ACTA ARITHMETICA
165.3 (2014)

On the fundamental units of some cubic orders generated by units

by

Jun Ho Lee (Seoul) and Stéphane R. Louboutin (Marseille)

1. Introduction. Let ϵ be a cubic algebraic unit. Let $\Pi_\epsilon(X) = X^3 - aX^2+bX-c \in \mathbb{Z}[X]$, with $c \in \{\pm 1\}$, be its minimal polynomial. Let ϵ, ϵ' and ϵ'' be the three conjugates of ϵ, i.e. the three distinct complex roots of $\Pi_\epsilon(X)$.

If ϵ is not totally real, it is known that in general ϵ is a fundamental unit of the cubic order $\mathbb{Z}[\epsilon]$ (see [Nag], [Lou06], [Lou08a] and [Lou10]).

Now, assume that ϵ is totally real. It is known (see [BHMMS], [MS] and [Lou12]) that in general there exists $\eta \in \mathbb{Z}[\epsilon]$ such that $\{\epsilon, \eta\}$ is a system of fundamental units of the cubic order $\mathbb{Z}[\epsilon]$. There are two different situations in which we might be able to make such a unit η explicit.

On the one hand, we might search for it of the form $r\epsilon + s$. For example, if we want $\epsilon - 1$ to be also a unit, we are led to consider the parametrized families of cubic polynomials $\Pi_l(X) = X^3 + (l-1)X^2 - lX - 1$, $l \geq 3$, and $\Pi_k(X) = X^3 - kX^2 - (k+3)X - 1$, $k \geq -1$, the latter being associated with the so-called simplest cubic fields (see [Enn1]). In that situation, we would try to prove that $\{\epsilon, \epsilon - 1\}$ is a system of fundamental units of the order $\mathbb{Z}[\epsilon]$. This is the approach developed in [Enn1], [Enn2] and [Tho]. We will improve on Ennola's result in [Enn2], who proved that we can take $\alpha = 1$ in the following theorem (from a computational point of view, in the case that $M = \mathcal{O}$ is the maximal order of F_l, the calculation of the index is explained in [Enn1, Proposition 3.1]):

Theorem 1.1. *Let F_l be the non-Galois totally real cubic number field generated by a root ϵ of $\Pi_l(X) = X^3 + (l-1)X^2 - lX - 1$, $l \geq 3$. Then $\{\epsilon, \epsilon-1\}$ is a system of fundamental units of the totally real cubic order $\mathbb{Z}[\epsilon]$. Moreover, let M be an order of F_l containing $\mathbb{Z}[\epsilon]$ and set $\alpha = 2 - 2/\sqrt{7} = 1.244\ldots$. If the index $(M : \mathbb{Z}[\epsilon])$ is less than or equal to $l^\alpha/4$, then $\{\epsilon, \epsilon-1\}$ is a system of fundamental units of M.*

2010 *Mathematics Subject Classification*: Primary 11R16; Secondary 11R27.
Key words and phrases: cubic units, cubic orders, fundamental units.

DOI: 10.4064/aa165-3-7

On the other hand, we might assume that $\mathbb{Q}(\epsilon)$ is Galois and that $\mathbb{Z}[\epsilon]$ is invariant under the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$. In that situation we might expect that we can take for η any of the two conjugates ϵ' or ϵ'' of ϵ. In [Lou12] we proved that if the order $\mathbb{Z}[\epsilon]$ is invariant under the action of $\mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$, then the index $(U_\epsilon : \langle -1, \epsilon, \epsilon' \rangle)$ is less than or equal to 3, where U_ϵ is the group of units of $\mathbb{Z}[\epsilon]$. While trying to prove that this index was equal to 1, we realized in [LL] that it seldom happens that $\mathbb{Z}[\epsilon]$ is invariant under the action of $\mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$. Essentially, it happens if and only if ϵ is a so-called simplest cubic unit. Hence, we had not considered the right problem: this order $\mathbb{Z}[\epsilon]$ is too small.

In the present paper, we deal with the larger order $\mathbb{Z}[\epsilon, \epsilon', \epsilon'']$. This totally real cubic order is invariant under the action of $\mathrm{Gal}(\mathbb{Q}(\epsilon)/\mathbb{Q})$, and its group of units is of rank 2. Since ϵ and ϵ' are multiplicatively independent units of this order (see Lemma 4.1), it is natural to ask whether $\{\epsilon, \epsilon'\}$ is a system of fundamental units of $\mathbb{Z}[\epsilon, \epsilon', \epsilon'']$. In the literature we found several papers in which the authors claimed that $\{\epsilon, \epsilon'\}$ is indeed a system of fundamental units of $\mathbb{Z}[\epsilon, \epsilon', \epsilon'']$, provided that ϵ ranges in several peculiar families of cubic units defined by parametrized families of cubic polynomials (see [Kish], [Tog04], [Tog06] and [Tog08]). However, there are serious gaps in their proofs (see Section 3). In the present paper, we will fill in these gaps and prove:

THEOREM 1.2. *Let ϵ, ϵ' and ϵ'' be the three real roots of any one of the following parametrized families of $\mathbb{Q}$-irreducible cubic polynomials of discriminants a square (for $n \in \mathbb{Z}$):*

$$\begin{aligned}
\Phi_n(X) &= X^3 - n(n^2+n+3)(n^2+2)X^2 - (n^3+2n^2+3n+3)X - 1,\\
\Xi_n(X) &= X^3 - (n^3-2n^2+3n-3)X^2 - n^2X - 1, \qquad n \neq 1, 2,\\
\Psi_n(X) &= X^3 + (n^8+2n^6-3n^5+3n^4-4n^3+5n^2-3n+3)X^2\\
&\quad - (n^3-2)n^2X - 1.
\end{aligned}$$

Then $\{1, \epsilon, \epsilon^2\epsilon'\}$ is a $\mathbb{Z}$-basis of the totally real cubic order $\mathbb{Z}[\epsilon, \epsilon']$, and $\{\epsilon, \epsilon'\}$ is a system of fundamental units of $\mathbb{Z}[\epsilon, \epsilon']$.

To prove Theorem 1.2, we develop a general machinery which could be used to obtain similar results for various families that might crop up in the future, as in [Tha].

Combining our ideas for proving Theorems 1.1 and 1.2 we derive a stronger statement (similar results can be obtained for the other two families):

THEOREM 1.3. *Let ϵ, ϵ' and ϵ'' be the three real roots of Ξ_n, $n \geq 3$. Let M be an order of the cyclic cubic field $\mathbb{Q}(\epsilon)$ containing the totally real cubic order $\mathbb{Z}[\epsilon, \epsilon']$. Set $\alpha = 4 - \sqrt{28/3} = 0.94494\ldots$. If the index $(M : \mathbb{Z}[\epsilon, \epsilon'])$ is less than or equal to $\frac{2}{9}n^\alpha$, then $\{\epsilon, \epsilon'\}$ is a system of fundamental units of M.*

From a computational point of view, in the case that $M = \mathcal{O}$ is the maximal order of the cyclic cubic field $K = \mathbb{Q}(\epsilon)$, the index $(M : \mathbb{Z}[\epsilon, \epsilon']) = f_{\mathbb{Z}[\epsilon,\epsilon']}/f_K = (n^2+3)(n^2-3n+3)/f_K$ can be calculated by using [Was1, Theorem 1] to determine the conductor f_K of K. (The same remark applies to the $\Phi_n(X)$'s by using [Kish, Theorem 1].)

2. Sketch of proof. Let $e_1, \dots, e_n$ be n elements of a number field K of degree n with complex imbeddings σ_k, $1 \le k \le n$. Their *discriminant* is the rational number $d(e_1, \dots, e_n) := (\det[\sigma_k(e_l)]_{1\le k,l\le n})^2$. It is equal to 0 if and only if $e_1, \dots, e_n$ are $\mathbb{Q}$-linearly dependent. If $e_k = \epsilon^{k-1}$, $1 \le k \le n$, for some $\epsilon \in K$, then $d(e_1, \dots, e_n) = d(1, \epsilon, \dots, \epsilon^{n-1})$ is equal to the discriminant d_ϵ of the minimal polynomial $\Pi_\epsilon(X) \in \mathbb{Q}[X]$ of ϵ if this minimal polynomial is of degree n, i.e. if $K = \mathbb{Q}(\epsilon)$, and is equal to 0 otherwise. If M is a free $\mathbb{Z}$-module of rank n of K, then $d_M = d(e_1, \dots, e_n)$ does not depend on the $\mathbb{Z}$-basis $\{e_1, \dots, e_n\}$ of M. It is called the *discriminant of the module* M. In particular, $d_{\mathbb{Z}[\alpha]} = d_\alpha$ if $K = \mathbb{Q}(\alpha)$. If $M \subseteq N$ are two free $\mathbb{Z}$-modules of rank n of K, then the index $(N : M)$ is finite and $d_M = (N : M)^2 d_N$. Hence, d_N divides d_M. If $\mathcal{O}$ is the maximal order of K, then $d_\mathcal{O} = d_K$, the discriminant of K. Finally, if K is a cyclic cubic field of conductor $f_K > 1$, then $d_K = f_K^2$ and for any free $\mathbb{Z}$-module M of rank 3 of $\mathcal{O}$ we have $d_M = (\mathcal{O} : M)^2 d_K = ((\mathcal{O} : M) f_K)^2$. Hence, $d_M = f_M^2$ is the square of $f_M > 0$, the *conductor of the cubic module* M, and f_K divides f_M.

