Gábor Nyul

Non-monogenity of multiquadratic number fields

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 10 (2002), No. 1, 85--93

Persistent URL: http://dml.cz/dmlcz/120589

Non-monogenity of multiquadratic number fields

Gábor Nyul

Abstract. Continuing the work of several authors on biquadratic number fields we consider the problem of power integral bases in multiquadratic fields of type $K = \mathbb{Q}(\sqrt{k_1}, \dots, \sqrt{k_n})$. We show that if the discriminant of K is odd, then its ring of integers is not monogeneous. Without any restrictions we prove that the indices of the elements in the order $\mathbb{Z}[\sqrt{k_1}, \dots, \sqrt{k_n}]$ are divisible by a high power of 2.

In octic fields ($n = 3$) we show the non-monogenity of the ring of integers of K assuming that the discriminants of the quadratic subfields $\mathbb{Q}(\sqrt{k_i})$ are coprime and at least one of them is imaginary.

1. Introduction

Consider an algebraic number field K of degree n. It is a classical problem of algebraic number theory to decide if K admits integral bases of the form $\{1, \alpha, \dots, \alpha^{n-1}\}$, that is *power integral bases*. If there exist power integral bases in K, then it is called *monogeneous*.

For any integral basis $\{1, \omega_2, \dots, \omega_n\}$ of K let

$$l^{(j)}(\underline{x}) = x_1 + x_2\omega_2^{(j)} + \cdots + x_n\omega_n^{(j)} \qquad (j = 1, \dots, n)$$

where the superscripts denote the conjugates. Then the *index form* $I(x_2, \dots, x_n)$ corresponding to the integral basis $\{1, \omega_2, \dots, \omega_n\}$ is defined by

$$\prod_{1 \le i < j \le n} \left(l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})\right)^2 = (I(x_2, \dots, x_n))^2 \cdot D_K \tag{1.1}$$

where $I(x_2, \dots, x_n)$ is a homogeneous polynomial in $n-1$ variables of degree $\frac{n(n-1)}{2}$ with integer coefficients. The element $\alpha = x_1 + x_2\omega_2 + \cdots + x_n\omega_n \in \mathbb{Z}_K$ generates a power integral basis if and only if $I(x_2, \dots, x_n) = \pm 1$ (for related results cf. [1]).

Received: December 17, 2001.

2000 *Mathematics Subject Classification:* 11D57.

Key words and phrases: multiquadratic number fields; index form equations; power integral bases.

Biquadratic number fields of type $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ (where m, n are distinct square-free rational integers) were considered by several authors (see e.g. [4], [3], [2], [6]) and the problem of their monogenity is completely solved. M.N.Gras and F.Tanoe [3] gave necessary and sufficient conditions for the monogenity of biquadratic number fields. I.Gaál, A.Pethő and M.Pohst [2] gave an algorithm for determining all generators of power integral bases in totally real biquadratic number fields using the integral basis given by K.S.Williams [8]. G.Nyul [6] gave necessary and sufficient conditions for totally complex biquadratic number fields to be monogeneous and described all generators of power integral bases in these fields.

In higher degree multiquadratic number fields of type $\mathbb{Q}(\sqrt{k_1}, \ldots, \sqrt{k_n})$ (with $k_1, \ldots, k_n \in \mathbb{Z}$) the problem of monogenity was not investigated yet. There are some results in connection with integral bases of multiquadratic number fields [7]. The purpose of the present paper is to prove the non-monogenity of some octic and general fields of this type and of an order of general multiquadratic fields.

In order to make easier to compare our results we find it better to state all our results in Section 2, the proofs are contained in Section 3.

2. Results on multiquadratic fields

Our first result concerns the monogenity of the *ring of integers* of multiquadratic fields with *odd discriminant.* The proof of the following statement depends on Dedekind's theorem (see e.g. [5] Theorem 4.13) and we shall utilize that 2 does not ramify in the field.

