ON THE FUNDAMENTAL UNIT OF A PURELY CUBIC FIELD

RONALD JOEL RUDMAN
ON THE FUNDAMENTAL UNIT OF A PURELY CUBIC FIELD

RONALD J. RUDMAN

Let \( a = D^3 + d \), where \( a, D, d \) are rational integers with \( D, a > 0 \), \( |d| > 1 \), and \( d \mid 3D^2 \). It is proved that the fundamental unit of the field \( \mathbb{Q}(\omega) \), where \( \omega = \sqrt[3]{a} \), is \( (\omega - D)^d/d \) with only six exceptions.

1. Introduction. The purpose of this paper is to establish the following result:

**Theorem 1.** Let \( a = D^3 + d \), where \( a, D, d \in \mathbb{Z} \), with \( a, D > 0 \), \( |d| > 1 \), and \( a \) cubefree. Then \( \varepsilon = (\omega - D)^d/d \), where \( \omega = \sqrt[3]{a} \), is a unit of \( K = \mathbb{Q}(\omega) \) if and only if \( d \mid 3D^2 \). Moreover, in this case \( \varepsilon = \eta \), the fundamental unit of \( K \), except for \((D, d) = (2, -6), (1, 3), (2, 2), (3, 1), \) and \((5, -25)\), where \( \varepsilon = \eta^2 \), and \((2, -4)\), where \( \varepsilon = \eta^3 \).

Here, \( \mathbb{Z}, \mathbb{Q} \) denote respectively the rational integers and the field of rationals.

Theorem 1 is an extension of a result of Stender [4], who showed that when

- (1) \( a = D^3 + d \), \( d \mid D, \ d > 1 \)
- (2) \( a = D^3 + 3d \), \( d \mid D, \ 3d \leq D, \ d > 0 \)
- (3) \( a = D^3 + 3D \), \( D \geq 2 \)
- (4) \( a = D^3 - d \), \( d \mid D, \ 4 < 4d \leq D \)

or

- (5) \( a = D^3 - 3d \), \( d \mid D, \ 12d \leq D, \ d > 0 \)

\( \varepsilon = (\omega - D)^d/(\omega^3 - D^3) = \eta \), except for \((D, d) = (2, 2)\) in (1), where \( \varepsilon = \eta^2 \). The case \( d = 1 \) in (1) and (4) had already been settled by Nagell [2], who proved that \( \varepsilon = \eta \) with the single exception of \( a = 28 \), when \( \varepsilon = \eta^3 \). The method of proof used here follows [4].

2. Preliminaries. We now make the assumption that \( d \mid 3D^2 \).

Since \( a \) is cubefree we put \( a = mn^3 \) with \( m \) squarefree. Also, \( d \) is cubefree, as \( d \mid 3a \).

Let \( \bar{a} = mn^2, \ \bar{\omega} = \sqrt[3]{\bar{a}} \), and \( \zeta \) be the fundamental unit of the ring \( R = [1, \omega, \bar{\omega}] \). It is well known that if \( a \not\equiv \pm 1 \pmod{9} \), an integral basis for \( K \) is \( \langle 1, \omega, \bar{\omega} \rangle \) (a field of the first kind). However, if \( a \equiv \pm 1 \pmod{9} \), an integral basis for \( K \) is given by
(a field of the second kind) and each integer of $K$ is representable in the form $(x + y\omega + z\bar{\omega})/3$. If $\zeta \neq \gamma$ then $K$ is of the second kind and $\zeta = \gamma^2$ [3].

Now, if $\vartheta \in K \cap (0, 1)$ and if $\varepsilon = \vartheta^t$, $t$ a natural number, then it is easily seen [4] that for $\varepsilon', \varepsilon''$ the (complex) conjugates of $\varepsilon$, $\vartheta = (x + y\omega + z\bar{\omega})/3$ implies that

$$\begin{cases} |x| < \sigma \\
|y| < \sigma/\omega \\
|z| < \sigma/\bar{\omega}
\end{cases}$$

where

$$\sigma = 1 + 2|\varepsilon'|^t.$$  

3. We observe that $\varepsilon = 1 + (3D^2/d)\omega - (3D/d)\omega^2$ satisfies the equation $\varepsilon^2 - 3\varepsilon + (3 + 27D^3a/d^2)t - 1 = 0$. Hence $\varepsilon$ is a unit of $K$ if and only if $a^2 | 27D^3a$. Putting $x = 3D^2/d = p/q$ with $(p, q) = 1$, we can write the quotient as $3x(x + 3)$, i.e., $3p(p + 3q)/q^2$. It follows that $\varepsilon$ is a unit if and only if $q^2 = 1$, i.e., $d | 3D^3$. But since $a$ is cubefree, this is equivalent to $d | 3D^2$.

