Noname manuscript No.
(will be inserted by the editor)

Elements with prime and small indices in bicyclic biquadratic number fields

Tímea Arnóczki

Received: date / Accepted: date

Abstract We give necessary and sufficient conditions for the existence of primitive algebraic integers with index A in totally complex bicyclic biquadratic number fields where A is an odd prime or a positive rational integer at most 10. We also determine all these elements and prove that there are infinitely many totally complex bicyclic biquadratic number fields containing elements with index A.

Keywords bicyclic biquadratic number fields · index · index form equation

Mathematics Subject Classification (2000) 11R16 · 11D57

1 Introduction

It is well known that all algebraic number fields have an integral basis. However, the existence of an integral basis of the form $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$, the so-called power integral basis, is not guaranteed. We say that a number field is monogeneous if it admits a power integral basis with α being its generator.

Let K be an algebraic number field of degree n. If $\alpha \in \mathbb{Z}_K$ is a primitive element of K, then the index $I(\alpha)$ of α is defined as the subgroup index $\left(\mathbb{Z}_K^+ : \mathbb{Z}[\alpha]^+\right)$. It can be proved that $D_{K/\mathbb{Q}}(\alpha) = D_K \cdot (I(\alpha))^2$, where $D_{K/\mathbb{Q}}(\alpha)$ and D_K denote the discriminants of α and K, respectively.

It follows directly from the definition that α generates a power integral basis if and only if $\mathbb{Z}[\alpha] = \mathbb{Z}_K$, that is, the index of α equals 1. It is also obvious that $\mathbb{Z}[a + \alpha] = \mathbb{Z}[\alpha]$ if $a \in \mathbb{Z}$, consequently $I(a + \alpha) = I(\alpha)$.

The field index and minimal index of K are defined as the greatest common divisor and the minimum of the indices of all primitive elements in $\mathbb{Z}_K$, respectively. It is easy to see that the minimal index of K equals 1 if and only if K is

Supported by the ÚNKP-16-2-II New National Excellence Program of the Ministry of Human Capacities

T. Arnóczki
Institute of Mathematics, University of Debrecen
H–4002 Debrecen P.O.Box 400, Hungary
E-mail: arnoczkitimi@gmail.com

monogeneous, furthermore, if K is monogeneous, then the field index of K equals 1.

Let $(\omega_1 = 1, \omega_2, \ldots, \omega_n)$ be an integral basis of K. Then there exists a homogeneous polynomial $I(X_2, \ldots, X_n)$ of degree $\frac{n(n-1)}{2}$ with rational integer coefficients and $n-1$ variables such that

$$D_{K/\mathbb{Q}}(x_1 + x_2\omega_2 + \ldots + x_n\omega_n) = D_K \cdot (I(x_2, \ldots, x_n))^2$$

if $x_1, \ldots, x_n \in \mathbb{Z}$. This polynomial is called the index form corresponding to the above integral basis.

If $\alpha = x_1 + x_2\omega_2 + \ldots + x_n\omega_n$ $(x_1, \ldots, x_n \in \mathbb{Z})$ is a primitive element in $\mathbb{Z}_K$, then $I(\alpha) = |I(x_2, \ldots, x_n)|$, hence finding elements with index A is equivalent to solving a certain type of diophantine equations, the so-called index form equation $I(x_2, \ldots, x_n) = \pm A$. This task is one of the essential problems of algebraic number theory.

K. Győry [9] effectively proved that index form equations have finitely many solutions, consequently, a number field has only finitely many elements with given index apart from translation by rational integers. However, there is no efficient algorithm for solving index form equations in general, only in case of some number fields of small degree or with special properties. For more details in connection with this topic, cf. [3], [10].

Henceforth, we will be concerned with the problem of monogeneity in bicyclic biquadratic number fields.

Let $m, n \in \mathbb{Z} \setminus \{0, 1\}$ be distinct square-free rational integers. Then number fields of the form $\mathbb{Q}(\sqrt{m}, \sqrt{n}) = \mathbb{Q}(\sqrt{m} + \sqrt{n})$ are called bicyclic biquadratic fields. These are the quartic fields whose Galois group is the Klein group.

The monogeneity and field index of bicyclic biquadratic fields were first studied by T. Nakahara [19], who proved that there are infinitely many bicyclic biquadratic fields having power integral basis and there exist infinitely many non-monogeneous bicyclic biquadratic fields, moreover, their minimal index can be greater than any given number. He also showed that the field index of a bicyclic biquadratic field is even if and only if its discriminant is odd, and for any positive divisor l of 12 there are infinitely many bicyclic biquadratic fields having field index l. I. Gaál, A. Pethő and M. Pohst [6] gave another proof for this latter statement and, in addition, established necessary and sufficient conditions for bicyclic biquadratic fields to have field index l for any positive divisor l of 12.

M.-N. Gras and F. Tanoé [8] gave necessary and sufficient conditions for bicyclic biquadratic fields to admit power integral bases, and Y. Motoda [14], [15] studied the monogeneity of bicyclic biquadratic fields on the grounds of these conditions.

I. Gaál, A. Pethő and M. Pohst [7] gave an algorithm for finding elements with given index in totally real bicyclic biquadratic fields ($m > 0$, $n > 0$) by solving systems of simultaneous Pellian equations.