Theorem 1. *Let $n \in \mathbb{N}$, $n \geq 3$, and let $k_1, \ldots, k_n$ be pairwise distinct square-free rational integers (not equal to 0 or 1), such that $K = \mathbb{Q}(\sqrt{k_1}, \ldots, \sqrt{k_n})$ is of degree 2^n with odd discriminant. Then the index of every integer of K is even, hence K is not monogeneous.*

The following result deals with *arbitrary* multiquadratic number fields (without restrictions on the discriminant). We consider the *order* $\mathcal{O} = \mathbb{Z}[\sqrt{k_1}, \ldots, \sqrt{k_n}]$ This is a subset of the ring of integers of the field. We show that the indices of the elements of this order are divisible not only by 2 but by a *high power of 2.*

Theorem 2. *Let $n \in \mathbb{N}$, let $k_1, \ldots, k_n$ be pairwise distinct square-free rational integers (not equal to 0 or 1), such that $\mathbb{Q}(\sqrt{k_1}, \ldots, \sqrt{k_n})$ is of degree 2^n. Set $\mathcal{O} = \mathbb{Z}[\sqrt{k_1}, \ldots, \sqrt{k_n}]$. In the order $\mathcal{O}$ the index of any element is divisible by* $2^{2^{n-1}(2^n-n-1)}$.

As a consequence we get:

Corollary 1. *For $n \geq 2$ the order $\mathcal{O}$ has no power integral bases.*

Finally, we consider octic fields $\mathbb{Q}(\sqrt{k}, \sqrt{l}, \sqrt{m})$. We study the monogenity in the *ring of integers* of this field. We assume that k, l, m are square-free and pairwise coprime. Under the assumption that k is negative we show the non-monogenity of the ring of integers. Note that this result is not covered by Theorem 1.

Theorem 3. *Let $k, l, m \in \mathbb{Z} \setminus \{0, 1\}$ be pairwise coprime, square-free, $k < 0$ and $l \equiv m \equiv 1 \pmod 4$. Then the octic field $N = \mathbb{Q}(\sqrt{k}, \sqrt{l}, \sqrt{m})$ has no power integral bases.*

3. Proofs

Proof of Theorem 1

The prime 2 does not divide the discriminant of K, hence $(2) = P_1 \cdot \dots \cdot P_g$ with distinct prime ideals P_j. Each P_j is of degree f with either $f = 1$ or $f = 2$ (see e.g. [5] Theorem 8.1). Now from $n \geq 3$ we get $g = \frac{2^n}{f} \geq 4$.

We have to observe that there are only two irreducible linear polynomials and one irreducible quadratic polynomial over the field $GF(2)$. Thus Dedekind's theorem (see e.g. [5] Theorem 4.13) implies that the indices of all elements of $\mathbb{Z}_K$ are even. □

In order to prove Theorem 2 we need the following Lemma.

Lemma 1. *If $n \in \mathbb{N}$, $k_1, \dots, k_n$ are pairwise distinct square-free rational integers (not equal to 0 or 1), and $\mathbb{Q}(\sqrt{k_1}, \dots, \sqrt{k_n})$ is an algebraic number field of degree 2^n, then the discriminant of the order $\mathcal{O} = \mathbb{Z}[\sqrt{k_1}, \dots, \sqrt{k_n}]$ is $D_{\mathcal{O}} = (k_1 \dots k_n)^{2^{n-1}} \cdot 2^{n \cdot 2^n}$.*

Proof of Lemma 1

Consider the integral basis

$$\left\{1, \sqrt{k_1}, \dots, \sqrt{k_n}, \sqrt{k_1 k_2}, \dots, \sqrt{k_{n-1} k_n}, \dots, \sqrt{k_1 \dots k_n}\right\}$$

of $\mathcal{O}$. Let $\left\{(\varepsilon_n^{(j)}, \dots, \varepsilon_1^{(j)}) \mid j = 1, \dots, 2^n\right\}$ be the set of all vectors with components ± 1 arranged in antilexicographical order. Then $D_{\mathcal{O}}$ is equal to the square of the determinant having

$$\Big(1, \varepsilon_1^{(j)} \sqrt{k_1}, \dots, \varepsilon_n^{(j)} \sqrt{k_n}, \varepsilon_1^{(j)} \varepsilon_2^{(j)} \sqrt{k_1 k_2}, \dots$$
$$\dots, \varepsilon_{n-1}^{(j)} \varepsilon_n^{(j)} \sqrt{k_{n-1} k_n}, \dots, \varepsilon_1^{(j)} \dots \varepsilon_n^{(j)} \sqrt{k_1 \dots k_n}\Big)$$

