Acta Acad. Paed. Agriensis, Sectio Mathematicae **28** *(2001) 79–86*

POWER INTEGRAL BASES IN MIXED BIQUADRATIC NUMBER FIELDS

Gábor Nyul (Debrecen, Hungary)

Abstract. We give a complete characterization of power integral bases in quartic number fields of type $K = \mathbf{Q}(\sqrt{m}, \sqrt{n})$ where m, n are distinct square-free integers with opposite sign. We provide a list of all fields of this type up to discriminant 10^4 in increasing order of discriminants containing field indices, minimal indices and all elements of minimal index.

AMS Classification Number: 11D57, 11Y50

Keywords: quartic number fields, power integral bases

1. Introduction

Let K be an algebraic number field of degree n. The index of a primitive element $\alpha \in \mathbf{Z}_K$ is defined by

$$I(\alpha) = (\mathbf{Z}_K^+ : \mathbf{Z}[\alpha]^+).$$

The existence of *power integral bases* $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a classical problem of algebraic number theory. The element α generates a power integral basis if and only if $I(\alpha) = 1$ (for related results cf. [1]). If the number field K admits power integral bases, it is called *monogeneous*. We recall that the *minimal index* of a number field K is the minimum of the indices of all primitive integers in the field. The *field index* is the greatest common divisor of the indices of all primitive integers of the field.

Let m, n be distinct square-free integers. Biquadratic fields of type $K = \mathbf{Q}(\sqrt{m}, \sqrt{n})$ were considered by several authors. K. S. Williams [6] described an integral basis of K. T. Nakahara [5] proved that infinitely many fields of this type have power integral bases, on the other hand for any given N there are infinitely many fields of this type with field index 1 but minimal index $> N$, consequently without power integral basis.

M. N. Gras and F. Tanoe [4] gave necessary and sufficient conditions for biquadratic fields to have power integral basis. In fact they characterized all mixed biquadratic fields having power integral basis and established further necessary conditions for totally real biquadratic fields to have power integral basis. Using the integral bases I. Gaál, A. Pethő and M. Pohst [3] formulated the corresponding

index forms and gave an algorithm for determining all generators of power integral bases in the totally real case by solving systems of simultaneous Pellian equations.

To complete the above theory of power integral bases in biquadratic fields our purpose is to *describe all generators of power integral bases* in mixed biquadratic number fields. The most interesting point is that it turns out, that surprisingly the coordinate vectors (with respect to the integral basis of [6]) of the generators of power integral bases in mixed biquadratic number fields are contained in a finite set of *constant vectors* for all these fields. We also provide a table of mixed biquadratic fields in increasing order of discriminants up to 10^4 displaying the field index, minimal index and all elements of minimal index.

2. Index form equation in mixed biquadratic fields

To fix our notation we shortly recall the integral bases and corresponding index forms of biquadratic number fields with mixed signature.

Let m, n be distinct square-free rational integers (not equal to 1), let $l = (m, n) > 0$ and let m_1, n_1 be defined by $m = lm_1$, $n = ln_1$. By K. S. Williams' result [6] all mixed biquadratic number fields can be given in the form $\mathbf{Q}(\sqrt{m}, \sqrt{n})$ so that the parameters belong to one of the following cases:

Case 1:	$m > 0$,	$n < 0$,	$m \equiv 1 \pmod 4$,		$n \equiv 1 \pmod 4$,	
			$m_1 \equiv 1 \pmod 4$,		$n_1 \equiv 1 \pmod 4$.	
Case 2:	$m > 0$,	$n < 0$,	$m \equiv 1 \pmod 4$,		$n \equiv 1 \pmod 4$,	
			$m_1 \equiv 3 \pmod 4$,		$n_1 \equiv 3 \pmod 4$.	
Case 3/A:	$m > 0$,	$n < 0$,	$m \equiv 1 \pmod 4$,		$n \equiv 2 \pmod 4$.	
Case 3/B:	$m < 0$,	$n > 0$,	$m \equiv 1 \pmod 4$,		$n \equiv 2 \pmod 4$.	
Case 4/A:	$m > 0$,	$n < 0$,	$m \equiv 2 \pmod 4$,		$n \equiv 3 \pmod 4$.	
Case 4/B:	$m < 0$,	$n > 0$,	$m \equiv 2 \pmod 4$,		$n \equiv 3 \pmod 4$.	
Case 5/A:	$m > 0$,	$n < 0$,	$m \equiv 3 \pmod 4$,		$n \equiv 3 \pmod 4$.	
Case 5/B:	$m < 0$,	$n < 0$,	$m \equiv 3 \pmod 4$,		$n \equiv 3 \pmod 4$.	

and the integral bases are given by

Case 1: $\left\{1, \dfrac{1+\sqrt{m}}{2}, \dfrac{1+\sqrt{n}}{2}, \dfrac{1+\sqrt{m}+\sqrt{n}+\sqrt{m_1 n_1}}{4}\right\}$.