B. Jadrijević [11], [12], partly in common with I. Gaál [4], determined the field index, minimal index and elements with minimal index in four parametric families of totally real bicyclic biquadratic fields.

Studying pure quartic fields, T. Funakura [2] proved that $\mathbb{Q}(\sqrt{-1}, \sqrt{n})$ ($n \geq 2$ is a square-free integer) is monogeneous if and only if $n = 2, 3, 5$.

G. Nyul [20] established necessary and sufficient conditions for the monogeneity of totally complex bicyclic biquadratic fields ($m < 0$ or $n < 0$) and determined

all generators of power integral bases. The complete proof can be found in [22]. Later, M.-L. Chang [1] also showed this theorem in a different way.

I. Gaál and G. Nyul [5] gave an efficient algorithm for solving the Mahler type variant of the index form equation, that is, for determining elements with index divisible only by some fixed primes in bicyclic biquadratic fields. By using this method, B. Jadrijević [13] considered the existence of elements with index 2^a3^b in one of the parametric bicyclic biquadratic fields mentioned above.

We remark that, as a generalization, the monogeneity of multiquadratic number fields $\mathbb{Q}(\sqrt{k_1},\ldots,\sqrt{k_r})$ was also studied in [21], [16], [17], [23].

In the present paper, after considering the results in Section 2 that we need later, in Section 3 we establish necessary and sufficient conditions for totally complex bicyclic biquadratic number fields to have elements with odd prime index (Theorem 3.1), and with the other indices between 2 and 10 (Theorem 3.2). We also describe all these elements with given index and show that infinitely many totally complex bicyclic biquadratic number fields contain elements with these indices. In order to prove our theorems, we solve multiparametric index form equations.

2 Bicyclic biquadratic number fields

In this section, we introduce some notations and summarize the results we need in the rest of the paper.

Consider the bicyclic biquadratic number field $\mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)$ where $m,n\in\mathbb{Z}\setminus\{0,1\}$ are distinct square-free integers. In the following, $d>0$ denotes the greatest common divisor of m and n, and let m_1 and n_1 be defined by $m=dm_1$ and $n=dn_1$. Then it is easy to see that

$$\mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)=\mathbb{Q}\left(\sqrt{m},\sqrt{m_1n_1}\right)=\mathbb{Q}\left(\sqrt{n},\sqrt{m_1n_1}\right).$$

By applying this, K. S. Williams [24] observed that any bicyclic biquadratic field $\mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)$ is included in one of the five cases listed below considering the residues of m and n modulo 4. In the totally complex case, G. Nyul [20] refined this classification with respect to the signs of m and n:

Case 1: $m\equiv n\equiv 1 \pmod 4$, $m_1\equiv n_1\equiv 1 \pmod 4$
($m>0$, $n<0$)

Case 2: $m\equiv n\equiv 1 \pmod 4$, $m_1\equiv n_1\equiv 3 \pmod 4$
($m>0$, $n<0$)

Case 3: $m\equiv 1 \pmod 4$ $n\equiv 2 \pmod 4$
(Case 3/A: $m>0$, $n<0$, Case 3/B: $m<0$, $n>0$)

Case 4: $m\equiv 2 \pmod 4$, $n\equiv 3 \pmod 4$
(Case 4/A: $m>0$, $n<0$, Case 4/B: $m<0$, $n>0$)

Case 5: $m\equiv n\equiv 3 \pmod 4$
(Case 5/A: $m>0$, $n<0$, Case 5/B: $m<0$, $n<0$)

In each case, K. S. Williams [24] gave the discriminant of $\mathbb{Q}\left(\sqrt{m},\sqrt{n}\right)$ and also described an integral basis:

Case 1: $\left(1,\frac{1+\sqrt{m}}{2},\frac{1+\sqrt{n}}{2},\frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right)$

Case 2: $\left(1,\frac{1+\sqrt{m}}{2},\frac{1+\sqrt{n}}{2},\frac{1-\sqrt{m}+\sqrt{n}+\sqrt{m_1n_1}}{4}\right)$

Case 3: $\left(1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n}+\sqrt{m_1 n_1}}{2}\right)$
Case 4: $\left(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{m}+\sqrt{m_1 n_1}}{2}\right)$
Case 5: $\left(1, \sqrt{m}, \frac{\sqrt{m}+\sqrt{n}}{2}, \frac{1+\sqrt{m_1 n_1}}{2}\right)$

I. Gaál, A. Pethő and M. Pohst [6] determined the corresponding index forms:
Case 1: $\left(d(X_2+\frac{X_4}{2})^2-\frac{n_1}{4}X_4^2\right)\left(d(X_3+\frac{X_4}{2})^2-\frac{m_1}{4}X_4^2\right)\left(n_1(X_3+\frac{X_4}{2})^2-m_1(X_2+\frac{X_4}{2})^2\right)$
Case 2: $\left(d(X_2-\frac{X_4}{2})^2-\frac{n_1}{4}X_4^2\right)\left(d(X_3+\frac{X_4}{2})^2-\frac{m_1}{4}X_4^2\right)\left(n_1(X_3+\frac{X_4}{2})^2-m_1(X_2-\frac{X_4}{2})^2\right)$
Case 3: $(dX_2^2-n_1X_4^2)\left(d(X_3+\frac{X_4}{2})^2-\frac{m_1}{4}X_4^2\right)(n_1(2X_3+X_4)^2-m_1X_2^2)$
Case 4: $\left(\frac{d}{2}(2X_2+X_4)^2-\frac{n_1}{2}X_4^2\right)\left(2dX_3^2-\frac{m_1}{2}X_4^2\right)\left(2n_1X_3^2-\frac{m_1}{2}(2X_2+X_4)^2\right)$
Case 5: $(d(2X_2+X_3)^2-n_1X_4^2)(dX_3^2-m_1X_4^2)\left(\frac{n_1}{4}X_3^2-m_1(X_2+\frac{X_3}{2})^2\right)$

