Journal de Théorie des Nombres
de Bordeaux **16** (2004), 569–575

Fundamental units in a family of cubic fields

par VEIKKO ENNOLA

RÉSUMÉ. Soit $\mathcal{O}$ l'ordre maximal du corps cubique engendré par une racine ε de l'equation $x^3 + (\ell - 1)x^2 - \ell x - 1 = 0$, où $\ell \in \mathbb{Z}$, $\ell \geq 3$. Nous prouvons que $\varepsilon, \varepsilon - 1$ forment un système fondamental d'unités dans $\mathcal{O}$, si $[\mathcal{O} : \mathbb{Z}[\varepsilon]] \leq \ell/3$.

ABSTRACT. Let $\mathcal{O}$ be the maximal order of the cubic field generated by a zero ε of $x^3 + (\ell - 1)x^2 - \ell x - 1$ for $\ell \in \mathbb{Z}$, $\ell \geq 3$. We prove that $\varepsilon, \varepsilon - 1$ is a fundamental pair of units for $\mathcal{O}$, if $[\mathcal{O} : \mathbb{Z}[\varepsilon]] \leq \ell/3$.

1. Introduction

Many computational methods in number theory depend on the knowledge of the unit group of an order in an algebraic number field. Especially, several parametrized families of cubic orders with a given fundamental pair of units are known (see, e.g., [3] and papers cited there). However, it seems that the results mostly suffer from the incompleteness that either it is not known whether the units also form a fundamental pair of units for the maximal order of the field (cf. the corrigendum to [4]), or this is achieved by imposing a further restrictive condition. E.g., in the case of a non-Galois cubic field this means in practice that the discriminant of the defining polynomial is assumed to be square-free.

In an earlier paper [2] we gathered together basic arithmetic facts and further results and conjectures about the two families of cubic fields containing exceptional units, the main emphasis laying on the non-abelian family. This is the set $\mathcal{F} = \{F_\ell\}$, where

$$F_\ell = \mathbb{Q}(\varepsilon), \quad \mathrm{Irr}(\varepsilon, \mathbb{Q}) = f_\ell(x) = x^3 + (\ell - 1)x^2 - \ell x - 1, \quad \ell \geq 3.$$

For each ℓ, we fix ε somehow among its conjugates in order to get a unique field F_ℓ. Here $\ell \geq 3$ is a natural limitation to avoid duplication and to exclude from the family three fields one of which is cyclic and the other two are not totally real.

E. Thomas [5] proved that $\varepsilon, \varepsilon - 1$ is a fundamental pair of units for the order $\mathbb{Z}[\varepsilon]$, and in [2, Conjecture 4.1] we conjectured that the same is true

Manuscrit reçu le 20 juin 2003.

for the maximal order $\mathcal{O} = \mathcal{O}_{F_\ell}$. Using the Voronoi algorithm in the cases when the discriminant $D = D(f_\ell)$ of the polynomial $f_\ell(x)$ is divisible by the square of a prime $p \neq 7$, we were able to show that the conjecture is true for $3 \leq \ell \leq 500$.

The main problem in this context is whether a unit of the form $\varepsilon^a(\varepsilon-1)^b$ is a non-trivial pth power in F_ℓ. For $(a,b) = (2,1)$ or $(1,2)$ we showed in [2] that it is not so if $p = 5$, and claimed that the same holds for any prime p. We have been able to prove this by means of a very tedious computation, the details of which are uninteresting. As suggested in [2], the crucial question here is a successful choice of the approximation polynomial q. The following construction seems to work in all cases: Suppose that $\eta^p = \varepsilon^a(\varepsilon-1)^b$, where $\eta \in F_\ell$, p is an odd prime, and a and b are coprime positive integers less than p. Put $\delta = 1$, if a is even and b is odd, and $\delta = -1$ otherwise. Take

$$q = \delta \mathrm{Tr}(\eta^{-a-b}) + \mathrm{Tr}(\eta^a) + \mathrm{Tr}(\eta^b),$$

where Tr denotes the trace from F_ℓ to $\mathbb{Q}$. This choice is different from the one in [2], but so far it has worked well in each case investigated.

Let j denote the index $[\mathcal{O} : \mathbb{Z}[\varepsilon]]$. Our purpose is to prove the following result which shows that the conjecture is true if j is not too large:

Theorem. *If $j = [\mathcal{O} : \mathbb{Z}[\varepsilon]] \leq \ell/3$, then $\varepsilon, \varepsilon - 1$ is a fundamental pair of units for the maximal order $\mathcal{O}$ of the field F_ℓ.*

Using Maple we have computed the prime factorization of D and have verified that, for $3 \leq \ell \leq 10000$, D has a squared factor k^2 with $k > \ell/3$ only in a few cases, and that in these cases $k \equiv 0 \mod 7$, $D \not\equiv 0 \mod 7^3$, so that (see Lemma 1) j is a divisor of $k/7$. One can then check that $j \leq \ell/3$. Therefore, $\varepsilon, \varepsilon - 1$ is a fundamental pair of units for $\mathcal{O}$ if $3 \leq \ell \leq 10000$.