Now, to simplify, assume that K is totally real, which will always be the case in the present paper. Let M be an order of K. The unit group U_M of M is of rank $n-1$. The *regulator of the order* M is defined by

$$\mathrm{Reg}(M) := \mathrm{Reg}(\epsilon_1, \dots, \epsilon_{n-1}) := |\det[\log|\sigma_k(\epsilon_l)|]_{1\le k,l\le n-1}| > 0$$

(notice that we do not take into account one of the n embeddings of K, namely σ_n, which may be chosen arbitrarily). It does not depend on the system of fundamental units $\{\epsilon_1, \dots, \epsilon_n\}$ of M.

Our first main tool is the following result of T. W. Cusick (we will explain in Section 3 how a misunderstanding of Proposition 2.1 created gaps in the proofs of the three items of Theorem 1.2 in [Kish], [Tog04], [Tog06] and [Tog08], gaps that will be filled in the present paper):

PROPOSITION 2.1 (see [Cus]). *For any order M of a totally real cubic number field there exists a unit ϵ_M of M such that*

$$\mathrm{Reg}(M) \ge \frac{1}{16}\log^2(d_{\epsilon_M}/4) \ge \frac{1}{16}\log^2(d_M/4). \tag{1}$$

Our second main tool is built from the results of the second author in [Lou12]:

PROPOSITION 2.2. *Let ϵ be an algebraic cubic unit with minimal polynomial $\Pi_\epsilon(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$, $c \in \{\pm 1\}$, of discriminant $d_\epsilon = -4a^3c - 4b^3 + a^2b^2 + 18abc - 27c^2$. Assume that $\mathbb{Q}(\epsilon)$ is Galois, i.e. $d_\epsilon = f_\epsilon^2$ is a square. Let ϵ, ϵ' and ϵ'' be the three conjugates of ϵ. Then*

$$\mathrm{Reg}(\epsilon, \epsilon') \le \frac{1}{4}\log^2(4d_\epsilon). \tag{2}$$

Proof. Since d_ϵ and $\mathrm{Reg}(\epsilon, \epsilon')$ remain unchanged if ϵ is changed into any of the units $\pm\epsilon$, $\pm 1/\epsilon$, $\pm\epsilon'$, $\pm 1/\epsilon'$, $\pm\epsilon''$, $\pm 1/\epsilon''$, we may assume that $\epsilon > 1 > |\epsilon'| \ge |\epsilon''| > 0$, as in [Lou12]. Using $\epsilon\epsilon'\epsilon'' = \pm 1$, we have

$$\begin{aligned}
\mathrm{Reg}(\epsilon, \epsilon') &:= \left|\det\begin{pmatrix} \log|\epsilon| & \log|\epsilon'| \\ \log|\epsilon'| & \log|\epsilon''| \end{pmatrix}\right| \\
&= (\log|\epsilon|)^2 + (\log|\epsilon|)(\log|\epsilon'|) + (\log|\epsilon'|)^2, \\
(\log|\epsilon|)(\log|\epsilon'|) + (\log|\epsilon'|)^2 &= -(\log|\epsilon'|)(\log|\epsilon''|) \le 0, \\
\mathrm{Reg}(\epsilon, \epsilon') &\le (\log|\epsilon|)^2.
\end{aligned}$$

By [Lou12, Lemmas 7–9], if $\Pi_\epsilon(X) \ne X^3 - 20X^2 - 9X - 1$ (for which (2) holds true), $\Pi_\epsilon(X) \ne X^3 - 9X^2 + 6X - 1$ (for which (2) holds true as well) and $\mathbb{Q}(\epsilon)$ is Galois, then

$$d_\epsilon \ge \min\bigl(4(\epsilon-1)^2\epsilon, \epsilon^2, (\epsilon-1)^4/\epsilon^2\bigr) = (\epsilon-1)^4/\epsilon^2 = ((\epsilon-1)/\epsilon)^4\epsilon^2 \ge \epsilon^2/4$$

for $\epsilon \ge 3.49$. Now, by [Lou12, Lemma 4], if $\epsilon < 3.49$, then $\Pi_\epsilon(X) = X^3 - 2X^2 - X + 1$, $X^3 - 3X^2 + 1$ or $X^3 - 3X^2 - X + 1$, and (2) holds true in these three cases. ∎

Let ϵ_1 and ϵ_2 be multiplicatively independent units of a totally real cubic order M. In practice, ϵ_1 and ϵ_2 are defined as any two of the three real roots of a parametrized family of irreducible polynomials $\Pi_n(X) = X^3 - a_nX^2 + b_nX \pm 1 \in \mathbb{Z}[X]$ with positive discriminants, and we take $M = \mathbb{Z}[\epsilon_1, \epsilon_2] = \mathbb{Z}[\epsilon_1, \epsilon_2, \epsilon_3]$, where $\epsilon_3 = a_n - \epsilon_1 - \epsilon_2$ is the third real root of $\Pi_n(X)$. (Or, as in the situation of Theorem 1.1, ϵ_1 and ϵ_2 are of the form $r\epsilon + s \in \mathbb{Z}[\epsilon]$ for some totally real cubic unit ϵ which is a root of a given parametrized family of irreducible cubic polynomials $\Pi_n(X)$, and we take $M = \mathbb{Z}[\epsilon]$.) Let U_M be the group of units of M. How could one prove that $\{\epsilon_1, \epsilon_2\}$ is a system of fundamental units of the order M (whose unit rank is equal to 2)? To begin with, one would try to prove that the index $(U_M : \langle -1, \epsilon_1, \epsilon_2\rangle)$ is uniformly bounded. Notice that (see e.g. [Was2, Lemma 4.15])

$$(U_M : \langle -1, \epsilon_1, \epsilon_2\rangle) = \mathrm{Reg}(\epsilon_1, \epsilon_2)/\mathrm{Reg}(M). \tag{3}$$

Hence using Propositions 2.1 and 2.2, we might expect to obtain a uniform bound on the index $(U_M : \langle -1, \epsilon_1, \epsilon_2\rangle)$.

For example, if ϵ is as in Proposition 2.2, then

$$(U_{\mathbb{Z}[\epsilon,\epsilon']} : \langle -1, \epsilon, \epsilon' \rangle) = \frac{\mathrm{Reg}(\epsilon, \epsilon')}{\mathrm{Reg}(\mathbb{Z}[\epsilon, \epsilon'])} \leq \left(\frac{2\log(4d_\epsilon)}{\log(d_{\mathbb{Z}[\epsilon,\epsilon']}/4)} \right)^2 = \left(\frac{2\log(2f_\epsilon)}{\log(f_{\mathbb{Z}[\epsilon,\epsilon']}/2)} \right)^2,$$

by (1) and (2), and

$$f_\epsilon = (\mathbb{Z}[\epsilon, \epsilon'] : \mathbb{Z}[\epsilon]) f_{\mathbb{Z}[\epsilon,\epsilon']}.$$

Hence, the unit index $(U_{\mathbb{Z}[\epsilon,\epsilon']} : \langle -1, \epsilon, \epsilon' \rangle)$ is small as soon as the order index $(\mathbb{Z}[\epsilon, \epsilon'] : \mathbb{Z}[\epsilon])$ is not too large. More precisely, for any given integer $N > 4$, we see that

$$(\mathbb{Z}[\epsilon, \epsilon'] : \mathbb{Z}[\epsilon]) < \frac{1}{4}(2f_\epsilon)^{1-2/\sqrt{N}} \quad \text{implies} \quad (U_{\mathbb{Z}[\epsilon,\epsilon']} : \langle -1, \epsilon, \epsilon' \rangle) < N.$$

If, as explained in Section 8, we do not know beforehand a formula (in terms of the coefficients of $\Pi_\epsilon(X) = X^3 - aX^2 + bX - c$) for the discriminant $d_{\mathbb{Z}[\epsilon,\epsilon']}$, at least we will be able to compute it for the three families considered in Theorem 1.2.