Finally, we recall the results of G. Nyul [20]. In Cases 1, 2 and 3/A, the field $\mathbb{Q}(\sqrt{m},\sqrt{n})$ is not monogeneous. In the other cases, the necessary and sufficient conditions for $\mathbb{Q}(\sqrt{m},\sqrt{n})$ to admit power integral bases and the coordinates of the generators $x_1\omega_1+x_2\omega_2+x_3\omega_3+x_4\omega_4$ $(x_1,x_2,x_3,x_4\in\mathbb{Z})$, where $(\omega_1,\omega_2,\omega_3,\omega_4)$ denotes the integral basis given by K. S. Williams, are listed in Table 1.

Table 1 Generators of power integral bases

Case	condition	(x_2,x_3,x_4)
3/B	$m_1=-1,\ d-4n_1=-1$	$\pm(1,1,-2),\pm(1,-1,2)$
4/A	$(m,n)=(2,-1)$	$\pm(0,0,1),\pm(1,0,-1)$
4/B	$m_1=-2,\ d-n_1=\pm2$	$\pm(0,0,1),\pm(1,0,-1)$
5/A	$(m,n)=(3,-1)$	$\pm(1,-2,1),\pm(-1,2,1),\ \pm(0,1,0),\pm(1,-1,0)$
	$n_1=-1,\ 4d-m_1=1,$ $(m,n)\neq(3,-1)$	$\pm(1,-2,1),\pm(-1,2,1)$
5/B	$d=1,\ m-n=\pm4$	$\pm(0,1,0),\pm(-1,1,0)$

3 Results

In this section, we state our main results, giving necessary and sufficient conditions for totally complex bicyclic biquadratic number fields to have elements first with odd prime index, then with index at most 10, and determining all these elements.

Theorem 3.1 *Let m, n be distinct square-free rational integers, not equal to 0 or 1, so that they belong to one of the eight cases listed in the totally complex case. Let $(\omega_1,\omega_2,\omega_3,\omega_4)$ denote the integral basis of the bicyclic biquadratic number field $\mathbb{Q}(\sqrt{m},\sqrt{n})$ given by K. S. Williams. The necessary and sufficient conditions for the existence of elements with index p in $\mathbb{Q}(\sqrt{m},\sqrt{n})$, where p denotes a positive odd prime, and the coordinates of these elements $x_1\omega_1+x_2\omega_2+x_3\omega_3+x_4\omega_4$ $(x_1,x_2,x_3,x_4\in\mathbb{Z})$ are contained in Table 2. (In Cases 1 and 2, there exist no elements with index p for any p.)*

Remark It is obvious from the conditions that there exist only finitely many rational integers m and n satisfying the conditions signed by $(*)$. However, we will

