Elements of small norm in Shanks’ cubic extensions of imaginary quadratic fields

Peter Kirschenhofer, Jörg M. Thuswaldner

Department of Mathematics and Statistics, University of Leoben, Franz-Josef-Strasse 18, A-8700 Leoben, Austria

Received 19 November 2003; accepted 18 May 2004
Available online 4 August 2004

Abstract

Let $k = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic number field with ring of integers $\mathbb{Z}_k$ and let $k(\alpha)$ be the cubic extension of $k$ generated by the polynomial

$$f_t(x) = x^3 - (t - 1)x^2 - (t + 2)x - 1$$

with $t \in \mathbb{Z}_k$. In the present paper we characterize all elements $\gamma \in \mathbb{Z}_k[\alpha]$ with norms satisfying $|N_{k(\alpha)/k}| \leq |2t + 1|$ for $|t| \geq 14$. This generalizes a corresponding result by Lemmermeyer and Pethő for Shanks’ cubic fields over the rationals.

© 2004 Elsevier Ltd. All rights reserved.

MSC: 11R16

Keywords: Shanks’ extension; Small norm

1. Introduction and main result

In Lemmermeyer and Pethő (1995) Lemmermeyer and Pethő have characterized the principal ideals of small norm in Shanks’ (Shanks, 1974) simplest cubic fields over the rationals. This result has turned out to be of great importance for the treatment of certain
classes of Thue equations (cf. Mignotte et al., 1996). In the present paper we will generalize the main result of Lemmermeyer and Pethő (1995) to the corresponding extensions over imaginary quadratic number fields \( \mathbb{Q}(\sqrt{-D}) \). Interestingly, for small discriminants \( D \) we face a richer variety of elements of small norm than in the rational case.

For square-free \( D \in \mathbb{N} \) let \( k := \mathbb{Q}(\sqrt{-D}) \) and \( \mathbb{Z}_k \) be the corresponding ring of integers. For \( t \in \mathbb{Z}_k \) we define the polynomial

\[
f_t(x) := x^3 - (t - 1)x^2 - (t + 2)x - 1.
\]

Let \( \alpha = \alpha^{(1)} \) be a root of \( f_t \). Then the other roots of \( f_t \) are given by

\[
\alpha^{(2)} = -1 - \frac{1}{\alpha}, \quad \alpha^{(3)} = -\frac{1}{\alpha + 1} \tag{1}
\]

(cf. Heuberger et al., 2002). It is easy to see that \( \{1, \alpha, \alpha^{(2)}\} \) is a basis of \( \mathbb{Z}_k[\alpha] \). Indeed, each power of \( \alpha \) can be represented with help of this basis because by (1) we have \( \alpha^2 = -\alpha^{(2)} + (t - 1)\alpha + (t + 1) \). Furthermore, \( \alpha^{(j)} \) (\( 1 \leq j \leq 3 \)) are units in \( \mathbb{Z}_k[\alpha] \) since the constant term of \( f_t(x) \) equals \(-1\). By (1), \( \alpha^{(j)} + 1 \) (\( 1 \leq j \leq 3 \)) are units, too.

Let

\[
m := t^2 + t + 7.
\]

Then \( m^2 \) is easily seen to be the discriminant of \( f_t \).

Our main result will be the following generalization of Lemmermeyer and Pethő (1995, Theorem 1) to imaginary quadratic number fields. We use the abbreviation

\[
b := \begin{cases} 
\frac{1 + i \sqrt{D}}{2}, & \text{for } D \equiv 3 \mod 4 \ 
i \sqrt{D}, & \text{for } D \not\equiv 3 \mod 4,
\end{cases} \tag{2}
\]

such that \( \{1, b\} \) forms an integer basis of \( k \).

**Theorem 1.1.** Let \( |t| \geq 14, \forall t > 0, \) and \( \gamma \in \mathbb{Z}_k[\alpha] \) where \( k := \mathbb{Q}(\sqrt{-D}) \) and \( f_t(\alpha) = 0 \). If \( | N_{k(\alpha)/k}(\gamma) | \leq |2t + 1| \) then \( \gamma \) is associated with an element of \( \mathbb{Z}_k \) or \( \gamma \) is associated with one of the conjugates in \( k(\alpha)/k \) of the elements according to the following list \( L(t, \alpha, \gamma) \).

| Discriminant | \( | N_{k(\alpha)/k}(\gamma) | \) | \gamma \text{ associated with an integer or to one of the conjugates of} |
|---------------|-----------------|----------------------------------|
| \( D = 2, 5, 6 \) or \( D \geq 10 \) \( t \not\in \{-1 + 10i\sqrt{2}, 10i\sqrt{2}\} \) | \( |2t + 1| \) | \( \alpha - 1 \) |
| \( D = 7 \) | \( |2t + 1| \) | \( \alpha - 1 \)  
| | \( |2t + 1 - 2\sqrt{7}| \) | \( \alpha + 1 - b \) |
The list \( \mathcal{L}(t, \alpha, \gamma) \)

| Discriminant | \(|N_{k(\alpha)/k}(\gamma)|\) | \(\gamma\) associated with an integer or to one of the conjugates of \(\alpha\) |
|--------------|-------------------------------|------------------------------------------------------------------|
| \(D = 3\)   | \(2t + 1\)                    | \(\alpha - 1\)                                                   |
|              | \(\sqrt{3}(2t + 1 - \frac{2}{3})\) | \(\alpha + 1 + b\)                                              |
|              | \(\sqrt{3}(2t + 1 + \frac{2}{3})\) | \(\alpha - b\)                                                  |
|              | \(\sqrt{3}(2t + 1 + \frac{2}{3})\) | \(\alpha + b\)                                                  |
|              | \(\sqrt{3}(2t + 1 - \frac{2}{3})\) | \(\alpha + 1 - b\)                                              |
| \(D = 2\)   | \(2t + 1\)                    | \(\alpha - 1\) or \(\alpha + 1 - b\)                            |
| \(t = -1 + 10i\sqrt{2}\) | \(2t + 1\) | \(\alpha - 1\) or \(\alpha - b\) |
| \(D = 2\)   | \(2t + 1\)                    | \(\alpha - 1\) or \(\alpha + b\) |
| \(t = 10i\sqrt{2}\) | \(2t + 1\) | \(\alpha - 1\) or \(\alpha + b\) |

In particular, for each fixed \(D\) the occurring moduli of norms are pairwise different.