3. Mistakes in the literature. In this section, we let the assumptions and notation be as in Proposition 2.2.

LEMMA 3.1. *Let α be a cubic algebraic number of minimal polynomial $\Pi_\alpha(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$, of discriminant d_α. Assume that $\mathbb{Q}(\alpha)$ is a cyclic cubic field, i.e. $d_\alpha = f_\alpha^2$ is a the square of some positive integer f_α. Let α, α' and α'' be the three conjugates of α. Then the conductor $f_{\mathbb{Z}[\alpha,\alpha']}$ divides* $\gcd(f_\alpha, a^2 - 3b, b^2 - 3ac)$.

Proof. Since both $d(1, \alpha, \alpha^2) = d_\alpha = f_\alpha^2$, $d(1, \alpha, \alpha')$ and $d(1, \alpha, \alpha^2\alpha')$ divide $d_{\mathbb{Z}[\alpha,\alpha']} = f^2_{\mathbb{Z}[\alpha,\alpha']}$, the desired result follows. Indeed, because of

$$\det \begin{pmatrix} 1 & \alpha & \alpha' \\ 1 & \alpha' & \alpha'' \\ 1 & \alpha'' & \alpha \end{pmatrix} = (\alpha'\alpha + \alpha''\alpha' + \alpha\alpha'') - (\alpha'^2 + \alpha''^2 + \alpha^2) = b - (a^2 - 2b)$$

and

$$\det \begin{pmatrix} 1 & \alpha & \alpha^2\alpha' \\ 1 & \alpha' & \alpha'^2\alpha'' \\ 1 & \alpha'' & \alpha''^2\alpha \end{pmatrix} = \alpha\alpha\alpha''(\alpha'' + \alpha + \alpha') - (\alpha^2\alpha'^2 + \alpha'^2\alpha''^2 + \alpha''^2\alpha^2)$$
$$= ca - (b^2 - 2ca),$$

we have $d(1, \alpha, \alpha') = (a^2 - 3b)^2$ and $d(1, \alpha, \alpha^2\alpha') = (b^2 - 3ac)^2$. ∎

In [Kish, (2.2), proof of Theorem 2], [Tog04, p. 67, line 9, displayed formula for a lower bound for $R_{\mathcal{O}}$, and (2.7) of the proof of Lemma 2.4], [Tog06, (2.7) of the proof of Lemma 2.2] and [Tog08, first assertion of Theorem 2.1], it is wrongly asserted that Cusick's result (Proposition 2.1) yields

$$\text{Reg}(\mathbb{Z}[\epsilon,\epsilon']) \geq \frac{1}{16}\log^2(d_\epsilon/4) = \frac{1}{4}\log^2(f_\epsilon/2). \tag{4}$$

Actually, Cusick proved a much weaker result: there exists some unit ϵ_M in $M = \mathbb{Z}[\epsilon,\epsilon']$ such that

$$\text{Reg}(\mathbb{Z}[\epsilon,\epsilon']) \geq \frac{1}{16}\log^2(d_{\epsilon_M}/4) \geq \frac{1}{16}\log^2(d_{\mathbb{Z}[\epsilon,\epsilon']}/4) = \frac{1}{4}\log^2(f_{\mathbb{Z}[\epsilon,\epsilon']}/2)$$

(since $d_{\mathbb{Z}[\epsilon,\epsilon']}$ divides ϵ, this latter lower bound is indeed weaker than (4)).

Let us give an explicit example showing that (4) can indeed be violated. The conductor $f_K > 1$ of the cubic field $K := \mathbb{Q}(\epsilon)$ divides $f_{\mathbb{Z}[\epsilon,\epsilon']}$, and $f_{\mathbb{Z}[\epsilon,\epsilon']}$ divides $\Delta := \gcd(f_\epsilon, a^2 - 3b, b^2 - 3ac)$ (see Lemma 3.1). Hence, if $\Delta = p$ is a prime number, then $f_K = f_{\mathbb{Z}[\epsilon,\epsilon']} = \Delta = p$. Therefore, $\mathbb{Q}(\epsilon)$ is the only cubic cyclic field K_p of conductor p, whose regulator $\text{Reg}(K_p)$ is given in [Coh, Appendix B.4] if $p \leq 43$, and $\mathbb{Z}[\epsilon,\epsilon']$ is its ring of algebraic integers, which yields $\text{Reg}(\mathbb{Z}[\epsilon,\epsilon']) = \text{Reg}(K_p)$ and makes it easy to check whether (4) is satisfied. For example, if $\Pi_\epsilon(X) = X^3 - 19196X^2 + 83X + 1$, then $f_\epsilon = 5552687$, $\Delta = 7$, $\text{Reg}(\mathbb{Z}[\epsilon,\epsilon']) = \text{Reg}(K_7) = 0.525\ldots$ and (4) is blatantly violated.

4. Lemmas on cubic units. In this short section we state four useful results on cubic units. Lemma 4.2 is an explicit formula for the roots of a cubic polynomial with three real roots. It will be used to compute asymptotics for regulators in parametrized families of cubic fields and numerical values of such regulators. Lemma 4.3 is a formula for the complex conjugates of a cubic algebraic number. Lemma 4.4 gives a $\mathbb{Z}$-generating system for the cubic or sextic order generated by all the complex conjugates of a cubic algebraic number. At the end of the paper we will show that if this order is sextic, then the $\mathbb{Z}$-generating system is a $\mathbb{Z}$-basis (see Lemma 8.1).

LEMMA 4.1. *Let $\epsilon \neq \pm 1$ be a cubic unit. Assume that $\mathbb{Q}(\epsilon)$ is Galois. Then ϵ and ϵ' are multiplicatively independent.*

Proof. Set $X = \log|\epsilon|$ and $Y = \log|\epsilon'|$. According to the beginning of the proof of Proposition 2.2, $\text{Reg}(\epsilon,\epsilon') = X^2 + XY + Y^2 = ((2X+Y)^2 + 3Y^2)/4$ is equal to 0 if and only if $X = Y = 0$. ∎

LEMMA 4.2. *We have $P(X) = X^3 - aX^2 + bX - c = Q(3X - a)/27$, where $Q(Y) = Y^3 - 3pY - q$ with $p = a^2 - 3b$ and $q = 2a^3 - 9ab + 27c$. Moreover, $d_Q = 27^2 d_P = 27(4p^3 - q^2)$. Finally, if $d_P > 0$ and $q \neq 0$, then*

$p > 0$ and the three real roots of $P(X)$ are

$$\epsilon_k := \frac{1}{3}\left(a + 2\frac{q}{|q|}\sqrt{p}\cos\left(\frac{1}{3}\arctan\left(\sqrt{\frac{4p^3-q^2}{q^2}}\right) + \frac{2k\pi}{3}\right)\right), \qquad k \in \{0,1,2\}.$$

LEMMA 4.3 (see [Lou12, proof of Proposition 10]). *Assume that $\Pi(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$ is $\mathbb{Q}$-irreducible and of discriminant $\Delta = -4a^3c - 4b^3 + a^2b^2 + 18abc - 27c^2 = D^2 = (-D)^2$ a square. Set $x(D) = 2a^2 - 6b \in \mathbb{Z}$, $y(D) = -(2a^3 - 7ab + 9c + D) \in \mathbb{Z}$ and $z(D) = a^2b + 3ac - 4b^2 + Da \in \mathbb{Z}$. Then α and*

$$\alpha' = \alpha(D) := \frac{x\alpha^2 + y(D)\alpha + z(D)}{2D}$$

and $\alpha'' = \alpha(-D)$ are the three real roots of $\Pi(X)$.