Case 2: $\left\{1, \dfrac{1+\sqrt{m}}{2}, \dfrac{1+\sqrt{n}}{2}, \dfrac{1-\sqrt{m}+\sqrt{n}+\sqrt{m_1 n_1}}{4}\right\}$.

Cases 3/A and 3/B: $\left\{1, \dfrac{1+\sqrt{m}}{2}, \sqrt{n}, \dfrac{\sqrt{n}+\sqrt{m_1 n_1}}{2}\right\}$.

Cases 4/A and 4/B: $\left\{1, \sqrt{m}, \sqrt{n}, \dfrac{\sqrt{m}+\sqrt{m_1 n_1}}{2}\right\}$.

Cases 5/A and 5/B: $\left\{1, \sqrt{m}, \dfrac{\sqrt{m}+\sqrt{n}}{2}, \dfrac{1+\sqrt{m_1 n_1}}{2}\right\}$.

The integral basis enables one to construct the corresponding index forms (cf. e.g. [2]):
Case 1:

$$\Big(l(x_2+\frac{x_4}{2})^2-\frac{n_1}{4}x_4^2\Big)\Big(l(x_3+\frac{x_4}{2})^2-\frac{m_1}{4}x_4^2\Big)\Big(n_1(x_3+\frac{x_4}{2})^2-m_1(x_2+\frac{x_4}{2})^2\Big).$$

Case 2:

$$\Big(l(x_2-\frac{x_4}{2})^2-\frac{n_1}{4}x_4^2\Big)\Big(l(x_3+\frac{x_4}{2})^2-\frac{m_1}{4}x_4^2\Big)\Big(n_1(x_3+\frac{x_4}{2})^2-m_1(x_2-\frac{x_4}{2})^2\Big).$$

Cases 3/A and 3/B:

$$\big(lx_2^2-n_1x_4^2\big)\Big(l(x_3+\frac{x_4}{2})^2-\frac{m_1}{4}x_4^2\Big)\big(n_1(2x_3+x_4)^2-m_1x_2^2\big).$$

Cases 4/A and 4/B:

$$\Big(\frac{l}{2}(2x_2+x_4)^2-\frac{n_1}{2}x_4^2\Big)\Big(2lx_3^2-\frac{m_1}{2}x_4^2\Big)\Big(2n_1x_3^2-\frac{m_1}{2}(2x_2+x_4)^2\Big).$$

Cases 5/A and 5/B:

$$\big(l(2x_2+x_3)^2-n_1x_4^2\big)\big(lx_3^2-m_1x_4^2\big)\Big(\frac{n_1}{4}x_3^2-m_1(x_2+\frac{x_3}{2})^2\Big).$$

As it is well-known (see e.g. [1]) $K=\mathbf{Q}(\sqrt{m},\sqrt{n})$ admits power integral bases if and only if the *index form equation*

$$I(x_2,x_3,x_4)=\pm1 \quad (\text{in } x_2,x_3,x_4\in\mathbf{Z}) \tag{1}$$

is solvable, where $I(x_2,x_3,x_4)$ is the index form given above. Moreover, all generators of power integral bases are of the form

$$\alpha=x_1+x_2\omega_2+x_3\omega_3+x_4\omega_4$$

where $\{1,\omega_2,\omega_3,\omega_4\}$ is the integral basis of K, (x_2,x_3,x_4) is a solution of the index form equation (1) and $x_1\in\mathbf{Z}$ is arbitrary.

Our main theorem characterizes the cases when K has power integral bases and describes all generators of power integral bases. M. N. Gras and F. Tanoe [4] has already described the monogeneous mixed biquadratic fields. Our main point is to show that the solutions of the index form equations in monogeneous mixed biquadratic fields belong to a *finite set of constant vectors*. Especially, the coordinates of the generators of power integral bases are explicitely given and *do not depend on the parameters* m,n,l.