Table 2 Elements with prime index

Case	condition	(x_2, x_3, x_4)
3/A	if $p \equiv 1 \pmod 4$: $d = 1$, $m - 4n = p$ $(*)$	$\pm(1, 1, 0), \pm(1, -1, 0)$
	if $p \equiv 1 \pmod 4$: $m_1 = 1$, $d - 4n_1 = p$ $(*)$	$\pm(1, -1, 2), \pm(1, 1, -2)$
3/B	if $p = 3$: $(m, n) = (-3, 6)$ $(*)$	$\pm(1, 0, 1), \pm(1, -1, 1),$ $\pm(-1, 0, 1), \pm(-1, -1, 1)$
	if $p \equiv 1 \pmod 4$: $m_1 = -1$, $d - 4n_1 = -p$	$\pm(1, -1, 2), \pm(1, 1, -2)$
	if $p \equiv 3 \pmod 4$: $m_1 = -1$, $d - 4n_1 = p$	
	if $p \equiv 3 \pmod 4$: $d = 1$, $4n - m = p$ $(*)$	$\pm(1, 1, 0), \pm(1, -1, 0)$
	if $p \equiv 5 \pmod{16}$, $p - 1$ is a square and $\frac{p+3}{4}$ is square-free: $(m, n) = (-3, \frac{p+3}{4})$ $(*)$	$\pm(\frac{\sqrt{p-1}}{2}, 0, 1), \pm(\frac{\sqrt{p-1}}{2}, -1, 1),$ $\pm(\frac{\sqrt{p-1}}{2}, 0, -1), \pm(\frac{\sqrt{p-1}}{2}, 1, -1)$
4/A	$m_1 = 2$, $d - n_1 = 2p$ $(*)$	$\pm(0, 0, 1), \pm(-1, 0, 1)$
	if $p = 3$: $(m, n) = (2, -1)$ $(*)$	$\pm(0, 1, 1), \pm(0, -1, 1),$ $\pm(-1, 1, 1), \pm(-1, -1, 1)$
	if $p \equiv 1 \pmod 4$, $p - 1$ is a square and $p + 1$ is square-free: $(m, n) = (p + 1, -1)$ $(*)$	$\pm(0, \frac{\sqrt{p-1}}{2}, 1), \pm(0, \frac{\sqrt{p-1}}{2}, -1),$ $\pm(-1, \frac{\sqrt{p-1}}{2}, 1), \pm(1, \frac{\sqrt{p-1}}{2}, -1)$
4/B	$m_1 = -2$, $d - n_1 = \pm 2p$	$\pm(-1, 0, 1), \pm(0, 0, 1)$
5/A	$d = 1$, $m - n = 4p$ $(*)$	$\pm(0, 1, 0), \pm(-1, 1, 0)$
	if $p \equiv 1 \pmod 4$: $n_1 = -1$, $4d - m_1 = p$	$\pm(-1, 2, 1), \pm(1, -2, 1)$
	if $p \equiv 3 \pmod 4$: $n_1 = -1$, $4d - m_1 = -p$	
	if $p \equiv 1 \pmod{16}$, $p - 1$ is a square and $\frac{3p+1}{4}$ is square-free: $(m, n) = (\frac{9p+3}{4}, \frac{-3p-1}{4})$ $(*)$	$\pm(0, 1, \frac{\sqrt{p-1}}{2}), \pm(0, -1, \frac{\sqrt{p-1}}{2}),$ $\pm(-1, 1, \frac{\sqrt{p-1}}{2}), \pm(1, -1, \frac{\sqrt{p-1}}{2})$
5/B	$d = 1$, $m - n = \pm 4p$	$\pm(0, 1, 0), \pm(-1, 1, 0)$
	if $p \equiv 1 \pmod 4$: $n_1 = -1$, $4d - m_1 = p$ $(*)$	$\pm(-1, 2, 1), \pm(1, -2, 1)$
	if $p \equiv 1 \pmod 4$: $m_1 = -1$, $4d - n_1 = p$ $(*)$	$\pm(1, 0, 1), \pm(-1, 0, 1)$

show in the proof that the number of pairs (m, n) satisfying the other equalities is infinite. In order to prove it, we will need Lemma 4.1.

In Case 5/B, we obtain the same number fields by interchanging m and n because of the symmetry of the conditions.

Theorem 3.2 *Let m, n be distinct square-free rational integers, not equal to 0 or 1, so that they belong to one of the eight cases listed in the totally complex case. Let $(\omega_1, \omega_2, \omega_3, \omega_4)$ denote the integral basis of the bicyclic biquadratic number field $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ given by K. S. Williams. The necessary and sufficient conditions for the existence of elements with index $A \in \{2, 4, 6, 8, 9, 10\}$ in $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ and the coordinates of these elements $x_1\omega_1 + x_2\omega_2 + x_3\omega_3 + x_4\omega_4$ $(x_1, x_2, x_3, x_4 \in \mathbb{Z})$ are contained in Tables 3–8. (If a case does not appear in the table of index A, it means there exist no elements with index A in that case.)*

Table 3 Elements with index $A = 2$

Case	condition	(x_2, x_3, x_4)
1	$(m, n) = (5, -15), (5, -3)$	$\pm(0, 0, 1), \pm(0, -1, 1), \pm(-1, 0, 1), \pm(-1, -1, 1)$
2	$(m, n) = (21, -7), (21, -3)$	$\pm(0, 0, 1), \pm(0, -1, 1), \pm(1, 0, 1), \pm(1, -1, 1)$
5/A	$(m, n) = (3, -5), (7, -1)$	$\pm(0, 1, 0), \pm(-1, 1, 0)$
5/B	$d = 1$, $m - n = \pm 8$	$\pm(0, 1, 0), \pm(-1, 1, 0)$

Table 4 Elements with index $A = 4$

Case	condition	(x_2, x_3, x_4)
2	$n_1 = -1,\ 4d - m_1 = 1$	$\pm(1,1,2), \pm(1,-3,2)$
	$n_1 = -1,\ d - 4m_1 = -1$	$\pm(2,-1,4), \pm(2,-3,4)$
	$n_1 = -1,\ d - m_1 = \pm 4$	$\pm(1,0,2), \pm(1,-2,2)$
3/A	$n_1 = -2,\ d - m_1 = \pm 4$	$\pm(0,0,1), \pm(0,-1,1)$
3/B	$(m,n) = (-3,2), (-3,6)$	$\pm(0,0,1), \pm(0,-1,1)$
	$m_1 = -1,\ d - 16n_1 = -1$	$\pm(1,-2,4), \pm(1,2,-4)$
5/A	$(m,n) = (3,-13), (11,-5)$	$\pm(0,1,0), \pm(-1,1,0)$
	$(m,n) = (3,-1)$	$\pm(0,1,1), \pm(-1,1,1), \pm(0,1,-1), \pm(-1,1,-1)$
	$(m,n) = (15,-1)$	$\pm(0,1,0), \pm(-1,1,0), \pm(-2,4,1), \pm(-2,4,-1)$
	$n_1 = -1,\ 16d - m_1 = 1,$ $(m,n) \neq (15,-1)$	$\pm(-2,4,1), \pm(-2,4,-1)$
5/B	$d = 1,\ m - n = \pm 16$	$\pm(0,1,0), \pm(-1,1,0)$