**Remark 1.2.** The condition \(\Re t > 0\) does not mean a loss of generality. Since \(N_{k(\alpha)/k}(\gamma) = \overline{N_{k(\alpha)/k}(\gamma)}\) the result follows for \(\Re t < 0\) just by complex conjugation. The case \(\Re t = 0\) is contained in Lemmermeyer and Pethő (1995, Theorem 1).

**Remark 1.3.** In the special instance \(t = -1 + 10i\sqrt{2}\) we have

\[ |N_{k(\alpha)/k}(\alpha - 1)| = |N_{k(\alpha)/k}(\alpha + 1 - b)| = |2t + 1|. \]

Nevertheless, none of the conjugates of \(\alpha - 1\) is associated with any of the conjugates of \(\alpha + 1 - b\) since

\[
\frac{N_{k(\alpha)/k}(\alpha + 1 - b)}{N_{k(\alpha)/k}(\alpha - 1)} = \frac{17 - 16i\sqrt{2}}{-1 + 20i\sqrt{2}} = \frac{-73 - 36i\sqrt{2}}{89} \notin \mathbb{Z}_k.
\]

The case \(t = 10i\sqrt{2}\) can be treated analogously.

The proof of Theorem 1.1 will be given in the subsequent sections, which are organized as follows. In Section 2 we show that it is sufficient to prove Theorem 1.1 for \(\Re t \leq -1/2\) and \(|t| \geq 13\) using reflection on the axis \(\Re t = -1/2\). In Section 3 we establish uniform estimates for the roots of the polynomial \(f_t\) in terms of \(t\). Section 4 is devoted to the generalization of a lemma of Mignotte et al. (1996, Lemma 3) for imaginary quadratic fields. This result allows one to associate with each \(\gamma \in \mathbb{Z}_k[\alpha]\) a well suited element \(\beta \in \mathbb{Z}_k[\alpha]\) whose conjugates are small in modulus. In Section 5 the central reduction result will be proved. If

\[ \beta = u + v\alpha + w\alpha(2) \]

with \(u, v, w \in \mathbb{Z}_k\), then \(u, v\) and \(w\) can attain only finitely many values for a given choice of \(t\). The proof relies heavily on a geometric argument. This argument yields a lower estimate
for the product of the distances of a point in the complex plane from three specified points in terms of the largest mutual distance between these points. In the final Section 6 we describe how the proof of Theorem 1.1 is completed on the basis of these reduction results using a Mathematica® program.

2. Reduction to \( \Re t \leq -1/2 \)

We now turn to the proof of the theorem. In a first step we show that it is sufficient to prove Theorem 1.1 for \( \Re t \leq -1/2 \) and \( |t| \geq 13 \).

**Proposition 2.1.** If Theorem 1.1 is valid for \( \Re t \leq -1/2 \), \( \Im t > 0 \) and \( |t| \geq 13 \) then it is valid for all \( t \) with \( \Im t > 0 \) and \( |t| \geq 14 \).

**Proof.** Let us assume that Theorem 1.1 holds for \( \Re t \leq -1/2 \) and \( |t| \geq 13 \) and let us consider now \( t \) with \( \Re t > -1/2 \), \( |t| \geq 14 \) and \( t \neq 10i \sqrt{2} \), and \( \gamma \in \mathbb{Z}_k[\alpha] \) where \( f_t(\alpha) = 0 \) and \( |N_{k(\alpha)/k}(\gamma)| \leq |2t + 1| \).

Setting \( t^* := 1 - i \) we have \( \Re t^* \leq -1/2 \), \( 3t^* > 0 \) and \( |t^*| \geq 13 \). Let \( \alpha^* := 1/\bar{\alpha} \). Since

\[
f_{t^*}(x) = -x^3 f_t\left(\frac{1}{x}\right)
\]

we have \( f_{t^*}(\alpha^*) = 0 \). Since \( \bar{\alpha} \) is a unit in \( k(\alpha^*) = \bar{k}(\alpha) \) we have

\[
\mathbb{Z}_k[\alpha^*] = \mathbb{Z}_k[1/\bar{\alpha}] = \mathbb{Z}_k[\bar{\alpha}] = \mathbb{Z}_k[\alpha].
\]

so \( \tilde{\gamma} \in \mathbb{Z}_k[\alpha^*] \) holds, too. By the assumption, the theorem holds for \( t^* \) and \( \tilde{\gamma} \). For the following we recall that \( N_{k(\alpha)/k}(\gamma) = \bar{N}_{k(\overline{\alpha})/k}((\tilde{\gamma}) \) so

\[
|N_{k(\alpha)/k}(\gamma)| = |N_{k(\overline{\alpha})/k}((\tilde{\gamma})|.
\]

Furthermore, we have

\[
|2t + 1| = |2t^* + 1|.
\]

Therefore, \( |N_{k(\alpha)/k}(\gamma)| \leq |2t + 1| \) is equivalent to \( |N_{k(\overline{\alpha})/k}((\tilde{\gamma})| \leq |2t^* + 1| \) so, by the assumption, \( \tilde{\gamma} \) is associated with an element of \( \mathbb{Z}_k \) or \( \tilde{\gamma} \) is associated with one of the conjugates in \( k(\alpha)/k \) of the elements given in the third column of the list \( \mathcal{L}(t^*, \alpha^*, \tilde{\gamma}) \), \( t^* \neq 10i \sqrt{2} \). If \( \tilde{\gamma} \) is associated with an element of \( \mathbb{Z}_k \), then the same holds for \( \gamma \). If \( \tilde{\gamma} \) is not associated with an integer we argue as follows.