in its jth row ($j = 1, \dots, 2^n$). Let us expand the common factors involving $\sqrt{k_1}, \dots, \sqrt{k_n}$ in the columns of this determinant (leaving the signs $\varepsilon_1^{(j)}, \dots, \varepsilon_n^{(j)}$ unchanged). Denote by D_n the remaining matrix. For any of $\sqrt{k_1}, \dots, \sqrt{k_n}$ there are exactly $\binom{n-1}{l}$ columns containing $\sqrt{k_j}$ as a factor of a product with $l + 1$ terms for $l = 0, \dots, n-1$. This implies

$$D_{\mathcal{O}} = \left(\left(\sqrt{k_1 \dots k_n}\right)^{\binom{n-1}{0}+\binom{n-1}{1}+\cdots+\binom{n-1}{n-1}}\right)^2 \cdot |D_n|^2 = (k_1 \dots k_n)^{2^{n-1}} \cdot |D_n|^2.$$

Finally, we show by induction on n that $|D_n|^2 = 2^{n \cdot 2^n}$.

Indeed, this is true for $n = 1$:

$$|D_1|^2 = \begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix}^2 = 2^2 = 2^{1 \cdot 2^1}$$

Assume that the equation $|D_n|^2 = 2^{n \cdot 2^n}$ holds for $n \geq 1$. Now in the determinant $|D_{n+1}|$ interchange the columns so that the first 2^n columns correspond to the columns of $1, \sqrt{k_1}, \dots, \sqrt{k_n}, \sqrt{k_1 k_2}, \dots, \sqrt{k_{n-1} k_n}, \dots, \sqrt{k_1 \dots k_n}$, and the last 2^n columns correspond to the columns of $\sqrt{k_{n+1}}, \sqrt{k_1 k_{n+1}}, \dots, \sqrt{k_n k_{n+1}}, \sqrt{k_1 k_2 k_{n+1}}, \dots, \sqrt{k_{n-1} k_n k_{n+1}}, \dots, \sqrt{k_1 \dots k_n k_{n+1}}$. After these changes we get:

$$|D_{n+1}|^2 = \begin{vmatrix} D_n & D_n \\ D_n & -D_n \end{vmatrix}^2 .$$

After subtracting the jth row from the $(2^n + j)$th one $(1 \leq j \leq 2^n)$ apply the theorem of Laplace to evaluate $|D_{n+1}|^2$:

$$|D_{n+1}|^2 = \begin{vmatrix} D_n & D_n \\ 0 & -2D_n \end{vmatrix}^2 = \left(2^{2^n} \cdot |D_n|^2\right)^2 = \left(2^{2^n} \cdot 2^{n \cdot 2^n}\right)^2 = 2^{(n+1) \cdot 2^{(n+1)}}$$

This completes the proof of the lemma. □

We are now in position to prove Theorem 2.

Proof of Theorem 2

Let us calculate the index form corresponding to the integral basis $\{1, \sqrt{k_1}, \dots, \sqrt{k_n}, \sqrt{k_1 k_2}, \dots, \sqrt{k_{n-1} k_n}, \dots, \sqrt{k_1 \dots k_n}\}$ of $\mathcal{O}$. Using the above notation let

$$l^{(j)}(\underline{x}) = x_1 + \varepsilon_1^{(j)} \sqrt{k_1} x_2 + \dots + \varepsilon_n^{(j)} \sqrt{k_n} x_{n+1} + \varepsilon_1^{(j)} \varepsilon_2^{(j)} \sqrt{k_1 k_2} x_{n+2} + \\ \dots + \varepsilon_1^{(j)} \dots \varepsilon_n^{(j)} \sqrt{k_1 \dots k_n} x_{2^n} \qquad (j = 1, \dots, 2^n).$$

We have

$$\left(\prod_{1 \leq i < j \leq 2^n} \left(l^{(i)}(\underline{x}) - l^{(j)}(\underline{x}) \right) \right)^2 = (I(x_2, \dots, x_{2^n}))^2 \cdot D_{\mathcal{O}}. \tag{3.1}$$