**Lemma 1.** If $(D, d) \neq (2, -6)$ then

$$1 < |\varepsilon'| < \begin{cases} \frac{6D\omega^2/d}{6D^2\omega^2/d^2} & \text{if } d > 0 \\
\frac{6D^2\omega^2/d}{6D\omega^2/d} & \text{if } d < 0
\end{cases}.$$

**Proof.** Since $(\omega - D)^3 = d - 3D\omega(\omega - D)$, we see that $(\omega - D)^3 < d$ if and only if $d > 0$ and hence $0 < \varepsilon < 1$. Therefore $\varepsilon + 2 < 3$ and since $\omega > 3/2$, 

$$1 < |\varepsilon'|^2 = \frac{1}{4}\left[2 - \frac{3D^2}{d}\omega + \frac{3D}{d}\omega^2 \right]^2 + \frac{3}{4}\left[\frac{3D}{d}\omega(D + \omega) \right]^2$$

$$< \left(\frac{3D}{d}\omega\right)^2\left[D^2 + \frac{3}{4}(D + \omega)^2\right]$$

and the result follows.

**Proposition 1.** If $(D, d) \neq (2, -6), (1, 3)$ then $\varepsilon$ is not a square in $R$.

**Proof.** We first assume that $d | D^2$. This implies that $d | a$ and hence we may write $d = uvz$ where $u | m$, $v | n$. Putting $D^2 = de$, $n = vr$ and assuming that $\varepsilon = (x + y\omega + z\bar{\omega})^2$, we obtain, by equating coefficients in the basis $\langle 1, \omega, \bar{\omega} \rangle$,
(7) \[ x^2 + 2mrvyz = 1 \]
(8) \[ az^2/v^2r^2 + 2xy = 3e \]
(9) \[ rvy^2 + 2xz = -3r(D/uv) \].

Since (7) implies \((x, r) = 1\) we see from (9) that \(r \mid 2z\) and hence \(r^2 \leq 4z^2\).

If \(d > 0\), so that \(u, e > 0\), (7) and (9) respectively imply that \(yz \leq 0\) and \(xz < 0\). Since \(y = 0\) implies that \(r = 3r^2(m/u)\), we conclude that \(xy > 0\). It therefore follows from (8) that \(Du < 12\). The pairs \((D, d)\) for which this inequality holds (and which are not considered in [4]) are seen to be \((2, 4), (3, 9), (5, 25), (6, 4), (6, 9), (6, 36), (10, 4), (10, 25), (10, 100),\) and \((11, 121)\). In each case it is immediate that (7), (8), and (9) cannot all be satisfied. We prove this for the pair \((6, 9)\), the other proofs being similar: here we obtain \(x^2 + 30yz = 1\), \(z^2j = 12\), and \(15y^2 + 2xz = -30\). These lead to \(xy < 6\) and hence \(30yz < 24\).

If \(d < 0\) then we see from (7), (8) that \(yz \leq 0\) and \(xy < 0\). Since \(z = 0\) implies that \(9de^2 = 16\), we conclude that \(xz > 0\). Hence \(|y| < (3D/d)|^{1/3}\), while (9) implies that \(8|xy| \geq (a/v^2) - 12e\). Combining these with (6) and Lemma 1 and assuming that \(D \geq 5\) we obtain after a straightforward calculation that \((D - 1)u < 13\). It then follows directly that none of the thirteen pairs \((D, d)\) for which this last inequality holds can satisfy (7), (8), and (9).