Each of the moduli of the norms of \( \tilde{\gamma} \) occurring in \( \mathcal{L}(t^*, \alpha^*, \tilde{\gamma}) \) can be written in the form

\[
|z(2t^* + 1 + \lambda i)| \quad \text{with} \quad z \in \mathbb{C} \quad \text{and} \quad \lambda \in \mathbb{R}.
\]

Now

\[
|z(2t^* + 1 + \lambda i)| = |z||1 - 2\tilde{t} + \lambda i| = |z||1 + 2\tilde{t} - \lambda i| = |z||2t + 1 + \lambda i| = |z(2t + 1 + \lambda i)|.
\]

Thus the list \( \mathcal{L}(t^*, \alpha^*, \tilde{\gamma}) \), \( t^* \neq 10i \sqrt{2} \) is equivalent to the list \( \mathcal{L}(t, \alpha^*, \tilde{\gamma}) \), \( t \neq -1 + 10i \sqrt{2} \).
Now we turn our attention to the last column of $\mathcal{L}(t, \alpha^*, \tilde{\gamma})$. Note that
\[ \tilde{\gamma} \sim \alpha^* + z \quad \text{is equivalent to} \quad \gamma \sim \frac{1}{\alpha} + \frac{1}{\bar{z}} \quad \text{for} \quad z \in \mathbb{Z}_k. \]
Furthermore, we will show that $1/\alpha + \bar{z}$ is associated with one of the conjugates of $\alpha + z$ for all situations occurring in the list $\mathcal{L}(t, \alpha^*, \tilde{\gamma})$:

- $\tilde{\gamma} \sim \alpha^* - 1$. This implies that
  \[ \gamma \sim \frac{1}{\alpha} - 1 = \frac{1}{\alpha} (\alpha - 1) \sim (\alpha - 1) \]
  since $\alpha$ is a unit.
- $D \equiv 3 \mod 4$ and $\tilde{\gamma} \sim \alpha^* + z$ with $z \in \{b, 1-b\}$. This implies that
  \[ \gamma \sim \frac{1}{\alpha} + \bar{z} \sim -1 - \alpha^{(2)} + \bar{z} \sim \alpha^{(2)} + 1 - \bar{z} = \alpha^{(2)} + z. \]
- $D = 3$ and $\tilde{\gamma} \sim \alpha^* + 1 + b$. This implies that
  \[ \gamma \sim \alpha^{(2)} + 1 - (b + 1) = \alpha^{(2)} + b - 1. \]
  Since $b$ is a unit and $b^2 = b - 1$, $\gamma$ is associated with
  \[ ba^{(2)} + b^2 - b = ba^{(2)} - 1 = -\frac{1}{\alpha^{(3)} + 1} b - 1 \sim \alpha^{(3)} + b + 1. \]
- $D = 3$ and $\tilde{\gamma} \sim \alpha^* - b$. This implies that
  \[ \gamma \sim \alpha^{(2)} + 1 + \bar{b} = \alpha^{(2)} - b + 2. \]
  Since $b$ is a unit and $b^2 = b - 1$, $\gamma$ is associated with
  \[ ba^{(2)} - b^2 + 2b = ba^{(2)} + b + 1 = -\frac{1}{\alpha} \sim \alpha - b. \]
- $D = 2$ and $t = -1 + 10i \sqrt{2}$ and $\tilde{\gamma} \sim \alpha^* + 1 - b$. This implies that
  \[ \gamma \sim \alpha^{(2)} + 1 - (1 - b) = \alpha^{(2)} - i \sqrt{2} \sim \alpha^{(2)} - b. \]
- $D = 1$ and $\tilde{\gamma} \sim \alpha^* + 1 - b$. This implies that
  \[ \gamma \sim \alpha^{(2)} + 1 - (1 - b) = \alpha^{(2)} - i. \]
  By multiplication by $-i$ we see that $\gamma$ is associated with
  \[ -i\alpha^{(2)} - 1 = (1 - i)\alpha^{(2)} - \alpha^{(2)} - 1 \sim 1 - i - \frac{\alpha^{(2)} + 1}{\alpha^{(2)}} = \alpha^{(3)} + 1 - b. \]
- $D = 1$ and $\tilde{\gamma} \sim \alpha^* + b$. This implies that
  \[ \gamma \sim \alpha^{(2)} + 1 - \bar{b} = \alpha^{(2)} + 1 + i \]
  \[ = -\frac{\alpha + 1}{\alpha} + 1 + i \sim -\alpha - 1 + (1 + i)\alpha = i\alpha - 1 \]
  and by multiplication by $-i$ we see that $\gamma$ is associated with $\alpha + i$.

Therefore, we have established the list $\mathcal{L}(t, \alpha, \gamma)$ for $\Re t \geq -1/2$ and the proposition is proved. □
3. Relations between $\alpha$ and $t$

By Proposition 2.1 in the remaining part of the proof of Theorem 1.1 we can confine ourselves to the case $\Re t \leq -1/2$ and $|t| \geq 13$.

We will make frequent use of uniform estimates of the roots $\alpha^{(j)}$ of $f_t$ in terms of $t$. To this end we need the following notation. For two functions $g$ and $h$ and a positive number $x_0$ we will write $g(x) = L_{x_0}(h(|x|))$ if $|g(x)| \leq h(|x|)$ for all $x$ with $|x| > x_0$.

**Lemma 3.1.** Let $t \in \mathbb{C}$. Then there is a root $\alpha$ of $f_t$ such that we have the following estimates in terms of $t$:

$$
\alpha = t + \frac{2}{t} - \frac{1}{t^2} - \frac{3}{t^3} + L_j \left( \frac{a_{1j}}{|t|^{1/2}} \right),
$$

$$
\alpha^{(2)} = -1 - \frac{1}{\alpha} = -1 - \frac{1}{t} + \frac{2}{t^2} + L_j \left( \frac{a_{2j}}{|t|^{1/2}} \right),
$$

$$
\alpha^{(3)} = -\frac{1}{\alpha + 1} = -\frac{1}{t} + \frac{1}{t^2} + \frac{1}{t^3} + L_j \left( \frac{a_{3j}}{|t|^{1/2}} \right),
$$

for $j \in \{6, 13\}$, where the constants $a_{ij}$ are given by the following table.