LEMMA 4.4. *Let α, α' and α'' be the three complex conjugates of a cubic algebraic number α. Then $\{1, \alpha, \alpha^2, \alpha', \alpha\alpha', \alpha^2\alpha'\}$ is a $\mathbb{Z}$-generating system of the cubic or sextic order $\mathbb{Z}[\alpha, \alpha'] = \mathbb{Z}[\alpha, \alpha', \alpha'']$.*

Proof. Since $\alpha + \alpha' + \alpha'' \in \mathbb{Z}$, we do have $\mathbb{Z}[\alpha, \alpha'] = \mathbb{Z}[\alpha, \alpha', \alpha'']$. Since $\alpha^n \in \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2$ and $\alpha'^n \in \mathbb{Z} + \mathbb{Z}\alpha' + \mathbb{Z}\alpha'^2$ for $n \geq 0$, we see that $\{e_{k,l} := \alpha^k\alpha'^l;\ 0 \leq k, l \leq 2\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\alpha, \alpha']$. We prove that we can dispense with $e_{0,2} = \alpha'^2$, $e_{1,2} = \alpha\alpha'^2$ and $e_{2,2} = \alpha^2\alpha'^2$. Indeed, let $\Pi_\alpha(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$ be the minimal polynomial of α. Then $\alpha'^2 = \alpha'^2 - (\alpha^2 - a\alpha + b - c/\alpha) = \alpha'^2 + \alpha'\alpha'' - (\alpha^2 - a\alpha + b) = (a - \alpha)\alpha' - (\alpha^2 - a\alpha + b)$. Hence $\alpha\alpha'^2 = (a\alpha - \alpha^2)\alpha' - (\alpha^3 - a\alpha^2 + b\alpha) = (a\alpha - \alpha^2)\alpha' + c$ and $\alpha^2\alpha'^2 = (a\alpha^2 - \alpha^3)\alpha' + c\alpha = (b\alpha - c)\alpha' + c\alpha$. ∎

5. Proof of Theorem 1.1. We assume that $l \geq 3$. We will use:

LEMMA 5.1 (see [Enn1, Theorem 4.1]). *Let $\mathcal{O}$ be the maximal order of the cubic number field generated by a root ϵ of $\Pi_l(X) = X^3 + (l-1)X^2 - lX - 1$, $l \geq 3$. None of the units $\pm\epsilon$, $\pm(\epsilon - 1)$, $\pm\epsilon(\epsilon - 1)$ and $\pm(\epsilon - 1)/\epsilon$ is a non-trivial power in $\mathcal{O}$, and none of the units $\epsilon^2(\epsilon - 1)$ and $\epsilon(\epsilon - 1)^2$ is a fifth power in $\mathcal{O}$. Hence, 2, 3 and 5 do not divide the index $(\mathcal{O}^* : \langle -1, \epsilon, \epsilon - 1\rangle)$.*

The discriminant d_l of $\Pi_l(X)$ is given by $d_l = (l^2 + 3l - 1)^2 - 32$. Clearly, it is positive and not a square. Hence $\Pi_l(X)$ has three distinct real roots and $K = \mathbb{Q}(\epsilon)$ is not Galois. With the notation of Lemma 4.2, we may assume that $\epsilon = \epsilon_0$, $\epsilon' = \epsilon_1$ and $\epsilon'' = \epsilon_2$. We obtain $\epsilon = -l + O\left(\frac{1}{l^2}\right)$, $\epsilon' = 1 + \frac{1}{l} - \frac{2}{l^2} + \frac{4}{l^3} + O\left(\frac{1}{l^4}\right)$ and $\epsilon'' = -\frac{1}{l} + O\left(\frac{1}{l^2}\right)$ (see also [Lou08b]). Hence,

$$\mathrm{Reg}(\epsilon, \epsilon - 1) = \left|\det\begin{pmatrix} \log|\epsilon| & \log|\epsilon - 1| \\ \log|\epsilon'| & \log|\epsilon' - 1| \end{pmatrix}\right|$$

$$= \left| \det \begin{pmatrix} \log l + O(\frac{1}{l^3}) & \log l + O(\frac{1}{l}) \\ \frac{1}{l} - \frac{5}{2l^2} + O(\frac{1}{l^3}) & -\log l - \frac{2}{l} + \frac{2}{l^2} + O(\frac{1}{l^3}) \end{pmatrix} \right|$$
$$= \log^2 l + \frac{3\log l}{l} - \frac{9\log l}{2l^2} + O\left(\frac{1}{l^2}\right)$$

is asymptotic to $\frac{1}{16}\log^2 d_l$. After having computed by hand an admissible constant κ in this $O(\frac{1}{l^2})$ error term and having done on a desk computer an exact computation of $\mathrm{Reg}(\epsilon, \epsilon')$ (by using Lemma 4.2 and by noticing that here $q = -2l^3 - 3l^2 + 3l + 29 < 0$ for all $l \geq 3$) for the small values of l for which the now explicit expression $-\frac{9\log l}{2l^2} + \frac{\kappa}{l^2}$ is non-negative, i.e. for $3 \leq l \leq e^{2\kappa/9}$, we deduce that

$$\mathrm{Reg}(\epsilon, \epsilon - 1) \leq \log^2 l + \frac{3\log l}{l}.$$

Using (1) and (3), and noticing that $d_M = d_l/(M : \mathbb{Z}[\epsilon])^2 \leq 4d_l/l^{2\alpha}$, we obtain

$$(\mathcal{O}^* : \langle -1, \epsilon, \epsilon - 1\rangle) = \frac{\mathrm{Reg}(\epsilon, \epsilon - 1)}{\mathrm{Reg}(M)} \leq \left(\frac{\log l + 3/(2l)}{\frac{1}{4}\log(d_l/l^{2\alpha})}\right)^2 < 7.$$

Indeed, with our choice of α we have

$$\frac{\sqrt{7}}{4}\log(d_l/l^{2\alpha}) - \log l - \frac{3}{2l} = \frac{\sqrt{7}}{4}\log(d_l/l^4) - \frac{3}{2l} = \frac{3(\sqrt{7}-1)}{2l} + O\left(\frac{1}{l^2}\right) > 0$$

for $l \geq 3$. Using Lemma 5.1, the desired result follows.

6. Proof of Theorem 1.2. Let us consider the family of cyclic cubic fields studied in [Kish]:

LEMMA 6.1. *For $n \in \mathbb{Z}$, the cubic polynomial $\Phi_n(X)$ is $\mathbb{Q}$-irreducible, of discriminant $d_n = f_n^2$ a square, with $f_n = (n^2+1)(n^2+3)(n^4+n^3+4n^2+3)$. Let ϵ, ϵ' and ϵ'' be the three real roots of $\Phi_n(X)$. Then $\{1, \epsilon, \epsilon^2\epsilon'\}$ is a $\mathbb{Z}$-basis of the order $\mathbb{Z}[\epsilon, \epsilon']$ and this order has discriminant $d_{\mathbb{Z}[\epsilon,\epsilon']} = f^2_{\mathbb{Z}[\epsilon,\epsilon']}$ $= d_n/(n^2+1)^2$, with $f_{\mathbb{Z}[\epsilon,\epsilon']} = (n^2+3)(n^4+n^3+4n^2+3)$. Moreover, the unit index $(U_{\mathbb{Z}[\epsilon,\epsilon']} : \langle -1, \epsilon, \epsilon'\rangle)$ is less than 3.*

Proof. We know that $\{1, \epsilon, \epsilon^2, \epsilon', \epsilon\epsilon', \epsilon^2\epsilon'\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\epsilon, \epsilon']$ (Lemma 4.4). Notice also that $\mathbb{Z}[\epsilon] = \mathbb{Z} + \mathbb{Z}\epsilon + \mathbb{Z}\epsilon^2$. Set

$$\eta_0 = \frac{\epsilon^2 - (n-1)\epsilon - n}{n^2+1} \quad \text{and} \quad \eta_1 = \frac{n\epsilon^2 + (n+1)\epsilon + 1}{n^2+1} = n\eta_0 + \epsilon + 1.$$

Since $\epsilon^3 = a\epsilon^2 - b\epsilon + c$ and $\epsilon^4 = (a^2-b)\epsilon^2 + (c-ab)\epsilon + ac$, we deduce that $\epsilon' = x\epsilon^2 + y\epsilon + z$ yields $\epsilon\epsilon' = (ax+y)\epsilon^2 + (z-bx)\epsilon + cx$ and $\epsilon^2\epsilon' = (a(ax+y) + z - bx)\epsilon^2 + (cx - b(ax+y))\epsilon + c(ax+y)$. Using Lemma 4.3, we then obtain $\epsilon' = -\eta_0 + P(\epsilon)$ with $P(\epsilon) \in \mathbb{Z}[\epsilon]$, $\epsilon\epsilon' = -\eta_1 + Q(\epsilon)$ with

$Q(\epsilon) \in \mathbb{Z}[\epsilon]$, and

$$\epsilon^2\epsilon' = \eta_0 - (n+1)(n^2+n+3)\epsilon - 1. \tag{5}$$

Hence, $\{1, \epsilon, \epsilon^2, \eta_0, \eta_1\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\epsilon, \epsilon']$. Since $\eta_1 - n\eta_0 = \epsilon + 1 \in \mathbb{Z}[\epsilon]$, $\{1, \epsilon, \epsilon^2, \eta_0\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\epsilon, \epsilon']$. Since $\epsilon^2 = (n^2+1)\eta_0 + (n-1)\epsilon + n$, $\{1, \epsilon, \eta_0\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\epsilon, \epsilon']$. Finally, by (5), $\{1, \epsilon, \epsilon^2\epsilon'\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\epsilon, \epsilon']$ and the expression for its discriminant follows from the last assertion of the proof of Lemma 3.1.