Theorem. *Let $K = \mathbf{Q}(\sqrt{m}, \sqrt{n})$ be a mixed biquadratic number field represented in one of the forms listed above.*
In cases 1, 2 and 3/A there are no power integral bases.
In the other cases the necessary and sufficient condition of the existence of power integral bases in K is
Case 3/B: $m_1 = -1$, $l - 4n_1 = -1$ *(and by the assumption $n_1 > 0$).*
Case 4/A: $m_1 = 2$, $n_1 = -1$, $l = 1$, *so $m = 2$ and $n = -1$.*
Case 4/B: $m_1 = -2$, $l - n_1 = \pm 2$ *(and by the assumption $n_1 > 0$).*
Case 5/A: $n_1 = -1$, $4l - m_1 = 1$ *(and by the assumption $m_1 > 0$).*
Case 5/B: $l = 1$, $n_1 - m_1 = \pm 4$ *(and by the assumption $m_1, n_1 < 0$).*
The solutions of the index form equation corresponding to the above integral basis are

Case 3/B		$(x_2, x_3, x_4) = (1, 1, -2), (1, -1, 2),$
Case 4/A		$(x_2, x_3, x_4) = (0, 0, 1), (1, 0, -1),$
Case 4/B		$(x_2, x_3, x_4) = (0, 0, 1), (1, 0, -1),$
Case 5/A	$m = 3$, $n = -1$	$(x_2, x_3, x_4) = (1, -2, 1), (1, -2, -1),$
		$(0, 1, 0), (1, -1, 0),$
Case 5/A	*other fields*	$(x_2, x_3, x_4) = (1, -2, 1), (1, -2, -1),$
Case 5/B		$(x_2, x_3, x_4) = (0, 1, 0), (1, -1, 0).$

Note that if (x_2, x_3, x_4) is a solution then so also is $(-x_2, -x_3, -x_4)$ but we include only one of them.

Proof of the Theorem. In each case we solve equation (1) using the relevant index form. In each case the index form splits into three factors taking integer values, hence all factors must be equal to ± 1. We detail some tipical cases, the others are similar to deal with.

Case 1. We have $m_1 > 0$, $n_1 < 0$, $m_1 \equiv 1 \pmod 4$, $n_1 \equiv 1 \pmod 4$. Set $\widetilde{n}_1 = |n_1| > 0$.

The first factor of the index form is non-negative. Multiplying by 4 we get

$$l(2x_2 + x_4)^2 + \widetilde{n}_1 x_4^2 = 4.$$

On the left hand side both terms are non-negative integers, hence we have to consider the following five cases (a. to e.):

(a) $l(2x_2 + x_4)^2 = 0$, $\widetilde{n}_1 x_4^2 = 4$

By $l > 0$, we have $2x_2 + x_4 = 0$, that is $2 \mid x_4$. On the other hand $(\widetilde{n}_1, x_4^2) = (1, 4), (4, 1)$, and x_4 is even which imply $\widetilde{n}_1 = 1$, that is $n_1 = -1$. Then we obtain $n_1 \not\equiv 1 \pmod 4$, a contradiction, hence in case a there are no solutions.

(b) $l(2x_2 + x_4)^2 = 1$, $\widetilde{n}_1 x_4^2 = 3$

This is only possible if $l = 1$, $2x_2 + x_4 = \pm 1$, $\widetilde{n}_1 = 3$ (that is $n_1 = -3$) and $x_4^2 = 1$. If $x_4 = 1$, then $x_2 = 0$ or $x_2 = -1$; if $x_4 = -1$, then $x_2 = 0$ or $x_2 = 1$. Then the third factor of the index form is not positive, hence it is equal to -1:

If $x_2 = 0$, $x_4 = 1$ or $x_2 = -1$, $x_4 = 1$, then $-3\left(x_3 + \frac{1}{2}\right)^2 - \frac{m_1}{4} = -1$, that is $3(2x_3 + 1)^2 + m_1 = 4$. The first term is non-negative, not greater than 4, divisible by 3 and odd, hence it is equal to 3. Then $3(2x_3 + 1)^2 = 3$ and $m_1 = 1$, hence $2x_3 + 1 = \pm 1$, $x_3 = 0$ or $x_3 = -1$.

If $x_2 = 0$, $x_4 = -1$ or $x_2 = 1$, $x_4 = -1$, then $-3\left(x_3 - \frac{1}{2}\right)^2 - \frac{m_1}{4} = -1$, that is $3(2x_3 - 1)^2 + m_1 = 4$. Similarly as above it follows that the first term is 3 and $m_1 = 1$, $x_3 = 0$ or $x_3 = 1$.

The remaining cases are $(x_3, x_4) = (0, 1), (-1, 1), (0, -1), (1, -1)$. Considering the second factor we get $\frac{l}{4} - \frac{m_1}{4} = \pm 1$. On the other hand we have $l = m_1 = 1$, hence $\frac{l - m_1}{4} = 0$. It means that there are no solutions in case b, either.