<table>
<thead>
<tr>
<th>$j$</th>
<th>$a_{1j}$</th>
<th>$a_{2j}$</th>
<th>$a_{3j}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>4.6</td>
<td>1.5</td>
<td>2.0</td>
</tr>
<tr>
<td>13</td>
<td>1.9</td>
<td>0.6</td>
<td>1.2</td>
</tr>
</tbody>
</table>

**Proof.** This can be shown by using Rouché’s Theorem in the same way as in Heuberger et al. (2002, Lemma 8). □

In the remaining part of the paper we will use the same numbering of the roots $\alpha = \alpha^{(1)}$, $\alpha^{(2)}$ and $\alpha^{(3)}$ as in Lemma 3.1. Furthermore, for $j > 3$, $\alpha^{(j)}$ has to be interpreted as $\alpha^{(j \mod 3)}$, where $j \mod 3$ is the smallest positive integer which is congruent to $j$ modulo 3.

**Lemma 3.2.** For $|t| \geq 6$ we have

$$
|\alpha| > \max(1, |\alpha^{(2)}|, |\alpha^{(3)}|)
$$

and

$$
\Re t \leq -\frac{1}{2} \iff \Re \alpha \leq -\frac{1}{2}.
$$

**Proof.** The first assertion follows by applying the triangular inequality to the representations in Lemma 3.1. Note that the modulus of the largest root of $f_t$ has to be greater than one because its norm is one (if this modulus was equal to one, $f_t$ would be a cyclotomic polynomial which is impossible).

In order to show the second assertion we first prove that $\Re t = -1/2 \iff \Re \alpha = -1/2$. The direction “$\Rightarrow$” has been shown in Heuberger et al. (2002, Lemma 8). In order to prove the other direction assume that $\Re \alpha = -1/2$. Since this implies that $\bar{\alpha} = -\alpha - 1$ we have

$$
f_t(-\alpha - 1) = f_t(\bar{\alpha}) = \overline{f_t(\alpha)}.
$$
Thus
\[
(-\alpha - 1)^3 - (\bar{t} - 1)(-\alpha - 1)^2 - (\bar{t} + 2)(-\alpha - 1) - 1 = 0.
\]
Dividing by \((\alpha + 1)^3\) we obtain
\[
\left(-\frac{1}{\alpha + 1}\right)^3 + (\bar{t} + 2)\left(-\frac{1}{\alpha + 1}\right)^2 + (\bar{t} - 1)\left(-\frac{1}{\alpha + 1}\right) - 1 = 0
\]
or
\[
(\alpha^{(3)})^3 + (\bar{t} + 2)(\alpha^{(3)})^2 + (\bar{t} - 1)\alpha^{(3)} - 1 = 0.
\]
Since \(\alpha^{(3)}\) has relative degree 3 over \(k\) this implies that
\[
x^3 + (\bar{t} + 2)x^2 + (\bar{t} - 1)x - 1 = x^3 - (t - 1)x^2 - (t + 2)x - 1.
\]
For the coefficients of \(x^2\) this yields \(\bar{t} + 2 = -(t - 1)\) and, hence, \(\Re t = 1/2\).
Since the real parts of the roots of a polynomial are continuous functions of its coefficients this implies that for all \(t\) satisfying \(\Re t < -1/2\) we have either \(\Re \alpha < -1/2\) or \(\Re \alpha > -1/2\). In order to show that the first alternative holds it suffices to check it for a single \(t\) in the half-plane \(\Re t < -1/2\). If we take for \(t\) a negative real number with large absolute value, this follows immediately from the expansion of \(\alpha\) in Lemma 3.

4. Reduction to numbers with small conjugates

We need an analogue of Mignotte et al. (1996, Lemma 3) for imaginary quadratic fields.

For the sake of brevity we will write \(N(\cdot)\) instead of \(N_{k(\alpha)}/k(\cdot)\) for the norm.

Lemma 4.1. Let \(\gamma \in \mathbb{Z}[\alpha]\) be nonzero and let \(c_1, c_2 \in \mathbb{R}\) be positive constants. If \(\Re t \leq -1/2\) and \(|t| \geq 6\) then there exist \(a_1, a_2 \in \mathbb{Z}\) and \(\beta \in \mathbb{Z}[\alpha]\) such that
\[
\gamma = \beta\alpha^{a_1}(\alpha^{(2)})^{a_2}
\]
with
\[
c_i \leq |\beta^{(i)}| \leq C(\alpha)c_i, \quad i \in \{1, 2\}, \quad \frac{|N(\gamma)|}{C(\alpha)^2c_1c_2} \leq |\beta^{(3)}| \leq \frac{|N(\gamma)|}{c_1c_2},
\]
where
\[
C(\alpha) := \left|\frac{\alpha}{\alpha^{(2)}}\right| = \left|\alpha - 1 - \alpha^{(3)}\right|.
\]

Proof. Arguing along the same lines as in the first part of the proof of Mignotte et al. (1996, Lemma 3) we get the result with
\[
C'(\alpha) = \max \left(\exp \left(|\log |\alpha|| + |\log |\alpha^{(2)}||\right), \exp \left(|\log |\alpha^{(2)}|| + |\log |\alpha^{(3)}||\right)\right)
\]
instead of \(C(\alpha)\). In order to prove our result we will show that \(C'(\alpha) = C(\alpha)\). For this purpose we distinguish three cases.
\[ |\alpha(2)| \leq 1 < |\alpha(3)|. \] In this case we have
\[ C'(\alpha) = \max \left( \frac{|\alpha|}{|\alpha(2)|}, \frac{|\alpha(3)|}{|\alpha(2)|} \right) = \left| \frac{\alpha}{\alpha(2)} \right| = |\alpha - 1 - \alpha(3)| \]
since \(|\alpha| > |\alpha(3)|\) holds by the definition of \(\alpha\).

\[ |\alpha(2)|, |\alpha(3)| \leq 1. \] In this case we have
\[ C'(\alpha) = \max \left( \frac{|\alpha|}{|\alpha(2)|}, \frac{1}{|\alpha(3)|} \right) = \left| \frac{\alpha}{\alpha(2)} \right| = |\alpha - 1 - \alpha(3)| \]
since \(\alpha = 1/(\alpha(2)\alpha(3))\).

\[ |\alpha(2)| > 1. \] This is impossible because by Lemma 3.2 we have \(8t\alpha \leq -1/2\) which yields \(|\alpha + 1| \leq |\alpha|\), so \(|\alpha(2)| \leq 1\), a contradiction. \(\square\)

**Remark 4.2.** If we drop the restriction \(|t| \geq 6\), the lemma remains valid. However, we can no longer guarantee that the root \(\alpha\) is the one corresponding to the expansion given in Lemma 3.1.

