepsilon_l - 1)$ is a 19-th power in $\mathbb{K}_l$ if and only if so is $\varepsilon_l^3(\varepsilon_l - 1)^2$.

Lemma 22. *Fix a prime number $p \geq 19$, and assume that $l \geq 3$.*

(1) *We have $F_{2,3}(s,t) = s^3 + t^5 - 5st^3 + 5s^2t + s^2 - 3st + 5t^2 - 5s - 2t + 3 = c_p w^{-4} + O(w^{-5})$, where $c_{19} = 30/19$ and $c_p = 1$ for $p > 19$. Hence, for $l \geq l_p$ large enough we have $0 < F_{2,3}(s,t) < 1$, and $\varepsilon_l^2(\varepsilon_l - 1)^3$ is not a p-th power in $\mathbb{K}_l$.*

(2) *We have $F_{3,2}(s,t) = s^3 - t^5 + 5st^3 - 5s^2t + s^2 - 3st - 5t^2 + 5s - 2t + 3 = c_p w^{-4} + O(w^{-5})$, where $c_{19} = 18/19$ and $c_p = 1$ for $p > 19$. Hence, for $l \geq l_p$ large enough we have $0 < F_{3,2}(s,t) < 1$, and $\varepsilon_l^2(\varepsilon_l - 1)^3$ is not a p-th power in $\mathbb{K}_l$.*

(3) *The units $\varepsilon_l^2(\varepsilon_l - 1)^3$ and $\varepsilon_l^3(\varepsilon_l - 1)^2$ are not 19-th powers in $\mathbb{K}_l$. Hence, 19 does not divide the unit index j_l, by Proposition 10 and the last points of Lemmas 16, 19, 20 and 21.*

Proof. Assume that $p \geq 19$. By Lemma 8 we have

$$
\begin{aligned}
S_{2,3,p}(l) &= -w^5 - w^{-2} + w^{-3} - \frac{3}{p} w^{5-p} + O(w^{-2-p}),\\
S_{-2,-3,p}(l) &= w^3 - w^2 - w^{-5} + \frac{4}{p} w^{3-p} + O(w^{2-p}),
\end{aligned}
$$

$$S_{3,2,p}(l) = -w^5 + w^{-2} - w^{-3} + -\frac{2}{p}w^{5-p} + O(w^{-2-p}),$$
$$S_{-3,-2,p}(l) = -w^3 + w^2 - w^{-5} - \frac{1}{p}w^{3-p} + O(w^{2-p}).$$

Finally, numerical computation shows that in the first case $l_{19} = 39$ and in the second case $l_{19} = 21$. Hence, the last assertion follows from Propositions 9 and 10. □

References

[1] T. W. Cusick, Lower bounds for regulators, In: Lecture Notes in Mathematics, Vol. **1068**, *Springer*, *Berlin*, 1984, 63–73.

[2] V. Ennola, Cubic number fields with exceptional units, In: Computational Number Theory (Debrecen, 1989), *de Gruyter*, *Berlin*, 1991, 103–128.

[3] V. Ennola, Fundamental units in a family of cubic fields, *J. Théor. Nombres Bordeaux* **16** (2004), 569–575.

[4] J. H. Lee and S. R. Louboutin, On the fundamental units of some cubic orders generated by units, *Acta Arith.* **165** (2014), 283–299.

[5] S. R. Louboutin and J. H. Lee, Fundamental units for a family of totally real cubic orders and the diophantine equation $u(u+a)(u+2a) = v(v+1)$, *Int. J. Number Theory* **13** (2017), 1729–1746.

[6] S. Louboutin, Class number and class group problems for some non-normal totally real cubic number fields, *Manuscripta Math* **106** (2001), 411–427.

[7] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers. Second Edition, *Springer-Verlag*, *Berlin; PWN – Polish Scientific Publishers, Warsaw*, 1990.

[8] V. Sprindžuk, Classical Diophantine equations, Lecture Notes in Mathematics, Vol. **1559**, *Springer-Verlag*, *Berlin*, 1993.

[9] E. Thomas, Fundamental units for orders in certain cubic number fields, *J. Reine Angew. Math.* **310** (1979), 33–55.

[10] L. C. Washington, Introduction to Cyclotomic Fields. Second Edition, Graduate Texts in Mathematics, Vol. **83**, *Springer-Verlag*, *New York*, 1997.

STÉPHANE R. LOUBOUTIN
AIX MARSEILLE UNIVERSITÉ
CNRS, CENTRALE MARSEILLE, I2M
MARSEILLE
FRANCE

POSTAL ADDRESS:
INSTITUT DE MATHÉMATIQUES DE MARSEILLE
AIX MARSEILLE UNIVERSITÉ
163 AVENUE DE LUMINY, CASE 907
13288 MARSEILLE CEDEX 9.
FRANCE

E-mail: stephane.louboutin@univ-amu.fr

(Received May 26, 2016; revised March 13, 2017)