It is easily seen that by calculating the differences $l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})$ $(1 \leq i < j \leq 2^n)$ each term either falls out or is duplicated. Hence from all differences $l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})$ a factor of 2 can be extracted, all together we can factor out 2 on the power $\binom{2^n}{2} = 2^{n-1}(2^n - 1)$. Moreover, $\sqrt{k_m}$ $(m = 1, \dots, n)$ can be extracted from the differences $l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})$ with $\varepsilon_m^{(i)} = -\varepsilon_m^{(j)}$ and $\varepsilon_h^{(i)} = \varepsilon_h^{(j)}$ $(1 \leq h \leq n, h \neq m)$. This yields 2^{n-1} possible values for $\varepsilon_h^{(i)} = \varepsilon_h^{(j)}$, $1 \leq h \leq n, h \neq m$. Hence $\left(\sqrt{k_m}\right)^{2^{n-1}}$ can be extracted from the above product $(m = 1, \dots, n)$. Summarizing,

$$\prod_{1 \leq i < j \leq 2^n} (l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})) = 2^{2^{n-1}(2^n - 1)} \cdot (\sqrt{k_1 \dots k_n})^{2^{n-1}} \cdot I_0(x_2, \dots, x_{2^n}), \tag{3.2}$$

where $I_0(x_2, \dots, x_{2^n})$ has coefficients in $\mathbb{Z}$.

Finally, by (3.1), (3.2) and using Lemma 1 we obtain

$$2^{2^n(2^n-1)} \left(\sqrt{k_1 \dots k_n}\right)^{2^n} \cdot (I_0(x_2, \dots, x_{2^n}))^2 = \\ = (I(x_2, \dots, x_{2^n}))^2 (k_1 \dots k_n)^{2^{n-1}} \cdot 2^{n \cdot 2^n},$$

where $I_0(x_2, \dots, x_{2^n})$ has rational integer values. This means

$$I(x_2, \dots, x_{2^n}) = 2^{2^{n-1}(2^n - n - 1)} \cdot I_0(x_2, \dots, x_{2^n}).$$

Thus the theorem is proved. □

We proceed by proving Theorem 3.

Proof of Theorem 3

In the following, we have to use some results about composits of number fields. Let L be a number field of degree l with integral basis $\{\xi_1 = 1, \xi_2, \dots, \xi_l\}$ and discriminant D_L, and M another number field of degree m with integral basis $\{\eta_1 = 1, \eta_2, \dots, \eta_m\}$ and discriminant D_M. Denote by $K = LM$ the composite of L and M and assume that the discriminants are coprime: $(D_L, D_M) = 1$. Then (cf. [5]) an integral basis of K is

$$\{\xi_j \eta_k \mid j = 1, \dots, l\ ;\ k = 1, \dots, m\} \tag{3.3}$$

and the discriminant of K is

$$D_K = D_L^m \cdot D_M^l. \tag{3.4}$$

Let $K = \mathbb{Q}(\sqrt{k})$, $L = \mathbb{Q}(\sqrt{l})$, $M = \mathbb{Q}(\sqrt{m})$. It is well-known that the integral bases of K, L, M are $\{1, \omega_1\}$, $\{1, \omega_2\}$, $\{1, \omega_3\}$, respectively, where

$$\omega_1 = \begin{cases} \frac{1+\sqrt{k}}{2} & \text{if } k \equiv 1 \pmod 4 \\ \sqrt{k} & \text{if } k \equiv 2 \text{ or } 3 \pmod 4 \end{cases}, \quad \omega_2 = \frac{1+\sqrt{l}}{2}, \quad \omega_3 = \frac{1+\sqrt{m}}{2}.$$

The discriminants are

$$D_K = \begin{cases} k & \text{if } k \equiv 1 \pmod 4 \\ 4k & \text{if } k \equiv 2 \text{ or } 3 \pmod 4 \end{cases}, \quad D_L = l, \ D_M = m.$$

By our assumptions k, l, m are pairwise coprime and l, m are odd, hence D_K, D_L, D_M are pairwise coprime. Using (3.3) and (3.4) we obtain that

$$\{1, \omega_1, \omega_2, \omega_3, \omega_1\omega_2, \omega_1\omega_3, \omega_2\omega_3, \omega_1\omega_2\omega_3\} \tag{3.5}$$

is an integral basis of N.

Let $\left\{(\varepsilon_1^{(j)}, \varepsilon_2^{(j)}, \varepsilon_3^{(j)}) \mid j = 1, \dots, 8\right\}$ be the set of all vectors with components ± 1 arranged in antilexicographical order.

We distinguish three cases.

Case 1: If $k \equiv 2$ or $3 \pmod 4$, but $k \neq -1$.