Observe that for \(|t| \geq 13\) the first case of the proof is not needed since \(|t| \geq 13\) implies that \(|\alpha(3)| < 1\).

Setting
\[ c_1 = c_2 = \left( \frac{|N(\gamma)|}{C(\alpha)} \right)^{1/3}, \]
Lemma 4.1 yields the following result.

**Corollary 4.3.** Let \(\gamma \in \mathbb{Z}_k[\alpha]\) be nonzero. If \(8t \leq -1/2\) and \(|t| \geq 6\) then there exists \(\beta \in \mathbb{Z}_k[\alpha]\) associated with \(\gamma\) such that
\[ |\beta(i)| \leq |N(\gamma)|^{1/3} C(\alpha)^{2/3}, \quad i \in \{1, 2, 3\}. \]

**5. Representations with respect to the integer base \(\{1, \alpha, \alpha(2)\}\)**

In the following we write
\[ \beta = u + v\alpha + w\alpha(2) \quad (3) \]
with \(u, v, w \in \mathbb{Z}_k\).

First of all, observe that in the case \(v = w = 0\), i.e. \(\beta = u, \gamma\) is certainly associated with an element of \(\mathbb{Z}_k\).

Thus in the following we may assume that \((v, w) \neq (0, 0)\). As in Lemmermeyer and Pethő (1995, p. 55) (note the sign typographical errors there) we find
\[ mu = -T(\beta(\alpha(2) - (\alpha(3))^2)), \]
\[ mv = -T(\beta(\alpha(3) - \alpha)), \]
\[ mw = T(\beta(\alpha(2) - \alpha(3))) \]
where $T(\cdot) = T_{k(\alpha)/k(\cdot)}$ denotes the trace. Applying Corollary 4.3 we get the bounds
\begin{equation}
|mv|, |mw| \leq |N(\gamma)|^{1/3} C(\alpha)^{2/3} (|\alpha - \alpha^{(2)}| + |\alpha^{(2)} - \alpha^{(3)}| + |\alpha^{(3)} - \alpha|).
\end{equation}

For
\[ \Delta := |\alpha - \alpha^{(2)}| + |\alpha - \alpha^{(3)}| + |\alpha^{(2)} - \alpha^{(3)}| \]
we have
\begin{equation}
\frac{\Delta}{|m|} = \frac{1}{|\alpha - \alpha^{(2)}||\alpha^{(2)} - \alpha^{(3)}|} + \frac{1}{|\alpha - \alpha^{(3)}||\alpha^{(2)} - \alpha^{(3)}|} + \frac{1}{|\alpha - \alpha^{(2)}||\alpha - \alpha^{(3)}|}.
\end{equation}

If $|\gamma| \leq 1/2$ and $|N(\gamma)| \leq 2|\gamma + 1|$ then
\begin{equation}
|N(\gamma)|^{1/3} \leq 2|\gamma + 1|^{1/3} \leq 2|\gamma|^{1/3}.
\end{equation}

From (4) and (6) we have that
\begin{equation}
|v|, |w| \leq 2|\gamma|^{1/3} C(\alpha)^{2/3} \frac{\Delta}{|m|}.
\end{equation}

For $|\gamma| \geq 13$ and $|\gamma| \leq 1/2$, Lemma 3.1 for $j = 13$ and the triangular inequality yield the following estimate:
\begin{equation}
|v|, |w| \leq 2^{1/3}|\gamma|^{1/3} \left(|\gamma| + 1 + \frac{3}{|\gamma|} + \frac{2}{|\gamma|^2} + \frac{4}{|\gamma|^3} + \frac{3.1}{|\gamma|^{7/2}} \right)^{2/3} \times 
\end{equation}
\begin{equation}
\left( |\gamma| - \frac{4}{|\gamma|} - \frac{3}{|\gamma|^2} - \frac{1}{|\gamma|^3} - \frac{1.8}{|\gamma|^5/2} - \frac{3.1}{|\gamma|^{7/2}} - \frac{5}{|\gamma|^4} - \frac{5.4}{|\gamma|^{9/2}} - \frac{2}{|\gamma|^5} - \frac{6.7}{|\gamma|^{11/2}} \right)^{-1}
\end{equation}
\begin{equation}
+ \left( |\gamma| - \frac{4}{|\gamma|} - \frac{1}{|\gamma|^2} - \frac{1}{|\gamma|^3} - \frac{1.8}{|\gamma|^5/2} - \frac{3}{|\gamma|^{7/2}} - \frac{4.3}{|\gamma|^4} - \frac{4}{|\gamma|^{9/2}} - \frac{5.4}{|\gamma|^5} - \frac{4}{|\gamma|^{11/2}} \right)^{-1}
\end{equation}
\begin{equation}
- \frac{3.1}{|\gamma|^{11/2}} - \frac{5}{|\gamma|^6} - \frac{11.5}{|\gamma|^{13/2}} - \frac{4.5}{|\gamma|^7} \right)^{-1}
\end{equation}
\begin{equation}
+ \left( |\gamma|^2 - |\gamma| - 6 - \frac{2}{|\gamma|^2} - \frac{5.6}{|\gamma|^5/2} - \frac{13}{|\gamma|^3} - \frac{3.1}{|\gamma|^{7/2}} - \frac{25}{|\gamma|^4} - \frac{16.8}{|\gamma|^{9/2}} - \frac{14}{|\gamma|^5} \right)^{-1}
\end{equation}
\begin{equation}
- \frac{8.1}{|\gamma|^{11/2}} - \frac{20}{|\gamma|^6} - \frac{25.5}{|\gamma|^{13/2}} - \frac{7.75}{|\gamma|^7} \right)^{-1}.
\end{equation}

The right hand side is monotonically decreasing in $|\gamma|$. Inserting $|\gamma| = 13$ yields the following lemma.