2. Basic lemmas

These lemmas are contained in [2], but in order to make the proof of the theorem self-contained, we repeat their proofs shortly here. Note that j^2 is a divisor of D, in fact, D/j^2 is the discriminant of the field F_ℓ. By $p^m \parallel c$ we mean that $p^m \mid c$, $p^{m+1} \nmid c$.

Lemma 1. (i) *If $\ell \not\equiv 2 \mod 7$, then $7 \nmid D$.*

(ii) *If $\ell \equiv 2 \mod 7$, but $\ell \not\equiv 23 \mod 49$, then $7^2 \parallel D$, $7 \nmid j$.*

(iii) *If $\ell \equiv 23 \mod 49$, then $7^3 \parallel D$, $7^1 \parallel j$.*

Proof. The polynomial discriminant D has the expression

$$D = \ell^4 + 6\ell^3 + 7\ell^2 - 6\ell - 31 = (\ell^2 + 3\ell - 1)^2 - 32. \tag{1}$$

Note that every prime divisor of D is $\equiv \pm 1 \mod 8$.

It is easy to see that (i) holds, e.g., by direct computation. Suppose therefore, that $\ell \equiv 2 \mod 7$. Substituting $\ell = 2 + 7n$ in (1) we get

$$D \equiv 49\big((2n+1)^2 + 14(n^2+n)\big) \mod 7^4.$$

Hence $7^3 \parallel D$ only for $n \equiv 3 \mod 7$, i.e., $\ell \equiv 23 \mod 49$, and otherwise $7^2 \parallel D$.

For $\ell \not\equiv 23 \mod 49$,

$$f_\ell(x+2) = x^3 + (\ell+5)x^2 + (3\ell+8)x + 2\ell + 3$$

is an Eisenstein polynomial modulo 7, so that 7 is fully ramified in F_ℓ, and (ii) follows.

For $\ell \equiv 23 \mod 49$, (iii) is a consequence of $(\varepsilon - 2)^2/7 \in \mathcal{O}$. This fact can be seen in many ways, the most straightforward but perhaps not the cleverest method being to compute the minimal polynomial. □

Lemma 2. *The ring $\mathcal{O}$ has a $\mathbb{Z}$-basis of the form $1, \varepsilon, \alpha$, where $\alpha = (u + v\varepsilon + \varepsilon^2)/j$, and the integers u, v are determined by $0 \le u, v < j$ and*

$$28u \equiv -2\ell^3 - 9\ell^2 - 11\ell + 11, \quad 28v \equiv \ell^3 + \ell^2 + 9\ell - 30 \mod (7, j)j. \tag{2}$$

Proof. We shall use a theorem of Voronoi [1, p. 111, Theorem I]. Put $a = 2(\ell^2 + \ell + 1)$, $b = \ell^2 - \ell - 9$. Since the resultant of a and b with respect to ℓ equals 336 and b is odd, the gcd (a, b) is a divisor of 21.

Firstly, we must show that the simultaneous congruences

$$f_\ell(x) \equiv 0 \mod k^3, \quad f'_\ell(x) \equiv 0 \mod k^2, \quad \tfrac{1}{2}f''_\ell(x) \equiv 0 \mod k$$

do not have a common solution for any $k > 1$. Suppose the contrary. It follows from the identities

$$\begin{aligned} 9f_\ell(x) - (3x + \ell - 1)f'_\ell(x) &= -ax + b, \\ -12f'_\ell(x) + f''_\ell(x)^2 &= 2a, \end{aligned} \tag{3}$$

that $k^2 \mid (a, b)$, a contradiction.

Hence $\mathcal{O}$ has an integral basis of the required form, where u and v have to be determined. Put $j' = j/(7, j)$, so that $7 \nmid j'$. By Voronoi's theorem we have

$$u \equiv t^2 + (\ell - 1)t - \ell, \quad v \equiv t + \ell - 1 \mod j', \tag{4}$$

where t is a solution of the congruences

$$f_\ell(t) \equiv 0 \mod j'^2, \quad f'_\ell(t) \equiv 0 \mod j'. \tag{5}$$

Further useful identities are

$$a^2 f'_\ell(b/a) = -9D, \tag{6}$$

$$a(3\ell^3 + 10\ell^2 - 22\ell - 41) + 392 = (6\ell - 10)D. \tag{7}$$

It follows from (7) that $(a, j') = 1$, and then from the equations (3), (6) that $t = b/a$ is a solution of (5). Substituting $t = b/a$ in (4) and using (7) to remove the denominators, we obtain after a short computation the congruences (2) modulo j'.