The cases

(c) $l(2x_2 + x_4)^2 = 2$, $\widetilde{n}_1 x_4^2 = 2$,

(d) $l(2x_2 + x_4)^2 = 3$, $\widetilde{n}_1 x_4^2 = 1$,

(e) $l(2x_2 + x_4)^2 = 4$, $\widetilde{n}_1 x_4^2 = 0$

are much simpler to consider.

Hence in case 1 there are no power integral bases.

Cases 2, 3/A, 3/B are similar to consider.

Case 4/A. Now we have $m_1 > 0$, $n_1 < 0$. Let $\widetilde{n}_1 = |n_1| > 0$.

The third factor is non-positive, so multiplying by -2 we get

$$4\widetilde{n}_1 x_3^2 + m_1(2x_2 + x_4)^2 = 2.$$

The first term is non-negative, less than or equal to 2 and divisible by 4, hence only $4\widetilde{n}_1 x_3^2 = 0$ and $m_1(2x_2 + x_4)^2 = 2$ are possible. These imply $x_3 = 0$, $m_1 = 2$ and $2x_2 + x_4 = \pm 1$. Then the second factor is $-x_4^2 = -1$, that is $x_4 = \pm 1$. If $x_4 = 1$, then $x_2 = 0$ or $x_2 = -1$, and if $x_4 = -1$, then $x_2 = 0$ or $x_2 = 1$. The remaining cases are $(x_2, x_4) = (0, 1), (-1, 1), (0, -1), (1, -1)$. Considering the first factor we get $\frac{l}{2} - \frac{n_1}{2} = \pm 1$. But $l > 0$, $n_1 < 0$, so $\frac{l - n_1}{2} > 0$, hence $\frac{l - n_1}{2} = 1$, that is $l - n_1 = 2$. On the other hand, by $l, n_1 \in \mathbf{Z}$, we get $l \geq 1$, $n_1 \leq -1$, hence $l - n_1 \geq 2$. In this inequality the equation holds, so we have $l = 1$, $n_1 = -1$. Summarizing, in this case $l = 1$, $m_1 = 2$, $n_1 = -1$ and the solutions of the index form equation are $(x_2, x_3, x_4) = \pm(0, 0, 1), \pm(1, 0, -1)$.

Case 4/B. In this case $n_1 > 0$, $m_1 < 0$, and set $\widetilde{m}_1 = |m_1| > 0$.

Now the second factor is not negative, hence it is equal to 1. If we multiply it by 2, we get

$$4lx_3^2 + \widetilde{m}_1 x_4^2 = 2.$$

On the left hand side the first term is equal to 0, because it is non-negative, not greater than 2 and divisible by 4, which implies $4lx_3^2 = 0$, $\widetilde{m}_1 x_4^2 = 2$. From these we get $x_3 = 0$, $\widetilde{m}_1 = 2$ (that is $m_1 = -2$), $x_4 = \pm 1$. Then the third factor is $(2x_2 + x_4)^2 = 1$, hence $2x_2 + x_4 = \pm 1$. If $x_4 = 1$, then $x_2 = 0$ or $x_2 = -1$; if $x_4 = -1$, then $x_2 = 0$ or $x_2 = 1$. In the remaining cases $((x_2, x_4) = (0,1), (-1,1), (0,-1), (1,-1))$ the first factor is $\frac{l}{2} - \frac{n_1}{2} = \pm 1$, that is $l - n_1 = \pm 2$. Summarizing, we get $m_1 = -2$, $l - n_1 = \pm 2$ and the solutions of the index form equation in this case are $(x_2, x_3, x_4) = \pm(0,0,1), \pm(1,0,-1)$.

Cases 5/A, 5/B can be discussed in a similar way.

In each case it is simple to verify by substitution that the triples (x_2, x_3, x_4) obtained above are indeed solutions of the index form equation.

3. Description of the table

We present a list of all mixed biquadratic fields up to discriminant 10^4. In this table D_K, m_K, μ denote the discriminant, the field index and the minimal index, respectively. They are followed by the solutions of $I(x_2, x_3, x_4) = \pm\mu$, that is the coordinates of the elements of minimal index. If (x_2, x_3, x_4) is a solution then so also is $(-x_2, -x_3, -x_4)$ but we list only one of them. To construct the table we used [6] (integral basis, D_K), [2] (to calculate m_K). In order to determine the minimal index μ we took the multiplies $k \cdot m_K$ of m_K until the index form equation with right hand side $\pm k \cdot m_K$ had solutions. In [3] the authors provided a similar list of totally real biquadratic fields. These computations were performed in MAPLE and took just a few minutes.