In this case the discriminant of N is $D_N = 256 k^4 l^4 m^4$ by (3.4). Consider the linear forms

$$\begin{aligned} l^{(j)}(\underline{x}) \ = \ & x_1 + x_2 \varepsilon_1^{(j)} \sqrt{k} + x_3 \frac{1 + \varepsilon_2^{(j)} \sqrt{l}}{2} + x_4 \frac{1 + \varepsilon_3^{(j)} \sqrt{m}}{2} + x_5 \varepsilon_1^{(j)} \sqrt{k} \frac{1 + \varepsilon_2^{(j)} \sqrt{l}}{2} \\ & + x_6 \varepsilon_1^{(j)} \sqrt{k} \frac{1 + \varepsilon_3^{(j)} \sqrt{m}}{2} + x_7 \frac{1 + \varepsilon_2^{(j)} \sqrt{l} + \varepsilon_3^{(j)} \sqrt{m} + \varepsilon_2^{(j)} \varepsilon_3^{(j)} \sqrt{lm}}{4} \\ & + x_8 \varepsilon_1^{(j)} \sqrt{k} \frac{1 + \varepsilon_2^{(j)} \sqrt{l} + \varepsilon_3^{(j)} \sqrt{m} + \varepsilon_2^{(j)} \varepsilon_3^{(j)} \sqrt{lm}}{4} \\ & (j = 1, \dots, 8) \end{aligned}$$

We subdivide the 28 differences of type $l^{(i)}(\underline{x}) - l^{(j)}(\underline{x})$ $(1 \le i < j \le 8)$ into seven groups (see a.-g. below), each with four differences, the product of which is an integer for any $x_2, \dots, x_8 \in \mathbb{Z}$. For distinct indices $e, f, i, j \in \{2, \dots, 8\}$ set

$$A_{efij} = 2x_e + 2x_f\sqrt{k} + x_i + x_j\sqrt{k}$$

$$\overline{A}_{efij} = 2x_e - 2x_f\sqrt{k} + x_i - x_j\sqrt{k}$$

$$A_{ij} = x_i + x_j\sqrt{k}$$

$$\overline{A}_{ij} = x_i - x_j\sqrt{k}$$

a.)

$$\left(l^{(1)}(\underline{x}) - l^{(2)}(\underline{x})\right)\left(l^{(3)}(\underline{x}) - l^{(4)}(\underline{x})\right)\left(l^{(5)}(\underline{x}) - l^{(6)}(\underline{x})\right)\left(l^{(7)}(\underline{x}) - l^{(8)}(\underline{x})\right) = \\ = m^2 \cdot F_1(\underline{x})$$

where

$$F_1(\underline{x}) = \frac{1}{4}\left(A_{4678}^2 - l \cdot A_{78}^2\right) \cdot \frac{1}{4}\left(\overline{A}_{4678}^2 - l \cdot \overline{A}_{78}^2\right).$$

By $l \equiv 1 \pmod 4$ it can be easily seen that both the first and the second factor is an element of $\mathbb{Z}_K$ and they are conjugates of each other, hence their product $F_1(\underline{x})$ is a rational integer.

b.)

$$\left(l^{(1)}(\underline{x}) - l^{(3)}(\underline{x})\right)\left(l^{(2)}(\underline{x}) - l^{(4)}(\underline{x})\right)\left(l^{(5)}(\underline{x}) - l^{(7)}(\underline{x})\right)\left(l^{(6)}(\underline{x}) - l^{(8)}(\underline{x})\right) = \\ = l^2 \cdot F_2(\underline{x})$$

where

$$F_2(\underline{x}) = \frac{1}{4}\left(A_{3578}^2 - m \cdot A_{78}^2\right) \cdot \frac{1}{4}\left(\overline{A}_{3578}^2 - m \cdot \overline{A}_{78}^2\right).$$

Similarly both factors are elements of $\mathbb{Z}_K$ by $m \equiv 1 \pmod 4$ and their product $F_2(\underline{x})$ is a rational integer.

c.)

$$\left(l^{(1)}(\underline{x}) - l^{(5)}(\underline{x})\right)\left(l^{(2)}(\underline{x}) - l^{(6)}(\underline{x})\right)\left(l^{(3)}(\underline{x}) - l^{(7)}(\underline{x})\right)\left(l^{(4)}(\underline{x}) - l^{(8)}(\underline{x})\right) = \\ = 16k^2 \cdot F_3(\underline{x})$$

where the product $F_3(\underline{x})$ takes rational integer values.

d.)