**Lemma 5.1.** Let $|\gamma| \leq 1/2$ and let $v, w$ be defined as in (3). If $|\gamma| \geq 13$ then
\begin{equation}
|v|, |w| < 2.9804.
\end{equation}
In order to prove Theorem 1.1 we have to identify the elements $\gamma \in \mathbb{Z}_k[\alpha]$ with small norm. In view of Lemma 4.1 we have

$$|N(\gamma)| = |N(\beta)| = |N(u + v\alpha + w\alpha^2)|.$$  

For fixed $v, w \in \mathbb{Z}_k$ we may consider

$$g_{v,w}(r) := (r + v\alpha + w\alpha^2)(r + v\alpha^2 + w\alpha^3)(r + v\alpha^3 + w\alpha)$$

as a function of $r \in \mathbb{C}$. Note that $g_{v,w}(u) = N(\beta)$. The polynomial $g_{v,w}$ has the roots

$$r_1 = -v\alpha - w\alpha^2, \quad r_2 = -v\alpha^2 - w\alpha^3, \quad r_3 = -v\alpha^3 - w\alpha.$$  

(8)

We can interpret $|g_{v,w}(r)|$ as the product of the distances of $r$ from the points $r_1, r_2$ and $r_3$ in the complex plane. In the following we use a geometric lower estimate for this product of distances. This lower bound depends on the largest mutual distance of the points $r_1, r_2, r_3$.

Lemma 5.2. Let $R \in \mathbb{R}$ and let $z, z_1, z_2, z_3 \in \mathbb{C}$ be disjoint. For $i \in \{1, 2, 3\}$ set $d_i = |z - z_i|$ and $d := \max_{i,j} |z_i - z_j|$. If $d_i \geq R$ for each $i \in \{1, 2, 3\}$ then

$$d_1d_2d_3 \geq R^2(d - R).$$

Proof. W.l.o.g., assume that $d = |z_1 - z_2|$. We denote by $\ell_i$ the length of the projection of the vector $\overrightarrow{z_i z}$ on the vector $\overrightarrow{z_1 z_2}$ ($i = 1, 2$).

By assumption we have

$$d_1d_2d_3 \geq d_1d_2R \geq \max(\ell_1, R) \max(\ell_2, R)R =: P.$$  

Furthermore, note that

$$\ell_1 \geq d - \ell_2 \quad \text{and} \quad \ell_2 \geq d - \ell_1.$$  

(9)

We distinguish four cases.

- $\ell_1, \ell_2 \geq R$: using (9), in this case we get

$$P = \ell_1\ell_2R \geq \ell_1 \max(|d - \ell_1|, R)R \geq R^2(d - R).$$

- $\ell_1 \geq R, \ell_2 < R$: by (9) we have

$$P = \ell_1R^2 \geq (d - R)R^2.$$  

- $\ell_1 < R, \ell_2 \geq R$ is treated in the same way as the previous case.
- $\ell_1 < R, \ell_2 < R$. By (9) in this case we have $2R > d$. Thus

$$P = R^3 > R^2(d - R). \quad \Box$$

In the following we will apply Lemma 5.2 for $z = r$ and $z_i = r_i$ $(1 \leq i \leq 3)$. We will choose $R$ such that

$$R^2(d - R) > |2r + 1|. $$
This implies that $|g_{v,w}(r)| > |2t + 1|$ if $|r - r_i| \geq R$ for all $i$. Thus for the proof of Theorem 1.1 we only need to consider values of $u$ obeying $|u - r_i| < R$ for at least one $i \in \{1, 2, 3\}$.

We start with the following estimates for $\alpha$ and its conjugates which can easily be deduced from Lemma 3.1. In fact, for $|t| \geq 13$ we have

$$\alpha = t + L_{13}(0.161370),$$
$$\alpha^{(2)} = -1 + L_{13}(0.077910),$$
$$\alpha^{(3)} = L_{13}(0.083447).$$

Therefore using (8) and Lemma 5.1 we get

$$r_1 = -vt + w + |v|L_{13}(0.161370) + |w|L_{13}(0.077910),$$
$$r_2 = v + |v|L_{13}(0.077910) + |w|L_{13}(0.083447),$$
$$r_3 = -wt + |v|L_{13}(0.083447) + |w|L_{13}(0.161370).$$

In the next step we establish a lower bound for $d$. To this end we distinguish two cases.

- $|v| = \max(|v|, |w|) > 0$. In this case

$$|r_1| \geq ||vt| - |v|L_{13}(0.161370) + |w|L_{13}(0.077910) + w||.$$

Observe that

$$||v|L_{13}(0.161370) + |w|L_{13}(0.077910) + w| \leq 3.69356 \leq |vt|$$

holds for $|t| \geq 13$. Therefore we find that

$$|r_1| \geq |vt| - |w| - |v|L_{13}(0.239280).$$

Furthermore,

$$|r_2| \leq |v| + |v|L_{13}(0.161357).$$

Thus we have

$$d \geq |r_1 - r_2| \geq |vt| - 2|v| - |v|L_{13}(0.400637)$$
$$\geq |v|(|t| - L_{13}(2.400637)).$$

- $|w| = \max(|v|, |w|) > 0$. In this case we find in a similar manner that

$$|r_3| \geq |vt| - |w|L_{13}(0.244817)$$

and

$$|r_2| \leq |w| + |w|L_{13}(0.161357)$$

hold. Thus we have

$$d \geq |r_3 - r_2| \geq |w|(|t| - L_{13}(1.400674)).$$
Summing up we find that for all $v, w$ the inequality
\[ d \geq \max(|v|, |w|)(|t| - L_{13}(2.400637)). \]
holds. In what follows we set $M := \max(|v|, |w|)$. In order to apply Lemma 5.2 we choose for $M > 0$
\[ R^2 = \frac{3.05}{M}. \]
With this choice we have for $|t| \geq 13$
\[ R^2(d - R) \geq R^2M(|t| - L_{13}(2.400637)) - R^3 \]
\[ = 3.05(|t| - L_{13}(2.400637)) - \left(\frac{3.05}{M}\right)^{3/2} \]
\[ \geq |t| \left(3.05 \left(1 - \frac{L_{13}(2.400637)}{|t|}\right) - \frac{3.05^{3/2}}{|t|}\right) \]
\[ \geq 2.07704|t| > 2|t| + 1 \geq |2t + 1|. \]

Consequently, we have proved the following lemma.