Table 5 Elements with index $A = 6$

Case	condition	(x_2, x_3, x_4)
1	$(m,n) = (5,-7), (5,-35)$	$\pm(0,0,1), \pm(0,-1,1), \pm(-1,0,1), \pm(-1,-1,1)$
2	$(m,n) = (21,-35), (21,-15),$ $(33,-11), (33,-3),$ $(77,-11), (77,-7)$	$\pm(0,0,1), \pm(0,-1,1), \pm(1,0,1), \pm(1,-1,1)$
5/A	$(m,n) = (7,-17), (11,-13),$ $(19,-5), (23,-1)$	$\pm(0,1,0), \pm(-1,1,0)$
5/B	$d = 1,\ m - n = \pm 24$	$\pm(0,1,0), \pm(-1,1,0)$

Table 6 Elements with index $A = 8$

Case	condition	(x_2, x_3, x_4)
1	$(m,n) = (5,-15)$	$\pm(0,-1,2), \pm(2,1,-2), \pm(1,1,-3),$ $\pm(1,2,-3), \pm(2,1,-3), \pm(2,2,-3)$
	$(m,n) = (5,-3)$	$\pm(0,1,1), \pm(0,-2,1), \pm(-1,1,1),$ $\pm(-1,-2,1), \pm(1,1,0), \pm(1,-1,0)$
2	$(m,n) = (69,-23)$	$\pm(2,-1,3), \pm(1,-1,3), \pm(2,-2,3), \pm(1,-2,3)$
	$(m,n) = (69,-3)$	$\pm(0,1,1), \pm(1,1,1), \pm(0,-2,1), \pm(1,-2,1)$
	$n_1 = -1,\ d - m_1 = \pm 8$	$\pm(1,0,2), \pm(1,-2,2)$
3/A	$n_1 = -2,\ d - m_1 = \pm 8$	$\pm(0,0,1), \pm(0,-1,1)$
3/B	$(m,n) = (-15,6), (-15,10),$ $(-7,2), (7,14)$	$\pm(0,0,1), \pm(0,-1,1)$
4/A	$n_1 = -1,\ d - m_1 = -1$	$\pm(-1,1,2), \pm(1,1,-2)$
5/A	$(m,n) = (3,-29), (11,-21),$ $(15,-17), (19,-13), (31,-1)$	$\pm(0,1,0), \pm(-1,1,0)$
5/B	$d = 1,\ m - n = \pm 32$	$\pm(0,1,0), \pm(-1,1,0)$

Remark In Cases 1 and 2, each number field containing elements with index A appears with two different parametrizations. For example $\mathbb{Q}(\sqrt{69}, \sqrt{-23}) = \mathbb{Q}(\sqrt{69}, \sqrt{-3})$ and $\mathbb{Q}(\sqrt{33}, \sqrt{-11}) = \mathbb{Q}(\sqrt{33}, \sqrt{-3})$ in Table 6 in Case 2.

Similarly to Theorem 3.1, it can be shown that there exist infinitely many pairs (m, n) satisfying the equalities that do not give particular number fields, furthermore, in Case 5/B, we get the same number fields again by interchanging m and n because of the symmetry of the conditions.

Finally, we remark that by using these tables and the theorem of G. Nyul at the end of Section 2, we can also describe the totally complex bicyclic biquadratic number fields whose minimal index is at most 10. The above tables mostly give