As in the proof of Theorem 1.1, with the notation of Lemma 4.2, we may assume that $\epsilon = \epsilon_0$, $\epsilon' = \epsilon_1$ and $\epsilon'' = \epsilon_2$. Noticing that $q > 0$ for $n \geq 0$ and $q < 0$ for $n \leq -1$, we obtain $\epsilon = n^5 + O(n^4) = n^5\big(1 + O\big(\frac{1}{n}\big)\big)$, $\epsilon' = -\frac{1}{n^2} + O\big(\frac{1}{n^3}\big) = -\frac{1}{n^2}\big(1 + O\big(\frac{1}{n}\big)\big)$, $\epsilon'' = -\frac{1}{n^3} + O\big(\frac{1}{n^4}\big) = -\frac{1}{n^3}\big(1 + O\big(\frac{1}{n}\big)\big)$ and

$$\begin{aligned}
\operatorname{Reg}(\epsilon, \epsilon') &= \left| \det \begin{pmatrix} \log|\epsilon| & \log|\epsilon'| \\ \log|\epsilon'| & \log|\epsilon''| \end{pmatrix} \right| \\
&= \left| \det \begin{pmatrix} 5\log|n| + O\big(\frac{1}{n}\big) & -2\log|n| + O\big(\frac{1}{n}\big) \\ -2\log|n| + O\big(\frac{1}{n}\big) & -3\log|n| + O\big(\frac{1}{n}\big) \end{pmatrix} \right| \\
&= 19\log^2|n| + O\left(\frac{\log|n|}{n}\right).
\end{aligned}$$

In fact, we have the more precise asymptotics

$$\operatorname{Reg}(\epsilon, \epsilon') = 19\log^2|n| + \frac{8\log|n|}{n} + O\left(\frac{\log|n|}{n^2}\right).$$

Since

$$\operatorname{Reg}(\mathbb{Z}[\epsilon, \epsilon']) \geq \frac{1}{16}\log^2\frac{d_{\mathbb{Z}[\epsilon,\epsilon']}}{4} = \frac{1}{4}\log^2\frac{(n^2+3)(n^4+n^3+4n^2+3)}{2},$$

we have

$$(U_{\mathbb{Z}[\epsilon,\epsilon']} : \langle -1, \epsilon, \epsilon' \rangle) = \frac{\operatorname{Reg}(\epsilon, \epsilon')}{\operatorname{Reg}(\mathbb{Z}[\epsilon, \epsilon'])} \leq \frac{19}{9} + O\left(\frac{1}{\log|n|}\right),$$

and $(U_{\mathbb{Z}[\epsilon,\epsilon']} : \langle -1, \epsilon, \epsilon' \rangle) < 3$ for $|n|$ large enough. After having computed by hand an admissible constant κ in this $O(1/\log|n|)$ error term and having done on a desk computer an exact computation of $\operatorname{Reg}(\epsilon, \epsilon')$ (by using Lemma 4.2) for the small values of n for which the now explicit expression $\frac{19}{9} + \frac{\kappa}{\log|n|}$ is not smaller than 3, i.e. for $|n| \leq e^{9\kappa/8}$, we deduce that the last assertion holds true for any $n \in \mathbb{Z}$ (notice that here $q < 0$ for all $n \in \mathbb{Z}_{\leq -1}$ and $q > 0$ for all $n \in \mathbb{Z}_{\geq 0}$). ∎

Let us now consider the family of cyclic cubic fields studied in [Tog04] and [Was1]:

LEMMA 6.2. *For $1 \neq n \in \mathbb{Z}$, the cubic polynomial $\Xi_n(X)$ is $\mathbb{Q}$-irreducible, of discriminant $d_n = f_n^2$ a square, with $f_n = (n-1)(n^2+3)(n^2-3n+3)$. Let ϵ, ϵ' and ϵ'' be the three real roots of $\Xi_n(X)$. Then $\{1, \epsilon, \epsilon^2\epsilon'\}$ is a $\mathbb{Z}$-basis of the order $\mathbb{Z}[\epsilon, \epsilon']$ and this order is of discriminant $d_{\mathbb{Z}[\epsilon,\epsilon']} = f^2_{\mathbb{Z}[\epsilon,\epsilon']} = d_n/(n-1)^2$, with $f_{\mathbb{Z}[\epsilon,\epsilon']} = (n^2+3)(n^2-3n+3)$. Moreover, for $n \neq 1, 2$, the unit index $(U_{\mathbb{Z}[\epsilon,\epsilon']} : \langle -1, \epsilon, \epsilon' \rangle)$ is less than 3.*

Proof. The proof is the same as that of Lemma 6.1. Set

$$\eta_0 = \frac{\epsilon^2 - 1}{n-1}.$$

We obtain $\epsilon = \eta_0 + P(\epsilon)$ with $P(\epsilon) \in \mathbb{Z}[\epsilon]$, $\epsilon\epsilon' = -\eta_0 + Q(\epsilon)$ with $Q(\epsilon) \in \mathbb{Z}[\epsilon]$, and

$$\epsilon^2\epsilon' = \eta_0 - (n^2+1)\epsilon - 1. \tag{6}$$

Hence, $\{1, \epsilon, \epsilon^2, \eta_0\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\epsilon, \epsilon']$. Since $\epsilon^2 = (n-1)\eta_0 + 1$, $\{1, \epsilon, \eta_0\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\epsilon, \epsilon']$. Finally, by (6), $\{1, \epsilon, \epsilon^2\epsilon'\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\epsilon, \epsilon']$ and the expression for its discriminant follows from the last assertion of the proof of Lemma 3.1.

With the notation of Lemma 4.2, we may assume that $\epsilon = \epsilon_0$, $\epsilon' = \epsilon_1$ and $\epsilon'' = \epsilon_2$. We obtain $\epsilon = n^3 + O(n^2) = n^3\big(1 + O\big(\frac{1}{n}\big)\big)$, $\epsilon' = -\frac{1}{n} + O\big(\frac{1}{n^2}\big) = -\frac{1}{n}\big(1 + O\big(\frac{1}{n}\big)\big)$, $\epsilon'' = -\frac{1}{n^2} + O\big(\frac{1}{n^3}\big) = -\frac{1}{n^2}\big(1 + O\big(\frac{1}{n}\big)\big)$ and

$$\begin{aligned}
\mathrm{Reg}(\epsilon, \epsilon') &= \left| \det \begin{pmatrix} \log|\epsilon| & \log|\epsilon'| \\ \log|\epsilon'| & \log|\epsilon''| \end{pmatrix} \right| \\
&= \left| \det \begin{pmatrix} 3\log|n| + O\big(\frac{1}{n}\big) & -\log|n| + O\big(\frac{1}{n}\big) \\ -\log|n| + O\big(\frac{1}{n}\big) & -2\log|n| + O\big(\frac{1}{n}\big) \end{pmatrix} \right| \\
&= 7\log^2|n| + O\left(\frac{\log|n|}{n}\right).
\end{aligned}$$

In fact, we have the more precise asymptotics

$$\mathrm{Reg}(\epsilon, \epsilon') = 7\log^2|n| - \frac{9\log|n|}{n} + O\left(\frac{\log|n|}{n^2}\right).$$

Since

$$\mathrm{Reg}(\mathbb{Z}[\epsilon, \epsilon']) \geq \frac{1}{16}\log^2\frac{d_{\mathbb{Z}[\epsilon,\epsilon']}}{4} = \frac{1}{4}\log^2\frac{(n^2+3)(n^2-3n+3)}{2},$$

we have

$$(U_{\mathbb{Z}[\epsilon,\epsilon']} : \langle -1, \epsilon, \epsilon' \rangle) = \frac{\mathrm{Reg}(\epsilon, \epsilon')}{\mathrm{Reg}(\mathbb{Z}[\epsilon, \epsilon'])} \leq \frac{7}{4} + O\left(\frac{1}{\log|n|}\right),$$

and $(U_{\mathbb{Z}[\epsilon,\epsilon']} : \langle -1, \epsilon, \epsilon' \rangle) < 3$ for $|n|$ large enough. As at the end of the proof of Lemma 6.1, we deduce that the last assertion holds true for any $1, 2 \neq n \in \mathbb{Z}$ (notice that here $q < 0$ for all $n \in \mathbb{Z}_{\leq 0}$ and $q > 0$ for all $n \in \mathbb{Z}_{\geq 1}$). Indeed, for $n = 2$, $\epsilon'\epsilon^2 = \eta_0 - (n^2+1)\epsilon = \epsilon^2 - 5\epsilon - 2 = \eta^3$ is a cube, where $\eta = \epsilon^2 - 4\epsilon - 2 \in \mathbb{Z}[\epsilon] \subseteq \mathbb{Z}[\epsilon, \epsilon']$ (check that $\phi_2(x) = x^3 - 3x^2 - 4x - 1$ divides $(x^2 - 4x - 2)^3 - (x^2 - 5x - 2)$). ∎

REMARK 6.3. Write $f_{\mathbb{Z}[\epsilon,\epsilon']} = (n^2+3)(n^2-3n+3) = 9^\delta b$, with $\delta = 0$ if $n \not\equiv 0 \pmod 3$ and $\delta = 1$ if $n \equiv 0 \pmod 3$ (hence, $\gcd(b, 3) = 1$). According to Lemma 6.2 and [Was1, Theorem 1], if b is squarefree, then $\mathbb{Z}[\epsilon, \epsilon']$ is the maximal order of $\mathbb{Q}(\epsilon)$.