D_K	m_1	n_1	l	m_K	μ	(x_2, x_3, x_4)
144	3	-1	1	1	1	(1, -2, 1), (1, -1, 0), (0, 1, 0), (1, -2, -1)
225	-3	5	1	2	2	(0, 1, -1), (0, 0, 1), (1, 0, -1), (1, 1, -1)
256	2	-1	1	1	1	(0, 0, 1), (1, 0, -1)
400	-1	-5	1	1	1	(0, 1, 0), (1, -1, 0)
441	-1	7	3	2	2	(0, 1, -1), (1, 0, 1), (1, -1, 1), (0, 0, 1)
576	-3	2	1	1	4	(0, 1, -1), (0, 0, 1)
576	-1	2	3	1	3	(1, 1, -1), (1, 0, -1), (1, 0, 1), (1, -1, 1)
784	7	-1	1	1	2	(1, -1, 0), (0, 1, 0)
1089	-1	11	3	2	4	(3, -1, 2), (1, 1, -2)
1225	-7	5	1	2	6	(0, 1, -1), (1, 1, -1), (1, 0, -1), (0, 0, 1)
1521	-3	13	1	2	10	(2, 1, -1), (2, 0, -1), (1, 0, 1), (1, -1, 1)
1600	5	-2	1	1	4	(0, 1, -1), (0, 0, 1)
1600	1	-2	5	1	4	(0, 1, -1), (0, 0, 1)
1936	11	-1	1	1	3	(1, -1, 0), (0, 1, 0)
2304	6	-1	1	1	5	(0, 1, -1), (0, 1, 1), (1, -1, -1), (1, 1, -1)
2304	-2	3	1	1	1	(1, 0, -1), (0, 0, 1)
2601	-3	17	1	2	20	(0, 1, -1), (1, -1, 0), (1, 1, 0), (1, 0, -1), (1, 1, -1), (0, 0, 1)
2704	-1	-13	1	1	3	(0, 1, 0), (1, -1, 0)
3025	-11	5	1	2	12	(0, 0, 1), (0, 1, -1), (1, 1, -1), (1, 0, -1)
3136	-7	2	1	1	8	(0, 1, -1), (0, 0, 1)
3136	-1	2	7	1	1	(1, -1, 2), (1, 1, -2)
3249	-1	19	3	2	14	(1, 0, -1), (2, -1, 1), (1, 1, -1), (2, 0, 1)
3600	15	-1	1	1	4	(1, -1, 0), (0, 1, 0), (2, -4, 1), (2, -4, -1)
3600	3	-5	1	1	2	(1, -1, 0), (0, 1, 0)
3600	3	-1	5	1	12	(0, 1, -1), (1, -1, 1), (0, 1, 1), (1, -1, -1)
4624	-1	-17	1	1	4	(0, 1, 0), (1, -1, 0)
4761	-1	23	3	2	8	(2, -1, 1), (1, 0, -1), (2, 0, 1), (1, 1, -1)
5776	19	-1	1	1	5	(1, -1, 0), (0, 1, 0)
5929	-1	11	7	2	4	(2, -1, 2), (0, 1, -2)
6400	10	-1	1	1	21	(0, 1, -1), (1, 1, -1), (1, -1, -1), (0, 1, 1)
6400	2	-5	1	1	3	(1, 0, -1), (0, 0, 1)
6400	2	-1	5	3	3	(1, 0, -1), (0, 0, 1)
7056	1	-7	3	1	18	(1, -1, 0), (0, 1, 0)
7056	1	-3	7	1	31	(1, 0, -1), (1, 0, 1)
7056	-1	-21	1	1	5	(0, 1, 0), (1, -1, 0)
7569	-3	29	1	2	26	(3, 1, -1), (2, -1, 1), (3, 0, -1), (2, 0, 1)
7744	-11	2	1	1	12	(0, 0, 1), (0, 1, -1)
7744	-1	2	11	3	3	(1, -1, 2), (1, 1, -2)
8281	-7	13	1	2	20	(1, 1, 0), (1, -1, 0)
8464	23	-1	1	1	6	(1, -1, 0), (0, 1, 0)
8649	-1	31	3	2	10	(2, -1, 1), (2, 0, 1), (1, 0, -1), (1, 1, -1)
9025	-19	5	1	2	24	(1, 1, 0), (1, -1, 0)

References

[1] Gaál, I., Power integer bases in algebraic number fields, *Annales Univ. Sci. Budapest Sect. Comp.*, **18** (1999), 61–87.

[2] Gaál, I., Pethő, A. and Pohst, M., On the indices of biquadratic number fields having Galois group V_4, *Arch. Math.*, **57** (1991), 357–361.

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

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

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

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

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