Considering separately \(D \leq 5, d < 0\), we obtain \(\eta\) directly by the algorithm of Berwick [1] which has been programmed by the author. The results show that for \((D, d) = (2, -2), (3, -9), (4, -4),\) and \((4, -2)\) we have \(\epsilon = \zeta = \gamma\), for \((2, -4)\) \(\epsilon = \zeta^2 = \gamma^2\), and for \((5, -25)\) \(\epsilon = \zeta = \gamma^2\). The proposition is therefore true in these cases also.

In general, \(d \mid 3D^2\) but we may now assume \(d \mid D^2\) so that \(d = 3d_0\), where \(d_0 \mid D^2\). Replacing \(d\) by \(d_0\) and proceeding as before, we obtain for \(d > 0\), \(Du < 4\), and for \(d < 0\), \((D - 3)u < 9\). Here it is easily seen that only in the cases \((D, d) = (2, -6), (1, 3)\) is \(\epsilon\) a square in \(R\).

**Proposition 2.** If \((D, d) \neq (2, -4)\) then \(\epsilon\) is not a cube in \(R\).

**Proof.** \(\epsilon^{1/3} = (\omega - D)/\sqrt[3]{d} \in K\) if and only if \(\sqrt[3]{d} \in K\). Since \(d\) is cubefree, this would imply that \(\sqrt[3]{d}\) generates \(K\). It then follows by considering traces that \(|d| = a\) or \(\bar{a}\), which forces us to conclude that \((D, d) = (2, -4)\).

**Proposition 3.** If \((D, d) \neq (2, -6), (2, -4), (1, 3),\) or \((5, -25)\), then \(\epsilon = \zeta\).

**Proof.** Let \(\zeta = (x + y\omega + z\bar{\omega})\) and suppose that \(\epsilon = \zeta^t, t > 1\).
By Propositions 1 and 2, \( t \) is not divisible by 2 or 3. Hence for \( d > 0 \) we obtain from (6) and Lemma 1 that \( |y| < 1/3 + 2/3 (6/D^2d)^{15} < 1 \). For \( d < 0 \) the cases \( D \leq 5 \) have already been considered in the proof of Proposition 1. We may therefore assume that \( D > 5 \) and hence \( |y| < 1/3 + 2/3 (6D^2/d(\omega)^{15} < 1 \). Thus \( y = 0 \), and expanding \((x + z\omega)^t\) we find that

\[
1 = \left( \sum_{k=0}^{t} \binom{t}{k} \frac{t}{3k} x^{t-k} z^k (\alpha)^k \right)
\]

and since each term in the sum is divisible by \( x \), \( x = \pm 1 \). But then \( 1 = N(\pm 1 + z\omega) = \pm 1 + \alpha z^2 \), together with \( \alpha > 2 \), yields a contradiction.

4. **Proof of Theorem 1.** By Proposition 3 we may assume \( K \) is of the first kind. Therefore it suffices to prove that \( 9e \neq (x + y\omega + z\omega)^2 \) for integral \( x, y, z \). We see that here \( d \mid D^2 \), for otherwise \( a = D^3 + 3d_0 \), where \( d_0 \mid D^2 \), \( 3 \nmid d_0 \), and since \( D^3 \equiv 0 \), \( \pm 1 \pmod{9} \), we have \( a \not\equiv \pm 1 \pmod{9} \).

Proceeding as in the proof of Proposition 1 we obtain

\[
\begin{align*}
x^2 + 2mrxyz &= 9 \\
xz^2 + 2xyr^2 &= 27e \\
rzy^2 + 2xzr &= -3r(D/uv)
\end{align*}
\]

Since \( 3 \mid r \) implies that \( a = mn^2 \equiv 0 \pmod{9} \) we again find that \((x, r) = 1 \). Here, we obtain for \( d > 0 \), \( Du < 108 \), while if \( d < 0 \) and \( D > 5 \) we have \((D - 1)u < 123 \). The result now follows by individually considering each of the fifty-three pairs \((D, d)\) to which these inequalities give rise, the equations (10) having no solution in these cases.

**References**


Received February 28, 1972. This research comprised a part of the author's Ph. D. thesis at the University of California, Los Angeles. The author wishes to express his gratitude to his advisor, Professor Basil Gordon, for numerous illuminating discussions.