Suppose finally that $7 \mid j$, i.e., $\ell \equiv 23 \mod 49$. In this case

$$f_\ell(2) \equiv 0 \mod 7^2, \quad f'_\ell(2) \equiv 0 \mod 7,$$

so that Voronoi's theorem implies $u \equiv 4$, $v \equiv 3 \mod 7$. This is in accordance with (2) modulo 49. □

3. Proof of the theorem

For the basic facts concerning Voronoi's algorithm in totally real cubic fields, see [1], Chapter IV. For any number $\vartheta \in F_\ell$, let $\vartheta, \vartheta', \vartheta''$ (or $\vartheta^{(i)}, i = 0, 1, 2$) be the conjugates, and let $\overline{\vartheta} = (\vartheta, \vartheta', \vartheta'')$ be the corresponding vector in $\mathbb{R}^3$. We choose the order of the conjugates so that

$$1 < \varepsilon < 1 + \ell^{-1}, \quad -\ell^{-1} < \varepsilon' < 0, \quad -\ell < \varepsilon'' < -\ell + \ell^{-2}. \tag{8}$$

Let $\Lambda = \{\overline{\vartheta} | \vartheta \in \mathcal{O}\}$ be the lattice in $\mathbb{R}^3$ corresponding to $\mathcal{O}$. The theorem is an immediate consequence of the following

Lemma 3. *Suppose that $j \le \ell/3$. Let $\overline{\xi}$ and $\overline{\eta}$ be the relative minima of Λ adjacent to $\overline{1}$ on the positive x- and y-axis, respectively. Then*

$$\xi = (\varepsilon - 1)^{-1}, \qquad \eta = \varepsilon^{-1}.$$

Proof. We apply the result of Lemma 2. Since $\varepsilon - 1$ is a unit, it is clear that $\overline{(\varepsilon - 1)^{-1}}$ is a relative minimum of Λ. It follows from (8) that

$$|\varepsilon' - 1|^{-1} < 1, \quad |\varepsilon'' - 1|^{-1} < 1,$$

so that ξ must satisfy the conditions

$$|\xi| \le |\varepsilon - 1|^{-1}, \quad |\xi'| < 1, \quad |\xi''| < 1. \tag{9}$$

Since $\xi \in \mathcal{O}$, there are integers x, y, z such that

$$x + y\varepsilon^{(i)} + z\alpha^{(i)} = \xi^{(i)} \qquad (i = 0, 1, 2). \tag{10}$$

Consider (10) as a system of linear equations in the unknowns x, y, z. The determinant of the system is $-\sqrt{D}/j$. Here the square root is positive, and to get the correct sign we use (8). It follows that

$$\sqrt{D}z/j = (\varepsilon' - \varepsilon'')\xi + (\varepsilon'' - \varepsilon)\xi' + (\varepsilon - \varepsilon')\xi''. \tag{11}$$

Changing the sign of ξ, if necessary, we may assume that $z \ge 0$.

From (1) we have $\sqrt{D} > \ell^2 + 3\ell - 2$, so that (11), (9) and (8) imply

$$\begin{aligned}(\ell^2 + 3\ell - 2)z/j &< (\varepsilon' - \varepsilon'')/(\varepsilon - 1) + \varepsilon - \varepsilon'' + \varepsilon - \varepsilon' \\ &= \ell - 1 + 3\varepsilon + \varepsilon(\ell + \varepsilon)(\varepsilon' - \varepsilon'') \\ &< \ell^2 + 3\ell + 6.\end{aligned}$$

Since $j \leq \ell/3$, it follows that $z \leq j$.

Subtract the equations (10) with $i = 1, 2$. Substituting the expressions of α' and α'' we obtain after a short computation

$$jy - (\ell - v)z = (\varepsilon - 1)z + j(\xi' - \xi'')/(\varepsilon' - \varepsilon''). \tag{12}$$

The absolute value of the right-hand side is less than

$$j(\varepsilon - 1 + 2/(\varepsilon' - \varepsilon'')).$$

We shall show that this expression is less than $3j/\ell \leq 1$, so that the final result will be

$$jy = (\ell - v)z. \tag{13}$$

For that purpose it is enough to show that

$$(1 + 3\ell^{-1} - \varepsilon)(\varepsilon' - \varepsilon'') > 2. \tag{14}$$

The following improved bound for ε is valid: $\varepsilon < r$, where

$$r = 1 + \ell^{-1} - 2\ell^{-2} + 4\ell^{-3}.$$

To see this, check that $f_\ell(1) < 0$, $f_\ell(r) > 0$. We then have

$$(1 + 3\ell^{-1} - \varepsilon)(\varepsilon' - \varepsilon'') > (1 + 3\ell^{-1} - r)(-\ell^{-1} + \ell - \ell^{-2}),$$

which is easily seen to be > 2 if $\ell \geq 4$. For $\ell = 3$ one can simply compute the approximate values of $\varepsilon, \varepsilon', \varepsilon''$ and check that (14) holds even then.