Let us finally consider the family of cyclic cubic fields studied in [Tog06]:

LEMMA 6.4. *For $n \in \mathbb{Z}$, the cubic polynomial $\Psi_n(X)$ is $\mathbb{Q}$-irreducible, of discriminant $d_n = f_n^2$ a square, with $f_n = (n^2 - n + 1)(n^3 + n - 1)$ $\times (n^4 + 2n^3 + 4n^2 + 3n + 3)(n^4 - n^3 + n^2 - 3n + 3)$. Let ϵ, ϵ' and ϵ'' be the three real roots of $\Psi_n(X)$. Then $\{1, \epsilon, \epsilon^2\epsilon'\}$ is a $\mathbb{Z}$-basis of the order $\mathbb{Z}[\epsilon, \epsilon']$ and this order is of discriminant $d_{\mathbb{Z}[\epsilon,\epsilon']} = f^2_{\mathbb{Z}[\epsilon,\epsilon']} = d_n/(n^3 - n + 1)^2$, with $f_{\mathbb{Z}[\epsilon,\epsilon']} = (n^2 - n + 1)(n^4 + 2n^3 + 4n^2 + 3n + 3)(n^4 - n^3 + n^2 - 3n + 3)$. Moreover, the unit index $(U_{\mathbb{Z}[\epsilon,\epsilon']} : \langle -1, \epsilon, \epsilon' \rangle)$ is less than 3.*

Proof. Here again, the proof is the same as that of Lemma 6.1. Set

$$\eta_1 = \frac{\epsilon^2 + \epsilon - n}{n^3 + n - 1} \quad \text{and} \quad \eta_0 = \frac{n^2\epsilon^2 + n^2\epsilon + n - 1}{n^3 + n - 1} = n^2\eta_1 + 1.$$

We obtain $\epsilon' = \eta_0 + P(\epsilon)$ with $P(\epsilon) \in \mathbb{Z}[\epsilon]$, $\epsilon\epsilon' = -n\eta_1 + Q(\epsilon)$ with $Q(\epsilon) \in \mathbb{Z}[\epsilon]$, and

$$\epsilon^2\epsilon' = \eta_1 + n\epsilon. \tag{7}$$

Hence, $\{1, \epsilon, \epsilon^2, \eta_0, \eta_1\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\epsilon, \epsilon']$. Since $\eta_0 - n^2\eta_1 = 1 \in \mathbb{Z}[\epsilon]$, $\{1, \epsilon, \epsilon^2, \eta_1\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\epsilon, \epsilon']$. Since $\epsilon^2 = (n^3 + n - 1)\eta_1 - \epsilon + n$, $\{1, \epsilon, \eta_1\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\epsilon, \epsilon']$. Finally, by (7), $\{1, \epsilon, \epsilon^2\epsilon'\}$ is a $\mathbb{Z}$-generating system of $\mathbb{Z}[\epsilon, \epsilon']$ and the expression for its discriminant follows from the last assertion of the proof of Lemma 3.1.

With the notation of Lemma 4.2, we may assume that $\epsilon = \epsilon_0$, $\epsilon' = \epsilon_1$ and $\epsilon'' = \epsilon_2$. We obtain $\epsilon = -n^8 + O(n^6) = -n^8\big(1 + O\big(\frac{1}{n^2}\big)\big)$, $\epsilon' = \frac{1}{n^3} + O\big(\frac{1}{n^5}\big) = \frac{1}{n^3}\big(1 + O\big(\frac{1}{n^2}\big)\big)$, $\epsilon'' = -\frac{1}{n^5} + O\big(\frac{1}{n^7}\big) = -\frac{1}{n^5}\big(1 + O\big(\frac{1}{n^2}\big)\big)$ and

$$\mathrm{Reg}(\epsilon, \epsilon') = \left| \det \begin{pmatrix} \log|\epsilon| & \log|\epsilon'| \\ \log|\epsilon'| & \log|\epsilon''| \end{pmatrix} \right|$$

$$= \left|\det \begin{pmatrix} 8\log|n| + O\left(\frac{1}{n^2}\right) & -3\log|n| + O\left(\frac{1}{n^2}\right) \\ -3\log|n| + O\left(\frac{1}{n^2}\right) & -5\log|n| + O\left(\frac{1}{n^2}\right) \end{pmatrix}\right|$$
$$= 49\log^2|n| + O\left(\frac{\log|n|}{n^2}\right).$$

In fact, we have the more precise asymptotics

$$\mathrm{Reg}(\epsilon,\epsilon') = 49\log^2|n| + \frac{24\log|n|}{n^2} + O\left(\frac{\log|n|}{n^3}\right).$$

Since

$$\mathrm{Reg}(\mathbb{Z}[\epsilon,\epsilon']) \geq \frac{1}{16}\log^2\frac{d_{\mathbb{Z}[\epsilon,\epsilon']}}{4}$$
$$= \frac{1}{4}\log^2\frac{(n^2-n+1)(n^4+2n^3+4n^2+3n+3)(n^4-n^3+n^2-3n+3)}{2},$$

we have

$$(U_{\mathbb{Z}[\epsilon,\epsilon']} : \langle -1,\epsilon,\epsilon'\rangle) = \frac{\mathrm{Reg}(\epsilon,\epsilon')}{\mathrm{Reg}(\mathbb{Z}[\epsilon,\epsilon'])} \leq \frac{49}{25} + O\left(\frac{1}{\log|n|}\right),$$

and $(U_{\mathbb{Z}[\epsilon,\epsilon']} : \langle -1,\epsilon,\epsilon'\rangle) < 3$ for $|n|$ large enough. As at the end of the proof of Lemma 6.1, we deduce that the last assertion holds true for any $1 \neq n \in \mathbb{Z}$ (notice that here $q < 0$ for all $n \in \mathbb{Z}$). ∎

LEMMA 6.5. *In the situation of Lemmas* 6.1, 6.2 *and* 6.4, *the unit index* $(U_{\mathbb{Z}[\epsilon,\epsilon']} : \langle -1,\epsilon,\epsilon'\rangle)$ *is odd.*

Proof. This index is even if and only if ϵ, $-\epsilon$, ϵ' or $-\epsilon'$ is a square, which implies that ϵ or $-\epsilon$ is totally positive. If $\Pi_\epsilon(X) = X^3 - aX^2 + bX - c$, this implies $a > 0$, $b > 0$ and $c > 0$, or $a < 0$, $b > 0$ and $c < 0$. Since in our situations we have $c = 1 > 0$, we only need to notice that $a < 0$ or $b < 0$. ∎

7. Proof of Theorem 1.3. Let us come back to the proof of Lemma 6.2. Since $n \geq 3$, we have $\mathrm{Reg}(\epsilon,\epsilon') < 7\log^2 n$, $d_{\mathbb{Z}[\epsilon,\epsilon']} = ((n^2+3)(n^2-3n+3))^2 \geq \frac{16}{81}n^8$ and $d_M = d_{\mathbb{Z}[\epsilon,\epsilon']}/(M : \mathbb{Z}[\epsilon,\epsilon'])^2 \geq 4n^{8-2\alpha}$. Hence,

$$(U_M : \langle -1,\epsilon,\epsilon'\rangle) = \frac{\mathrm{Reg}(\epsilon,\epsilon')}{\mathrm{Reg}(M)} \leq \frac{16\mathrm{Reg}(\epsilon,\epsilon')}{\log^2(d_M/4)} < \frac{16\cdot 7}{4(4-\alpha)^2} = 3.$$

8. Conclusion and open problems

8.1. Remarks on Godwin's example. Let us consider the family of cyclic cubic fields (introduced in [God]) associated with the polynomials $\Pi_b(X) = X^3 - X^2 - \frac{9b^2-1}{4}X + b^2$, with b odd, of discriminant $d_b = (b(27b^2+1)/4)^2$ a square (in fact, in [God] it is assumed that $b = B^2$ is a square). If θ denotes any of its three real roots, then its conjugates

are $\phi = \left(\theta^2 - \frac{b+1}{2}\theta - \frac{3b^2-b}{2}\right)/b$ (by Lemma 4.3) and $\psi = 1 - \theta - \phi$. Set $\epsilon := (3\phi - 1)/(3\theta - 1)$. After a little computation we found that

$$\epsilon = \frac{6}{b}\theta^2 - \frac{3}{b}\theta - \frac{27b+1}{2}$$

and that ϵ is a cubic algebraic unit of the minimal polynomial

$$\Pi_m(X) = X^3 - mX^2 - (m+3)X - 1 \quad \text{with } m = -3(9b+1)/2.$$

Hence, Godwin's cubic fields are simplest cubic fields and he should have cited [Cohn] for the evenness of the class number and [Sha] for the fundamental units.