Wayne State University
<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allan Francis Abrahamse</td>
<td>Uniform integrability of derivatives on ( \sigma )-lattices</td>
<td>1</td>
</tr>
<tr>
<td>Ronald Alter and K. K. Kubota</td>
<td>The diophantine equation ( x^2 + D = p^n )</td>
<td>11</td>
</tr>
<tr>
<td>Grahame Bennett</td>
<td>Some inclusion theorems for sequence spaces</td>
<td>17</td>
</tr>
<tr>
<td>William Cutler</td>
<td>On extending isotopies</td>
<td>31</td>
</tr>
<tr>
<td>Robert Jay Daverman</td>
<td>Factored codimension one cells in Euclidean ( n )-space</td>
<td>37</td>
</tr>
<tr>
<td>Patrick Barry Eberlein and Barrett O’Neill</td>
<td>Visibility manifolds</td>
<td>45</td>
</tr>
<tr>
<td>M. Edelstein</td>
<td>Concerning dentability</td>
<td>111</td>
</tr>
<tr>
<td>Edward Graham Evans, Jr.</td>
<td>Krull-Schmidt and cancellation over local rings</td>
<td>115</td>
</tr>
<tr>
<td>C. D. Feustel</td>
<td>A generalization of Kneser’s conjecture</td>
<td>123</td>
</tr>
<tr>
<td>Avner Friedman</td>
<td>Uniqueness for the Cauchy problem for degenerate parabolic equations</td>
<td>131</td>
</tr>
<tr>
<td>David Golber</td>
<td>The cohomological description of a torus</td>
<td>149</td>
</tr>
<tr>
<td>Alain Goullet de Rugy</td>
<td>Un théorème du genre “Andô-Edwards” pour les Fréchet ordonnés normaux</td>
<td>155</td>
</tr>
<tr>
<td>Louise Hay</td>
<td>The class of recursively enumerable subsets of a recursively enumerable set</td>
<td>167</td>
</tr>
<tr>
<td>John Paul Helm, Albert Ronald da Silva Meyer, Paul Ruel Young</td>
<td>On orders of translations and enumerations</td>
<td>185</td>
</tr>
<tr>
<td>Julien O. Hennefeld</td>
<td>A decomposition for ( B(X)^* ) and unique Hahn-Banach extensions</td>
<td>197</td>
</tr>
<tr>
<td>Gordon G. Johnson</td>
<td>Moment sequences in Hilbert space</td>
<td>201</td>
</tr>
<tr>
<td>Thomas Rollin Kramer</td>
<td>A note on countably subparacompact spaces</td>
<td>209</td>
</tr>
<tr>
<td>Yves A. Lequain</td>
<td>Differential simplicity and extensions of a derivation</td>
<td>215</td>
</tr>
<tr>
<td>Peter Lorimer</td>
<td>A property of the groups ( Aut , PU(3, q^2) )</td>
<td>225</td>
</tr>
<tr>
<td>Yasou Matsugu</td>
<td>The Levi problem for a product manifold</td>
<td>231</td>
</tr>
<tr>
<td>John M.F. O’Connell</td>
<td>Real parts of uniform algebras</td>
<td>235</td>
</tr>
<tr>
<td>William Lindall Paschke</td>
<td>A factorable Banach algebra without bounded approximate unit</td>
<td>249</td>
</tr>
<tr>
<td>Ronald Joel Rudman</td>
<td>On the fundamental unit of a purely cubic field</td>
<td>253</td>
</tr>
<tr>
<td>Tsuan Wu Ting</td>
<td>Torsional rigidities in the elastic-plastic torsion of simply connected cylindrical bars</td>
<td>257</td>
</tr>
<tr>
<td>Philip C. Tonne</td>
<td>Matrix representations for linear transformations on analytic sequences</td>
<td>269</td>
</tr>
<tr>
<td>Jung-Hsien Tsai</td>
<td>On ( E )-compact spaces and generalizations of perfect mappings</td>
<td>275</td>
</tr>
<tr>
<td>Alfons Van Daele</td>
<td>The upper envelope of invariant functionals majorized by an invariant weight</td>
<td>283</td>
</tr>
<tr>
<td>Giulio Varsi</td>
<td>The multidimensional content of the frustum of the simplex</td>
<td>303</td>
</tr>
</tbody>
</table>