$$F_4(\underline{x}) = \\ = \left(l^{(1)}(\underline{x}) - l^{(4)}(\underline{x})\right)\left(l^{(2)}(\underline{x}) - l^{(3)}(\underline{x})\right)\left(l^{(5)}(\underline{x}) - l^{(8)}(\underline{x})\right)\left(l^{(6)}(\underline{x}) - l^{(7)}(\underline{x})\right) = \\ = \frac{1}{4}\left(l \cdot A_{3578}^2 - m \cdot A_{4678}^2\right) \cdot \frac{1}{4}\left(l \cdot \overline{A}_{3578}^2 - m \cdot \overline{A}_{4678}^2\right)$$

Here by $l \equiv m \pmod 4$ we get that each factor is in $\mathbb{Z}_K$ and they are conjugates of each other, hence their product $F_4(\underline{x})$ is a rational integer.

e.)

$$F_5(\underline{x}) = \left(l^{(1)}(\underline{x}) - l^{(6)}(\underline{x})\right)\left(l^{(2)}(\underline{x}) - l^{(5)}(\underline{x})\right)\left(l^{(3)}(\underline{x}) - l^{(8)}(\underline{x})\right)\left(l^{(4)}(\underline{x}) - l^{(7)}(\underline{x})\right)$$

is a rational integer, too.

f.)

$$F_6(\underline{x}) = \left(l^{(1)}(\underline{x}) - l^{(7)}(\underline{x})\right)\left(l^{(2)}(\underline{x}) - l^{(8)}(\underline{x})\right)\left(l^{(3)}(\underline{x}) - l^{(5)}(\underline{x})\right)\left(l^{(4)}(\underline{x}) - l^{(6)}(\underline{x})\right)$$

is an element of $\mathbb{Z}$.

g.) Finally let

$$F_7(\underline{x}) = \left(l^{(1)}(\underline{x}) - l^{(8)}(\underline{x})\right)\left(l^{(2)}(\underline{x}) - l^{(7)}(\underline{x})\right)\left(l^{(3)}(\underline{x}) - l^{(6)}(\underline{x})\right)\left(l^{(4)}(\underline{x}) - l^{(5)}(\underline{x})\right)$$

If we write down these four differences we can see that they are conjugates of each other over K, hence $F_7(\underline{x})$ takes values in $\mathbb{Z}_K$. But if we multiply the first factor by the last one, and the second by the third one, we get

$$\begin{aligned} F_7(\underline{x}) &= \\ &= \left[k\left(2x_2 + x_5 + x_6 + x_8\frac{1+\sqrt{lm}}{2}\right)^2 - \left(x_3\sqrt{l} + x_4\sqrt{m} + x_7\frac{\sqrt{l}+\sqrt{m}}{2}\right)^2\right]\cdot \\ &\cdot\left[k\left(2x_2 + x_5 + x_6 + x_8\frac{1-\sqrt{lm}}{2}\right)^2 - \left(x_3\sqrt{l} - x_4\sqrt{m} + x_7\frac{\sqrt{l}-\sqrt{m}}{2}\right)^2\right] \end{aligned}$$

We can see that if we perform this multiplication, then there remain no terms depending on $\sqrt{k}$. It means that $F_7(\underline{x})$ has rational integer values.

Now by (1.1) the index form corresponding to the integral basis (3.5) is

$$\left(16k^2l^2m^2\prod_{j=1}^{7}F_j(\underline{x})\right)^2 = (I(x_2,\dots,x_8))^2\cdot D_N,$$

$$I(x_2,\dots,x_8) = \prod_{j=1}^{7}F_j(\underline{x}).$$

We obtained that if $x_2,\dots,x_8 \in \mathbb{Z}$, then $F_j(\underline{x}) \in \mathbb{Z}$ $(j = 1,\dots,7)$. So if we want to solve the index form equation with ±1 on the right hand side, then $F_j(\underline{x}) = \pm1$ $(j = 1,\dots,7)$ must hold.