We have thus proved (13). We contend that $(j, \ell - v) = 1$ which implies

$$y = \ell - v, \quad z = j, \tag{15}$$

because $z \leq j$, $v < j \leq \ell/3$, and the possibility $z = y = 0$ is absurd.

Suppose that $\ell - v$ and j are both divisible by a prime p. If $p = 7$, then Lemma 1 gives $\ell \equiv 23 \mod 49$, but then $v \equiv \ell \equiv 2 \mod 7$ leads to a contradiction with (2). Hence $p \neq 7$. From (2) we have $h(\ell) \equiv 0 \mod p$, where

$$h(\ell) = \ell^3 + \ell^2 - 19\ell - 30.$$

On the other hand

$$(3\ell^2 + \ell - 7)h(\ell) - (3\ell - 14)D = 112(\ell - 2),$$

so that $\ell \equiv 2 \mod p$ and $h(\ell) \equiv h(2) \equiv -56 \mod p$, which is impossible.

Hence (15) is true, whence $\xi = x + u + \ell\varepsilon + \varepsilon^2 = x + u + (\varepsilon - 1)^{-1}$. Looking at (8), one can see that the two last conditions (9) are only satisfied for

$x+u=0$ or 1. However, the first condition (9) does not hold for $x+u=1$. It follows that $\xi=(\varepsilon-1)^{-1}$, and the first part of the lemma is proved.

The proof that $\eta=\varepsilon^{-1}$ is very much the same. The number η satisfies the conditions

$$|\eta|<1, \quad |\eta'|\le|\varepsilon'|^{-1}, \quad |\eta''|<1. \tag{16}$$

Again there are integers x,y,z such that

$$x+y\varepsilon^{(i)}+z\alpha^{(i)}=\eta^{(i)} \qquad (i=0,1,2). \tag{17}$$

We may assume that $z\ge 0$, and we can prove that $z\le j$ as before. Subtracting the equations (17) with $i=0,2$ we obtain the following analogue of (12):

$$jy-(\ell-v-1)z=\varepsilon' z+j(\eta-\eta'')/(\varepsilon-\varepsilon''). \tag{18}$$

In order to achieve the result

$$jy=(\ell-v-1)z \tag{19}$$

we have to show that the absolute value of the right-hand side of (18) is less than 1. This is true if we can show that

$$(\varepsilon-\varepsilon'')(3\ell^{-1}+\varepsilon')>2. \tag{20}$$

But (20) follows easily from (8). Hence (19) holds.

Suppose now that j and $\ell-v-1$ are both divisible by a prime p. If $p=7$, then $\ell\equiv 23 \mod 49$ and $v\equiv\ell-1\equiv 1 \mod 7$, which contradicts (2). Thus $p\ne 7$. Since $v\equiv\ell-1 \mod p$, it follows from (2) that $h(\ell)+28\equiv 0 \mod p$. On the other hand,

$$(2\ell^3+9\ell^2+11\ell-11)(h(\ell)+28)-(2\ell^2-\ell-26)D=-784,$$

which is impossible. As before, we now have

$$y=\ell-v-1, \quad z=j,$$

so that $\eta=x+u+\ell+\varepsilon^{-1}$. However, the first and third condition (16) are only satisfied for $x+u+\ell=0$. This completes the proof. □

References

[1] B. N. DELONE, D. K. FADDEEV, *The Theory of Irrationalities of the Third Degree.* Trudy Mat. Inst. Steklov, vol. **11** (1940); English transl., Transl. Math. Monographs, vol. **10**, Amer. Math. Soc., Providence, R. I., Second printing 1978.

[2] V. ENNOLA, *Cubic number fields with exceptional units.* Computational Number Theory (A. Pethö et al., eds.), de Gruyter, Berlin, 1991, pp. 103–128.

[3] H. G. GRUNDMAN, *Systems of fundamental units in cubic orders.* J. Number Theory **50** (1995), 119–127.

[4] M. MIGNOTTE, N. TZANAKIS, *On a family of cubics.* J. Number Theory **39** (1991), 41–49, Corrigendum and addendum, **41** (1992), 128.

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

Veikko ENNOLA
Department of Mathematics
University of Turku
FIN-20014, Finland
E-mail : ennola@utu.fi