8.2. The discriminant of the sextic order $\mathbb{Z}[\epsilon, \epsilon', \epsilon'']$ when $\mathbb{Q}(\epsilon)$ is not Galois

LEMMA 8.1. *Let α, α' and α'' be the three complex conjugates of a cubic algebraic number α. Assume that the cubic extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois. Then $\{1, \alpha, \alpha^2, \alpha', \alpha\alpha', \alpha^2\alpha'\}$ is a $\mathbb{Z}$-basis of the order $\mathbb{Z}[\alpha, \alpha'] = \mathbb{Z}[\alpha, \alpha', \alpha'']$ and $d(1, \alpha, \alpha^2, \alpha', \alpha\alpha', \alpha^2\alpha') = d_\alpha^3$.*

Proof. The normal closure N of the cubic number field $\mathbb{Q}(\alpha)$ is a sextic number field with Galois group the permutation group $\mathcal{S}_3 = \{\sigma_i;\ 0 \le i \le 5\}$ of order 6, where $\sigma_0 = \mathrm{Id}$, $\sigma_1 = (1,2)$, $\sigma_2 = (2,3)$, $\sigma_3 = (3,1)$, $\sigma_4 = (1,2,3)$ and $\sigma_5 = (1,3,2)$. Here, $\mathcal{S}_3$ acts on the three roots $\alpha_1 = \alpha$, $\alpha_2 = \alpha'$ and $\alpha_2 = \alpha''$ by permutation of the indices. The first assertion of the lemma follows from Lemma 4.4. To compute $d(1, \alpha, \alpha^2, \alpha', \alpha\alpha', \alpha^2\alpha') = \det\left[\mathrm{Tr}_{N/\mathbb{Q}}(\eta_i\eta_j)\right]_{1\le i,j\le 6}$, where $\eta_1 = 1$, $\eta_2 = \alpha$, $\eta_3 = \alpha^2$, $\eta_4 = \alpha'$, $\eta_5 = \alpha\alpha'$ and $\eta_6 = \alpha^2\alpha'$, we notice that

$$\begin{aligned}\mathrm{Tr}_{N/\mathbb{Q}}(\alpha^k\alpha'^l) &= \sum_{i=1}^{6} \sigma_i(\alpha_1)^k\sigma_i(\alpha_2)^l \\ &= (\alpha^k\alpha'^l + \alpha^l\alpha'^k) + (\alpha^k\alpha''^l + \alpha^l\alpha''^k) + (\alpha'^k\alpha''^l + \alpha'^l\alpha''^k)\end{aligned}$$

is a symmetric polynomial in α, α' and α''. Hence, it can be expressed as a polynomial in $\mathbb{Z}[a, b, c]$, where $\Pi_\alpha(X) = X^3 - aX^2 + bX - c \in \mathbb{Z}[X]$ of discriminant $d_\alpha = -4a^3c - 4b^3 + a^2b^2 + 18abc - 27c^2$ is the minimal polynomial of α. We deduce that $d(1, \alpha, \alpha^2, \alpha', \alpha\alpha', \alpha^2\alpha')$ is equal to

$$\det\begin{pmatrix} 6 & 2a & 2a^2-4b & 2a & 2b & ab-3c \\ 2a & 2a^2-4b & U & 2b & ab-3c & V \\ 2a^2-4b & U & W & ab-3c & V & X \\ 2a & 2b & ab-3c & 2a^2-4b & ab-3c & 2b^2-4ac \\ 2b & ab-3c & V & ab-3c & 2b^2-4ac & Y \\ ab-3c & V & X & 2b^2-4ac & Y & Z \end{pmatrix},$$

where $U = 2a^3 - 6ab + 6c$, $V = a^2b - ac - 2b^2$, $W = 2a^4 - 8a^2b + 8ac + 4b^2$, $X = a^3b - a^2c - 3ab^2 + 5bc$, $Y = -2a^2c + ab^2 - bc$ and $Z = -2a^3c + a^2b^2 + 4abc - 2b^3 - 3c^2$, and any mathematical software yields the desired result. ∎

This lemma raises the following more general question:

QUESTION 1. Let α be an algebraic number of degree n. Let α_k, $1 \le k \le n$, be its complex conjugates. Assume that the normal closure $N = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ of $\mathbb{Q}(\alpha)$ is of degree $n!$. Is the discriminant $d_{\mathbb{Z}[\alpha_1,\dots,\alpha_n]}$ of the order $\mathbb{Z}[\alpha_1, \dots, \alpha_n]$ an explicit perfect power of d_α? And can one exhibit a $\mathbb{Z}$-basis of this order?

8.3. System of fundamental units for some totally imaginary sextic orders. Let $\epsilon > 1$ be a real cubic unit of negative discriminant $-d_\epsilon < 0$. Then $K = \mathbb{Q}(\epsilon)$ is not normal, the conjugates of ϵ are ϵ, η and $\bar{\eta}$ for some non-real algebraic unit η. The normal closure $N = \mathbb{Q}(\epsilon, \eta)$ of K is a totally imaginary sextic field. The unit rank U_M of the sextic order $M = \mathbb{Z}[\epsilon, \eta] = \mathbb{Z}[\epsilon, \eta, \bar{\eta}]$ is equal to 2, and using $|\eta| = 1/\sqrt{\epsilon}$ we have

$$\mathrm{Reg}(\epsilon, \eta) = \left| \det \begin{pmatrix} 2\log|\epsilon| & 2\log|\eta| \\ 2\log|\eta| & 2\log|\bar{\eta}| \end{pmatrix} \right| = 3\log^2 \epsilon \neq 0.$$

Hence, ϵ and η are multiplicatively independent, and it is natural to ask:

QUESTION 2. Is $\{\epsilon, \eta\}$ a system of fundamental units of this order?

Recall that (3) gives $(U_M : \langle -1, \epsilon, \eta \rangle) = \mathrm{Reg}(\epsilon, \eta)/\mathrm{Reg}(M)$. Since $d_\epsilon \ge \epsilon^2/3$ (see [Lou06, Theorem 2] or [Lou10, Theorem 1]), we have

$$\mathrm{Reg}(\epsilon, \eta) \le \frac{3}{4} \log^2(3d_\epsilon).$$

On the other hand, $d_M = d_{\mathbb{Z}[\epsilon,\eta]} = d_\epsilon^3$. Using [CF] and [Sil] we deduce that $\mathrm{Reg}(N) \gg \log^2 d_K$. Hence, if we could adapt the proofs of these papers to the case of arbitrary modules M of N, we could expect a lower bound $\mathrm{Reg}(M) \gg \log^2 d_M = 9 \log^2 d_\epsilon$ and we we would end up with a uniform bound on $(U_M : \langle -1, \epsilon, \eta \rangle)$. At least, let us give here a precise general result:

THEOREM 8.2. *Let $\epsilon > 1$ be a real cubic unit of negative discriminant $-d_\epsilon < 0$. Let η be any complex conjugate of ϵ. Let $N = \mathbb{Q}(\epsilon, \eta)$ be the normal closure of the cubic field $K = \mathbb{Q}(\epsilon)$. Let $L = \mathbb{Q}(\sqrt{-d_\epsilon})$ be the imaginary quadratic subfield of N. Assume that $U_L = \mu_L = \{\pm 1\}$ and ϵ is the fundamental unit of the order $\mathbb{Z}[\epsilon]$ (see* [Lou06, Theorem 4] *and* [Nag] *for a characterization). Set $M = \mathbb{Z}[\epsilon, \eta]$. Then $(U_M : \langle -1, \epsilon, \eta \rangle)$ divides 9.*