It means that $F_1(\underline{x}) = \pm1$. But $F_1(\underline{x})$ is a product of two integers in $\mathbb{Z}_K$. In Case 1 only ±1 are units in $\mathbb{Z}_K$, hence the first factor is

$$\frac{1}{4}\left[A_{4678}^2 - l\cdot A_{78}^2\right] = \pm1.$$

Similarly using $F_2(\underline{x}) = \pm1$, $F_4(\underline{x}) = \pm1$ we get

$$\frac{1}{4}\left[A_{3578}^2 - m\cdot A_{78}^2\right] = \pm1,$$

$$\frac{1}{4}\left[l\cdot A_{3578}^2 - m\cdot A_{4678}^2\right] = \pm1.$$

For brevity set $x = A_{78}^2$, $y = A_{3578}^2$, $z = A_{4678}^2$. With this notation our system of equations is (the signs are independent)

$$\begin{aligned} y - mx &= \pm 4, \\ z - lx &= \pm 4, \\ ly - mz &= \pm 4. \end{aligned} \tag{3.6}$$

From the first two equations we get $y = mx \pm 4$, $z = lx \pm 4$. Substitute these equations into the third one to get

$$l(mx \pm 4) - m(lx \pm 4) = \pm 4,$$

whence

$$\pm l \pm m = \pm 1.$$

But the sum and the difference of l and m is even, because $l \equiv m \pmod 4$. It is a contradiction, which means that the index form equation with ± 1 on the right hand side is unsolvable.

Case 2: If $k = -1$.

In this case the first part of the proof is the same as in Case 1. But in this case the units in $\mathbb{Z}_K = \mathbb{Z}_{\mathbb{Q}(\sqrt{i})}$ are i^α ($\alpha = 0, 1, 2, 3$). Hence using the notation of Case 1, instead of (3.6) we get the system of equations

$$\begin{aligned} y - mx &= 4i^{\alpha_1}, \\ z - lx &= 4i^{\alpha_2}, \\ ly - mz &= 4i^{\alpha_3}, \end{aligned}$$

with exponents $\alpha_1, \alpha_2, \alpha_3 \in \{0, 1, 2, 3\}$.

After substitutions

$$l(mx + 4i^{\alpha_1}) - m(lx + 4i^{\alpha_2}) = 4i^{\alpha_3},$$

that is

$$li^{\alpha_1} - mi^{\alpha_2} = i^{\alpha_3}.$$

Then $1 = |i^{\alpha_3}| = |li^{\alpha_1} - mi^{\alpha_2}| \geq \big|\, |li^{\alpha_1}| - |mi^{\alpha_2}| \,\big| = \big|\, |l| - |m| \,\big| \geq 2$, because of the assumptions $l \equiv m \equiv 1 \pmod 4$, $(l, m) = 1$ and $l, m \neq 1$. It is a contradiction, which, similarly to Case 1 means that the index form equation is again unsolvable.

Case 3: If $k \equiv 1 \pmod 4$.

The proof in this case can be done similarly to Cases 1 and 2. Since by (3.4) in this case the discriminant $D_N = k^4 l^4 m^4$ of N is odd, hence the non-monogenity of N follows from Theorem 1, too.

In each case we showed that the index form equation is unsolvable with ± 1 on the right hand side, that is N is not monogeneous. □

Acknowledgement

The author would like to thank the referee for the valuable remarks and for suggesting Theorem 1.

References

[1] I.Gaál, Diophantine equations and power integral bases, Birkhauser Boston, 2002.

[2] I.Gaál, A.Pethő and M.Pohst, *On the resolution of index form equations in biquadratic number fields, III. The bicyclic biquadratic case*, J.Number Theory, **53** (1995), 100–114.

[3] M.N.Gras and F.Tanoe, *Corps biquadratiques monogénes*, Manuscripta Math., **86** (1995), 63–79.

[4] T.Nakahara, *On the indices and integral bases of non-cyclic but abelian biquadratic fields*, Archiv. der Math., **41** (1983), 504–508.

[5] W.Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Second Edition, Springer Verlag, 1990.

[6] G.Nyul, *Power integral bases in totally complex biquadratic number fields*, Acta Acad. Paed. Agriensis, Sectio Mathematicae, **28** (2001), 79-86.

[7] B.Schmal, *Diskriminanten, $\mathbb{Z}$-Ganzheitsbasen und relative Ganzheitsbasen bei multiquadratischen Zahlkörpern*, Arch. Math., **52** (1989), 245-257.

[8] K.S.Williams, *Integers of biquadratic fields*, Canad. Math. Bull., **13** (1970), 519–526.

University of Debrecen, Institute of Mathematics and Informatics, H–4010
Debrecen Pf.12., Hungary
E-mail address: gnyul@dragon.klte.hu