Table 7 Elements with index $A = 9$

case	condition	(x_2, x_3, x_4)
3/B	$m_1 = -1,\ 9d - 4n_1 = -1$	$\pm(3,-1,2), \pm(3,1,-2)$
	$m_1 = -1,\ d - 36n_1 = -1$	$\pm(1,-3,6), \pm(1,3,-6)$
	$m_1 = -1,\ d - 4n_1 = -9$	$\pm(1,-1,2), \pm(1,1,-2)$
	$m_1 = -3,\ d - 4n_1 = 1$	
4/A	$(m,n) = (2,-17), (6,-1),$ $(10,-65), (14,-77), (22,-77),$ $(26,-65), (34,-17)$	$\pm(0,0,1), \pm(-1,0,1)$
4/B	$m_1 = -2,\ 9d - n_1 = \pm 2$	$\pm(1,0,1), \pm(-2,0,1)$
	$m_1 = -2,\ d - 9n_1 = \pm 2$	$\pm(-1,0,3), \pm(-2,0,3)$
	$m_1 = -2,\ d - n_1 = \pm 18$	$\pm(-1,0,1), \pm(0,0,1)$
	$m_1 = -6,\ d - n_1 = \pm 2$	
5/A	$(m,n) = (7,-29), (19,-17),$ $(23,-13), (31,-5)$	$\pm(0,1,0), \pm(-1,1,0)$
	$(m,n) = (35,-1)$	$\pm(0,1,0), \pm(-1,1,0), \pm(-3,6,1), \pm(3,-6,1)$
	$n_1 = -1,\ 36d - m_1 = 1,$ $(m,n) \neq (35,-1)$	$\pm(-3,6,1), \pm(3,-6,1)$
	$n_1 = -1,\ 4d - 9m_1 = 1$	$\pm(-1,2,3), \pm(-1,2,-3)$
	$n_1 = -1,\ 4d - m_1 = 9$	$\pm(-1,2,1), \pm(-1,2,-1)$
	$n_1 = -3,\ 4d - m_1 = -1$	
5/B	$(m,n) = (-41,-5)$	$\pm(0,1,0), \pm(-1,1,0), \pm(-1,3,0), \pm(-2,3,0)$
	$(m,n) = (-5,-41)$	$\pm(0,1,0), \pm(-1,1,0), \pm(1,1,0), \pm(-2,1,0)$
	$(m,n) = (-5,-1)$	$\pm(-1,2,1), \pm(1,-2,1), \pm(-1,3,0), \pm(-2,3,0)$
	$(m,n) = (-1,-5)$	$\pm(1,1,0), \pm(-2,1,0), \pm(1,0,1), \pm(1,0,-1)$
	$d = 1,\ m - n = \pm 36,$ $(m,n) \neq (-5,-41), (-41,-5)$	$\pm(0,1,0), \pm(-1,1,0)$
	$d = 3,\ m - n = \pm 12$	
	$d = 1,\ m - 9n = \pm 4,$ $(m,n) \neq (-5,-1), (-41,-5)$	$\pm(-1,3,0), \pm(-2,3,0)$
	$d = 1,\ 9m - n = \pm 4,$ $(m,n) \neq (-1,-5), (-5,-41)$	$\pm(1,1,0), \pm(-2,1,0)$

Table 8 Elements with index $A = 10$

Case	condition	(x_2, x_3, x_4)
1	$(m,n) = (13,-39)$	$\pm(1,1,-3), \pm(2,1,-3), \pm(1,2,-3), \pm(2,2,-3)$
	$(m,n) = (13,-3)$	$\pm(0,1,1), \pm(0,-2,1), \pm(-1,1,1), \pm(-1,-2,1)$
2	$(m,n) = (93,-31)$	$\pm(2,-1,3), \pm(1,-1,3), \pm(2,-2,3), \pm(1,-2,3)$
	$(m,n) = (93,-3)$	$\pm(0,1,1), \pm(1,1,1), \pm(0,-2,1), \pm(1,-2,1)$
5/A	$(m,n) = (3,-37), (7,-33),$ $(11,-29), (19,-21),$ $(23,-17), (39,-1)$	$\pm(0,1,0), \pm(-1,1,0)$
5/B	$d = 1,\ m - n = \pm 40$	$\pm(0,1,0), \pm(-1,1,0)$

the necessary and sufficient conditions for a number field to have minimal index $A \in \{2, \ldots, 10\}$. Though there are number fields occuring in more tables, for example $\mathbb{Q}(\sqrt{-3}, \sqrt{6})$ contains elements with index 3, 4 and 5. In this case, we just have to find their first appearance to determine the minimal index.

4 Proof

In this section, firstly we collect the main ingredients of the proofs of our theorems, then we discuss the details.

In each case, the index form splits into the product of three quadratic forms with integer coefficients, let $Q_i(X_2, X_3, X_4)$ $(i = 1, 2, 3)$ denote these factors in the order given previously. In the totally complex case, two of them are semidefinite. It will cause no confusion in the rest of the proof if we use the abbreviation Q_i $(i = 1, 2, 3)$ to denote both the ith quadratic factor and its value after substituting integers.

The factors are linearly dependent and, substituting integers, the following congruences hold:
Cases 1 and 2: $m_1Q_1 + dQ_3 = n_1Q_2$, hence $Q_1 + Q_3 \equiv Q_2 \pmod 4$
Case 3: $m_1Q_1 + dQ_3 = 4n_1Q_2$, hence $Q_1 + Q_3 \equiv 0 \pmod 4$
Case 4: $m_1Q_1 + dQ_3 = n_1Q_2$, hence $2Q_1 + Q_3 \equiv 3Q_2 \pmod 4$
Case 5: $m_1Q_1 + 4dQ_3 = n_1Q_2$, hence $Q_1 \equiv Q_2 \pmod 4$

We remark that the dependency of the quadratic forms also appears in [7], but only concerning the absolute values of the factors. We will need these stronger relations.

In Cases 1 and 2, all factors cannot be odd because of the above congruence, hence there are no elements with odd index in these cases. This also follows from the results of T. Nakahara [19] or I. Gaál, A. Pethő and M. Pohst [6].

As we have mentioned before, in order to prove the remark in respect of the number of totally complex bicyclic biquadratic number fields containing elements with given index, we will need the following lemma by T. Nagel [18].

Lemma 4.1 *Let $f(x) \in \mathbb{Z}[x]$ be a primitive polynomial of degree k ($k \geq 2$) whose discriminant is not equal to 0. If $\gcd\{f(a) \mid a \in \mathbb{N}\}$ is k-power-free, then the values of $f(x)$ are k-power-free for infinitely many natural numbers.*

The proof of Theorem 3.1 is represented through Case 3/B, since the most important ideas appear here. The other cases and the whole Theorem 3.2 can be handled similarly.