**Lemma 5.3.** Let $u, v, w$ be defined as in (3), $M := \max(|v|, |w|) > 0$ and $r_1, r_2, r_3$ be defined as in (8). Suppose that $u$ has distance greater than
\[ R = \sqrt{\frac{3.05}{M}} \]
from each of the points $r_1, r_2, r_3$; then $|N(u + v\alpha + w\alpha^{(2)})| > |2t + 1|$.  

Thus Lemma 5.3 implies that for the proof of Theorem 1.1 it suffices to consider the instances where $u$ is within one of the discs of radius $R$ around $r_1, r_2$ or $r_3$.

In order to determine a list containing all the candidates $u$ we first approximate $r_1, r_2$ and $r_3$ by points of the lattice $\mathbb{Z}_k$:
\[ p_1 := -vt + w, \]
\[ p_2 := v, \]
\[ p_3 := -wt. \]

From (10) it follows that
\[ |r_i - p_i| \leq ML_{13}(0.244817) \quad (1 \leq i \leq 3). \]

Setting
\[ \tilde{R} := \sqrt{\frac{3.05}{M}} + 0.244817M < 1.99124 < 2 \]
it suffices for the proof of Theorem 1.1 to consider all numbers $u$ with distance less than $2$ from at least one of the points $p_i$.

In the following we give a concrete list of these numbers $u$ depending on $D$. 
Lemma 5.4. The numbers \( u \) with distance less than 2 from at least one of the points \( p_i \) are all points of the form \( u = p_i + \xi \) with \( p_i \) defined in (14) and

- for \( D \equiv 3 \pmod{4} \) and \( b := \sqrt{D} \),
  \[
  \xi \in \{0, \pm 1\} \quad \text{for } D \geq 5, \\
  \xi \in \{0, \pm 1, \pm b, \pm (1 \pm b)\} \quad \text{for } D \in \{1, 2\},
  \]

- for \( D \equiv 3 \pmod{4} \) and \( b := \frac{1 + \sqrt{D}}{2} \),
  \[
  \xi \in \{0, \pm 1\} \quad \text{for } D \geq 15, \\
  \xi \in \{0, \pm 1, \pm b, \pm (-1 + b)\} \quad \text{for } D \in \{7, 11\}, \\
  \xi \in \{0, \pm 1, \pm b, \pm (-1 + b), \pm (1 + b), \pm (-2 + b) \pm (-1 + 2b)\} \quad \text{for } D = 3.
  \]

Proof. Immediate. \( \square \)

In a similar way we also get the following lists for \( u \) and \( v \). (Note that Lemma 5.1 motivates the choice 3 as a bound for the modulus.)

Lemma 5.5. The numbers \( v \) and \( w \) with modulus less than 3 are given by the following lists for \( v \) and \( w \):

- for \( D \equiv 3 \pmod{4} \) and \( b := \sqrt{D} \),
  \[
  v, w \in \{0, \pm 1, \pm 2\} \quad \text{for } D \geq 10, \\
  v, w \in \{0, \pm 1, \pm 2, \pm b, \pm (1 \pm b)\} \quad \text{for } D \in \{5, 6\}, \\
  v, w \in \{0, \pm 1, \pm 2, \pm b, \pm (1 \pm b), \pm (2 \pm b), \pm 2b\} \quad \text{for } D = 2, \\
  v, w \in \{0, \pm 1, \pm 2, \pm b, \pm (1 \pm b), \pm (2 \pm b), \pm 2b, \pm (1 \pm 2b), \pm (2 \pm 2b)\} \quad \text{for } D = 1,
  \]

- for \( D \equiv 3 \pmod{4} \) and \( b := \frac{1 + \sqrt{D}}{2} \),
  \[
  v, w \in \{0, \pm 1, \pm 2\} \quad \text{for } D \geq 35, \\
  v, w \in \{0, \pm 1, \pm 2, \pm b, \pm (-1 + b)\} \quad \text{for } D = 31, \\
  v, w \in \{0, \pm 1, \pm 2, \pm b, \pm (-1 + b), \pm (1 + b), \pm (-2 + b)\} \quad \text{for } D \in \{11, 15, 19, 23\}, \\
  v, w \in \{0, \pm 1, \pm 2, \pm b, \pm (-1 + b), \pm (1 + b), \pm (-2 + b), \pm (2 + b), \pm (-3 + b), \pm 2b, \pm (-1 + 2b), \pm (-2 + 2b)\} \quad \text{for } D = 7, \\
  v, w \in \{0, \pm 1, \pm 2, \pm b, \pm (-1 + b), \pm (1 + b), \pm (-2 + b), \pm (2 + b), \pm (-3 + b), \pm 2b, \pm (-1 + 2b), \pm (-2 + 2b), \pm (1 + 2b), \pm (-3 + 2b), \pm (-1 + 3b), \pm (-2 + 3b)\} \quad \text{for } D = 3.
  \]

Proof. Immediate. \( \square \)
Summing up we get the following proposition.

**Proposition 5.6.** Suppose that $|t| \geq 13$ and $\Re t \leq -1/2$, and let $u, v, w$ be defined as in (3). Then $|N(u + v\alpha + w\alpha^{(2)})| \leq |2t + 1|$ implies that $v, w$ have to be chosen as in Lemma 5.5 and $u$ has to be chosen as in Lemma 5.4.

6. Computer aided conclusion of the proof

Note that for fixed $t$, by Proposition 5.6 the proof of Theorem 1.1 has been reduced to checking the norms of an explicitly known finite list of numbers. For those instances of $D$ where the lists for $\xi, v$ and $w$ only contain reals the proof of Theorem 1.1 follows by arguing along the same lines as in the case $t \in \mathbb{Z}$ (cf. Lemmermeyer and Pethö, 1995, p. 56f). The only formal difference consists in replacing the real inequalities for the norms by the corresponding inequalities for the moduli of the norms in question. This yields the following result.