Proof. We adapt the proof of [FT, Theorem 43]. We stick to their notation: σ is the generator of $\mathrm{Gal}(N/L)$ such that $\sigma(\epsilon) = \bar{\tau}$ and τ is the nontrivial element of $\mathrm{Gal}(N/K)$. Then $K_2 = \mathbb{Q}(\eta)$ and $K_3 = \mathbb{Q}(\bar{\eta})$. Since ϵ is the fundamental unit of the order $\mathbb{Z}[\epsilon]$, it follows that η and $\bar{\eta}$ are the fundamental units of $\mathbb{Z}[\eta]$ and $\mathbb{Z}[\bar{\eta}]$, respectively. Now, if $\beta \in U_N$, then $N_{N/L}(\beta) \in U_L = \mu_L = \{\pm 1\}$. Hence, if $\alpha \in U_M$, then $\alpha^3 = \pm\alpha^{1+\tau}\alpha^{1+\sigma\tau}\alpha^{1+\sigma^2\tau}$. Now, we claim that $\alpha^{1+\tau} \in \mathbb{Z}[\epsilon]$, $\alpha^{1+\sigma\tau} \in \mathbb{Z}[\eta]$ and $\alpha^{1+\sigma^2\tau} \in \mathbb{Z}[\bar{\eta}]$, which will yield $\alpha^3 \in \langle -1, \epsilon, \eta\rangle)$, and will give the desired result (in our situation we cannot use [FT]'s last argument to prove that this index divides 3, for ϵ could be a cube in K without being a cube in $\mathbb{Z}[\epsilon]$). So, let $\alpha = \sum_{1\le k,l\le m} a_{k,l}\epsilon^k\eta^l$ be in $\mathbb{Z}[\epsilon,\eta]$, $a_{k,l} \in \mathbb{Z}$. Since $\tau(\epsilon) = \epsilon$ and $\tau(\eta) = \bar{\eta}$, we have

$$\alpha^{1+\tau} = \sum_{\substack{1\le k,l,k',l'\le m\\ l<l'}} a_{k,l}a_{k',l'}\epsilon^{k+k'}(\eta^{l'-l} + \bar{\eta}^{l'-l}) + \sum_{1\le k,l,k'} a_{k,l}a_{k',l}\epsilon^{k+k'}(\eta\bar{\eta})^l.$$

Since $\eta\bar{\eta} = 1/\epsilon \in \mathbb{Z}[\epsilon]$ (for ϵ is a unit of this order) and $\eta^n + \bar{\eta}^n = \mathrm{Tr}_{K/\mathbb{Q}}(\epsilon^n) - \epsilon^n \in \mathbb{Z}[\epsilon]$ it follows that $\alpha^{1+\tau} \in \mathbb{Z}[\epsilon]$. The proofs of the other two claims are similar (for example, to prove $\alpha^{1+\sigma\tau} \in \mathbb{Z}[\eta]$, notice that $\mathbb{Z}[\epsilon,\eta] = \mathbb{Z}[\epsilon,\eta,\bar{\eta}] = \mathbb{Z}[\eta,\bar{\eta}]$ for $\mathrm{Tr}_{K/\mathbb{Q}}(\epsilon) = \epsilon+\eta+\bar{\eta} \in \mathbb{Z}$, and that $\sigma\tau(\eta) = \eta$ and $\sigma\tau(\bar{\eta}) = \epsilon$). ∎

This also leaves open the following question (we know the answer if M is a totally real cubic order, by [BHMMS], [MS] and [Lou12]):

Question 3. If ϵ is a given unit of a totally imaginary sextic order M, does there always exist a second unit $\eta \in M$ such that $\{\epsilon, \eta\}$ is a system of fundamental units of this order?

8.4. The discriminant of the cubic order $\mathbb{Z}[\epsilon, \epsilon', \epsilon'']$ when $\mathbb{Q}(\epsilon)$ is Galois. Let ϵ be a cubic algebraic unit. Assume that $\mathbb{Q}(\epsilon)$ is Galois. We know that $\{1, \epsilon, \epsilon^2, \epsilon', \epsilon\epsilon', \epsilon^2\epsilon'\}$ is a $\mathbb{Z}$-generating system of the order $\mathbb{Z}[\epsilon, \epsilon']$ (Lemma 4.4). Lemma 3.1 gives some information on the conductor of this cubic order.

Question 4. Is it possible to derive (from Lemma 4.3?) an expression for a $\mathbb{Z}$-basis of this order and/or to compute its discriminant and conductor?

References

[BHMMS] J. Beers, D. Henshaw, C. Mccall, S. Mulay and M. Spindler, *Fundamentality of a cubic unit u for $\mathbb{Z}[u]$*, Math. Comp. 80 (2011), 563–578; Corrigenda and addenda, ibid. 81 (2012), 2383–2387.

[Coh] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, Berlin, 1993.

[Cohn] H. Cohn, *A device for generating fields of even class number*, Proc. Amer. Math. Soc. 7 (1956), 595–598.

[CF] A. Costa and E. Friedman, *Ratios of regulators in extensions of number fields*, Proc. Amer. Math. Soc. 119 (1993), 381–390.

[Cus] T. W. Cusick, *Lower bounds for regulators*, in: Lecture Notes in Math. 1068, Springer, Berlin, 1984, 63–73.

[Enn1] V. Ennola, *Cubic number fields with exceptional units*, in: Computational Number Theory (Debrecen, 1989), de Gruyter, Berlin, 1991, 103–128.

[Enn2] V. Ennola, *Fundamental units in a family of cubic fields*, J. Théor. Nombres Bordeaux 16 (2004), 569–575.

[FT] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Stud. Adv. Math. 27, Cambridge Univ. Press, Cambridge, 1993.

[God] H. J. Godwin, *A parametrized set of cyclic cubic fields with even class-number*, J. Number Theory 22 (1986), 246–248.

[Kish] Y. Kishi, *A family of cyclic cubic polynomials whose roots are systems of fundamental units*, J. Number Theory 102 (2003), 90–106.

[LL] J. H. Lee and S. Louboutin, *Determination of the orders generated by a cyclic cubic unit that are Galois invariant*, submitted.

[Lou06] S. Louboutin, *The class-number one problem for some real cubic number fields with negative discriminants*, J. Number Theory 121 (2006), 30–39.

[Lou08a] S. Louboutin, *The fundamental unit of some quadratic, cubic or quartic orders*, J. Ramanujan Math. Soc. 23 (2008), 191–210.

[Lou08b] S. Louboutin, *Localization of the complex zeros of parametrized families of polynomials*, J. Symbolic Comput. 43 (2008), 304–309.

[Lou10] S. Louboutin, *On some cubic or quartic algebraic units*, J. Number Theory 130 (2010), 956–960.

[Lou12] S. Louboutin, *On the fundamental units of a totally real cubic order generated by a unit*, Proc. Amer. Math. Soc. 140 (2012), 429–436.

[MS] S. Mulay and M. Spindler, *The positive discriminant case of Nagell's theorem for certain cubic orders*, J. Number Theory 131 (2011), 470–486.

[Nag] T. Nagell, *Zur Theorie der kubischen Irrationalitäten*, Acta Math. 55 (1930), 33–65.

[Sha] D. Shanks, *The simplest cubic fields*, Math. Comp. 310 (1979), 33–55.

[Sil] J. H. Silverman, *An inequality relating the regulator and the discriminant of a number field*, J. Number Theory 19 (1984), 437–442.

[Tha] F. Thaine, *On the construction of families of cyclic polynomials whose roots are units*, Experiment. Math. 17 (2008), 315–331.

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

[Tog04] A. Togbé, *A parametric family of cubic Thue equations*, J. Number Theory 107 (2004), 63–79.

[Tog06] A. Togbé, *Complete solutions of a family of cubic Thue equations*, J. Théor. Nombres Bordeaux 18 (2006), 285–298.

[Tog08] A. Togbé, *On the solutions of a parametric family of cubic Thue equations*, Bull. Braz. Math. Soc. 39 (2008), 537–554.

[Was1] L. C. Washington, *A family of cubic fields and zeros of 3-adic L-functions*, J. Number Theory 63 (1997), 408–417.

[Was2] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1997.

Jun Ho Lee
School of Mathematics
Korea Institute for
Advanced Study (KIAS)
85 Hoegiro, Dongdaemun-gu
Seoul 130-722, Republic of Korea
E-mail: jhleee@kias.re.kr

Stéphane R. Louboutin
Aix Marseille Université
CNRS, Centrale Marseille, I2M, UMR 7373
13453 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 on 6.3.2014
and in revised form on 22.5.2014 (7746)