Let $\widetilde{m}_1 = -m_1$. Then we have to solve the index form equation

$$(dx_2^2 - n_1x_4^2)\left(d(x_3 + \frac{x_4}{2})^2 + \frac{\widetilde{m}_1}{4}x_4^2\right)(n_1(2x_3 + x_4)^2 + \widetilde{m}_1x_2^2) = \pm p$$

in order to find elements with index p. In this case Q_2 and Q_3 are positive semidefinite and $Q_1 + Q_3 \equiv 0 \pmod 4$, hence (Q_1, Q_2, Q_3) can be $(\pm 1, 1, p)$, $(-1, p, 1)$ or $(\pm p, 1, 1)$.

I. If $(Q_1, Q_2, Q_3) = (\pm 1, 1, p)$, then the second factor implies the equality $d(2x_3 + x_4)^2 + \widetilde{m}_1x_4^2 = 4$. A square number is congruent to either 0 or 1 modulo 4, and in this case $\widetilde{m}_1$ is odd, hence $\widetilde{m}_1x_4^2 \equiv 0, 1$ or $3 \pmod 4$. Thus we have to consider the following four possibilities:

(i) $d(2x_3 + x_4)^2 = 4$ and $\widetilde{m}_1x_4^2 = 0$
Now we have $x_4 = 0$, $d = 1$ and $x_3 = \pm 1$. By substituting these values into Q_1, we obtain $x_2^2 = \pm 1$, hence $x_2 = \pm 1$, $Q_1 = 1$. Then $p \equiv 3 \pmod 4$ follows from the congruence of the factors mentioned above. From the third factor, we get the relation $4n - m = p$. (There exist only finitely many m and n satisfying this equality according to their signs.) Under these conditions, the solutions of the index form equation are $(x_2, x_3, x_4) = \pm(1, 1, 0), \pm(1, -1, 0)$.

(ii) $d(2x_3 + x_4)^2 = 3$ and $\widetilde{m}_1x_4^2 = 1$
In this case $d = 3$, $2x_3 + x_4 = \pm 1$, $\widetilde{m}_1 = 1$ and $x_4 = \pm 1$. From the third factor

we get the equality $n_1 + x_2^2 = p$. Since $n_1 \equiv 2 \pmod 4$, $x_2^2 \equiv 0$ or $1 \pmod 4$ and p is odd, it follows that $p \equiv 3 \pmod 4$. The congruence of the factors implies $Q_1 = 1$, that is $3x_2^2 - n_1 = 1$.

Adding the equalities obtained from the third and first factors, we have the equation $(2x_2 - 1)(2x_2 + 1) = p$. It is possible if and only if $p = 3$, $x_2 = \pm 1$, since p is a prime number, and these also imply $n_1 = 2$. Hence, under the conditions $p = 3$, $m = -3$, $n = 6$, the solutions of the index form equation are $(x_2, x_3, x_4) = \pm(1, 0, 1), \pm(1, -1, 1), \pm(-1, 0, 1), \pm(-1, -1, 1)$.

(iii) $d(2x_3 + x_4)^2 = 1$ and $\widetilde{m}_1 x_4^2 = 3$

These equalities give $d = 1$, $2x_3 + x_4 = \pm 1$, $\widetilde{m}_1 = 3$ and $x_4 = \pm 1$. Then $n_1 + 3x_2^2 = p$ holds for Q_3. Similarly to case (ii), we get $p \equiv 1 \pmod 4$, hence $Q_1 = -1$, that is $x_2^2 - n_1 = -1$.

By solving the system of equations obtained from Q_1 and Q_3, we have $x_2 = \pm\frac{\sqrt{p-1}}{2}$ and $n_1 = \frac{p+3}{4}$. Then $p-1$ must be a square so that $x_2 \in \mathbb{Z}$. Since $n_1 \equiv 2 \pmod 4$, it follows that $p \equiv 5 \pmod{16}$. Furthermore, $n_1 = \frac{p+3}{4}$ is square-free. Then we have $m = -3$, $n = \frac{p+3}{4}$ and under these conditions, the solutions of the index form equation are $(x_2, x_3, x_4) = \pm(\frac{\sqrt{p-1}}{2}, 0, 1), \pm(\frac{\sqrt{p-1}}{2}, -1, 1), \pm(\frac{\sqrt{p-1}}{2}, 0, -1), \pm(\frac{\sqrt{p-1}}{2}, 1, -1)$.

(iv) $d(2x_3 + x_4)^2 = 0$ and $\widetilde{m}_1 x_4^2 = 4$

It is possible if and only if $2x_3 + x_4 = 0$, $\widetilde{m}_1 = 1$ and $x_4 = \pm 2$. Then from Q_3 we get $x_2^2 = p$, which has no integer solutions.

II. If $(Q_1, Q_2, Q_3) = (-1, p, 1)$, then $n_1(2x_3 + x_4)^2 + \widetilde{m}_1 x_2^2 = 1$ holds by the third factor. It is possible if and only if $n_1(2x_3 + x_4)^2 = 0$ and $\widetilde{m}_1 x_2^2 = 1$ because of the evenness of n_1.