**Proposition 6.1.** Theorem 1.1 is true in the following cases:

- $D \equiv 3 \mod 4$ and $D \geq 35$,
- $D \not\equiv 3 \mod 4$ and $D \geq 10$.

Thus it remains to deal with the cases

$$D \in \{1, 2, 3, 5, 6, 7, 11, 15, 19, 23, 31\}.$$ 

This has been done using a Mathematica® program which makes use of the formula

$$N(u + v\alpha + w\alpha^{(2)}) = u^3 + v^3 + w^3 + (t - 1)u^2v + (t - 1)u^2w + 3uvw - (t^2 + t + 4)v^2w - (t + 2)uv^2 - (t + 2)uw^2 + (t^2 - t + 3)uvw$$

for the norm (cf. Lemmermeyer and Pethö, 1995).

Let $t = c_1 + c_2b$. By Proposition 5.6 we have to check finitely many inequalities of the shape

$$|N(u + v\alpha + w\alpha^{(2)})| \leq |2t + 1|.$$  

For each of the finitely many constellations $u, v, w, D$ this inequality depends on the parameters $c_1, c_2$.

We used Mathematica® in order to check these inequalities. There occur three possibilities.

- The simplification algorithm of Mathematica® detects inequality (15) to be false for a given constellation $u, v, w, D$. In all these cases the norm in (15) is greater than $|2t + 1|$ and we have nothing to do.
- The algorithm detects inequality (15) to be true for a given constellation $u, v, w, D$. In these cases we need to check whether $\beta = u + v\alpha + w\alpha^{(2)}$ is associated with an element of $\mathcal{L}(t, \alpha, \gamma)$ according to the modulus of its norm.
• Inequality (15) cannot be decided by the simplification algorithm for a given constellation \( u, v, w, D \). In this case the \( \text{Mathematica}\) program splits up inequality (15) depending on whether \( c_1 \) and \( c_2 \) are large or small. This leads to finitely many subclasses. If \( \text{Mathematica}\) can decide each of these subclasses we are in one of the above cases. If one of these subclasses cannot be solved it has to be examined further.

In all cases where (15) is not detected to be true, the \( \text{Mathematica}\) program generates a list containing all numbers \( \beta = u + v\alpha + w\alpha^2 \) whose norms either fulfill (15) or whose norm cannot be related to \( |2t + 1| \). If two of the elements in this list are associated with each other it suffices to check one of them. Thus in a next step the program tries to find associated elements in the list. To this end each number is associated with three “normal forms” via the following algorithm.

\textbf{Require:} \( \beta = u + v\alpha + w\alpha^2 \)

\textbf{Ensure:} three “normal forms” \( f_1, f_2, f_3 \) for \( \beta \)

\begin{verbatim}
for j = 1, 2, 3 do
  \( f_j \leftarrow \beta \)
  express all occurrences of \( \alpha, \alpha^2, \alpha^3 \) in \( f_j \) by \( \alpha^j \) according to (1)
  expand \( f_j \) in powers of \( \alpha^j \)
  divide \( f_j \) by the lowest power of \( \alpha^j \) occurring in this expansion
  expand \( f_j \) in powers of \( \alpha^j + 1 \)
  divide \( f_j \) by the lowest power of \( \alpha^j + 1 \) occurring in this expansion
end for
\end{verbatim}

Applying this algorithm to each element of the list yields a list of triples of normal forms. Now we have to distinguish three cases according to the unit group of \( \mathbb{Z}_k \):

- \( D = 1 \). If we find two triples \( (f_1, f_2, f_3) \) and \( (g_1, g_2, g_3) \) such that \( g_i = ef_j \) with \( e \in \{ \pm 1, \pm i \} \) then we can drop one of these triples.
- \( D = 3 \). If we find two triples \( (f_1, f_2, f_3) \) and \( (g_1, g_2, g_3) \) such that \( g_i = ef_j \) with \( e \in \{ \pm 1, \pm b, \pm (b-1) \} \) then we can drop one of these triples.
- \( D \notin \{1, 3\} \). If we find two triples \( (f_1, f_2, f_3) \) and \( (g_1, g_2, g_3) \) such that \( g_i = \pm f_j \) then we can drop one of these triples.

If we reduce the list according to these rules and select one element of each of the remaining triples we obtain a list of elements according to \( D \). Ruling out the elements of \( \mathbb{Z}_k \) we obtain the following list of elements.

<table>
<thead>
<tr>
<th>Discriminant</th>
<th>( \gamma ) associated with an integer or to a conjugate of</th>
</tr>
</thead>
<tbody>
<tr>
<td>( D \in {2, 5, 6, 11, 15, 19, 23, 31} ) and ( t \neq -1 + 10i\sqrt{2} )</td>
<td>( \alpha - 1 )</td>
</tr>
<tr>
<td>( D = 7 )</td>
<td>( \alpha - 1 ) or ( \alpha + 1 - b )</td>
</tr>
<tr>
<td>( D = 3 )</td>
<td>( \alpha - 1, \alpha + 1 + b, \alpha - b, \alpha + b ) or ( \alpha + 1 - b )</td>
</tr>
<tr>
<td>( D = 2 ) and ( t = -1 + 10i\sqrt{2} )</td>
<td>( \alpha - 1 ) or ( \alpha + 1 - b )</td>
</tr>
<tr>
<td>( D = 1 )</td>
<td>( \alpha - 1, \alpha + b ) or ( \alpha + 1 - b )</td>
</tr>
</tbody>
</table>
Computing the moduli of the norms of the elements in this list we immediately find the values contained in $L(t, \alpha, \gamma)$ as well as $|N(\alpha - 1)| = |\alpha + 1 - b| = |2t + 1|$ in the instance $t = -1 + 10i\sqrt{2}$. The fact that for each fixed $D$ the occurring moduli of norms are pairwise different is an easy consequence of $|t| \geq 13$ and the triangular inequality.

According to Proposition 2.1 the theorem is proved.

Acknowledgement

The authors were supported by project S8310 of the Austrian Science Foundation.

References