Then $2x_3 + x_4 = 0$, $\widetilde{m}_1 = 1$ and $x_2 = \pm 1$. Hence, from Q_2 we have the equality $x_4^2 = 4p$, which has no integer solutions.

III. If $(Q_1, Q_2, Q_3) = (\pm p, 1, 1)$, considering Q_3, we have the equations $n_1(2x_3 + x_4)^2 = 0$ and $\widetilde{m}_1 x_2^2 = 1$. It means that $2x_3 + x_4 = 0$, $\widetilde{m}_1 = 1$ and $x_2 = \pm 1$. It follows from Q_2 that $x_4^2 = 4$, that is $x_4 = \pm 2$. Hence, $d - 4n_1 = \pm p$ must hold for Q_1.

If $p \equiv 1 \pmod 4$, then the congruence of the factors implies that $d - 4n_1 = -p$. By using Lemma 4.1, there exist infinitely many $c \in \mathbb{N}$ so that $(2c+1)(16c+8-p)$ is square-free and both of its factors are positive. Let $n_1 = 4c+2$ and $d = 16c+8-p$. Then $m = -(16c + 8 - p)$ and $n = (4c + 2)(16c + 8 - p)$ are distinct square-free integers and satisfy the above conditions and the conditions of Case 3/B, as well.

If $p \equiv 3 \pmod 4$, then the congruence of the factors implies that $d - 4n_1 = -p$. Similarly as above, there are infinitely many $c \in \mathbb{N}$ so that $(2c + 1)(16c + 8 + p)$ is square-free. By the choices $n_1 = 4c + 2$ and $d = 16c + 8 + p$, we get that there exist infinitely many m and n satisfying the conditions.

In both cases, the solutions are $(x_2, x_3, x_4) = \pm(1, -1, 2), \pm(1, 1, -2)$.

References

1. M.-L. Chang, Monogeneity in biquadratic fields, Int. J. Pure Appl. Math. 31, 481–490 (2006)
2. T. Funakura, On integral bases of pure quartic fields, Math. J. Okayama Univ. 26, 27–41 (1984)

3. I. Gaál, Diophantine Equations and Power Integral Bases, Birkhäuser (2002)
4. I. Gaál and B. Jadrijević, Determining elements of minimal index in an infinite family of totally real bicyclic biquadratic number fields, JP J. Algebra Number Theory Appl. 39, 307–326 (2017)
5. I. Gaál and G. Nyul, Index form equations in biquadratic fields: the p-adic case, Publ. Math. Debrecen 68, 225–242 (2006)
6. I. Gaál, A. Pethő and M. Pohst, On the indices of biquadratic number fields having Galois group V_4, Arch. Math. 57, 357–361 (1991)
7. 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, 100–114 (1995)
8. M.-N. Gras and F. Tanoé, Corps biquadratiques monogènes, Manuscripta Math. 86, 63–79 (1995)
9. K. Győry, Sur les polinômes à coefficients entiers et de discriminant donné III., Publ. Math. Debrecen 23, 141–165 (1976)
10. K. Győry, Discriminant Equations in Diophantine Number Theory, Cambridge University Press (2017)
11. B. Jadrijević, Establishing the minimal index in a parametric family of bicyclic biquadratic fields, Period. Math. Hungar. 58, 155–180 (2009)
12. B. Jadrijević, Solving index form equations in two parametric families of biquadratic fields, Math. Commun. 14, 341–363 (2009)
13. B. Jadrijević, On elements with index of the form 2^a3^b in a parametric family of biquadratic fields, Glas. Mat. 50, 43–63 (2015)
14. Y. Motoda, Notes on quartic fields, Rep. Fac. Sci. Engrg. Saga Univ. Math. 32, 1–19 (2003); 37, 1–8 (2008)
15. Y. Motoda, On integral bases of certain real monogenic biquadratic fields, Rep. Fac. Sci. Engrg. Saga Univ. Math. 33, 9–22 (2004)
16. Y. Motoda and T. Nakahara, Power integral bases in algebraic number fields whose Galois groups are 2-elementary abelian, Arch. Math. 83, 309–316 (2004)
17. Y. Motoda, T. Nakahara and K. H. Park, On power integral bases of the 2-elementary abelian extension fields, Trends Math. 9, 55–63 (2006)
18. T. Nagel, Zur Arithmetik der Polynome, Abh. Math. Sem. Univ. Hamburg 1, 179–194 (1922)
19. T. Nakahara, On the indices and integral bases of non-cyclic but abelian biquadratic fields, Arch. Math. 41, 504–508 (1983)
20. G. Nyul, Power integral bases in totally complex biquadratic number fields, Acta Acad. Paedagog. Agriensis Sect. Mat. 28, 79–86 (2001)
21. G. Nyul, Non-monogenity of multiquadratic number fields, Acta Math. Inform. Univ. Ostraviensis 10, 85–93 (2002)
22. G. Nyul, Monogenity of algebraic number fields (in Hungarian), PhD Thesis, University of Debrecen (2007)
23. A. Pethő and M. E. Pohst, On the indices of multiquadratic number fields, Acta Arith. 153, 393–414 (2012)
24. K. S. Williams, Integers of biquadratic fields, Canad. Math. Bull. 13, 519–526 (1970)