Power integral bases in parametric families of biquadratic fields

István Gaál * and Tímea Szabó
University of Debrecen, Mathematical Institute
H–4010 Debrecen Pf.12., Hungary
e–mail: igaal@science.unideb.hu, timi.taylor168@gmail.com

14th September 2011

Abstract

We consider two families of totally complex biquadratic fields depending on two parameters. These families were recently considered by J.G.Huard, B.K.Spearman and K.S.Williams [8]. Using our general method [4] and the integral basis described by [8] we solve the index form equations in a parametric form in these families and prove that (up to equivalence) they admit only one generator of power integral bases. Note that these are the first families of number fields with *two parameters* where all generators of power integral bases are determined.

*Research supported in part by K67580 and K75566 from the Hungarian National Foundation for Scientific Research and by the TAMOP 4.2.1./B-09/1/KONV-2010-0007 project implemented through the New Hungary Development Plan co-financed by the European Social Fund, and the European Regional Development Fund

2010 *Mathematics Subject Classification*: Primar 11R16; Secondary 11D59, 11Y50

Key words and phrases: biquadratic fields, power integral bases

1 Introduction

It is an essential question in algebraic number theory to decide if a number field K is *monogene*, that is if it admits a *power integral basis* of the form $\{1, \alpha, \ldots, \alpha^{n-1}\}$. It is well known that up to equivalence (translation by numbers of $\mathbb{Z}$) there are only finitely many generators of power integral bases in each number field.

There is an extensive literature of algorithms to deteremine all generators of power integral bases in specific number fields (cf. [2]). Determining the generators of power integral bases is equivalent to solving the corresponding *index form equation* (see [2]).

It is a delicate problem to consider the same problem in infinite parametric families of number fields, when we are faced to solving the index form equation in a parametric form. This was however succesfully done for certain families of number fields E.Thomas [10], I.Gaál [1], I.Gaál and M.Pohst [7], etc.

Note that using the integral basis given by K.S.Williams [11] we could construct the index from equation in quartic fields of type $\mathbb{Q}(\sqrt{a}, \sqrt{b})$. This made possible to describe completely the field indices of these fields [3] and give a general method to solve index form equations in such fields [5]. In the totally complex case G.Nyul [9] could characterize all quartic fields of type $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ that are monogene, explicitely giving all generators of power integral bases, as well.

J.G.Huard, B.K.Spearman and K.S.Williams [8] recently gave explicitely the integral bases in biquadratic number fields of type $\mathbb{Q}(\sqrt{a + b\sqrt{c}})$. Using this we will consider the field indices and monogenity of such fields in a separately paper.

In their paper J.G.Huard, B.K.Spearman and K.S.Williams [8] also considered two infinite parametric families of fields of type $\mathbb{Q}(\sqrt{a + b\sqrt{c}})$ involving two parameters. The authors proved that these families admit power integral bases.

In our paper *we solve completely the index form equation in these parametric families of biquadratic fields* and show that all power integral bases are those given in [8]. This is the first time that the index form equation is solved completely in infinite parametric families of number fields, involving *two parameters*.

Note that using the integral bases in [8] our method makes possible to solve the index form equation in any totally complex quartic field of type

$\mathbb{Q}(\sqrt{a+b\sqrt{c}})$. Since by [8] there is a huge number of cases to consider, this will be done separately.

2 Parametric families of totally complex bi-quadratic fields

Let $c<0$ be an integer and for positive integers k set

$$f_c(k)=16k^2+24k+(9-4c),\ a_k=4k+3,\ b_k=2 \text{ for } c\equiv 1\ (\mathrm{mod}4)$$

$$f_c(k)=4k^2+4(c+1)k+(c^2+c+1),\ a_k=2k+c+1,\ b_k=1 \text{ for } c\equiv 2,3\ (\mathrm{mod}\ 4)$$

Following the arguments of [8] we conclude that for each c, $f_c(k)$ is square-free for infinitely many k. We denote by S the set of pairs (c,k) with $c<-3$, $k>|c|$ and $f_c(k)$ square-free. Obviously, S is an infinite set. Further, for each c we have $f_c(k)=a_k^2-cb_k^2$ greater than c, hence $L_{c,k}=\mathbb{Q}(\sqrt{a_k+b_k\sqrt{c}})$ is a quartic extension of $\mathbb{Q}$. $L_{c,k}$ contains the complex quadratic field $\mathbb{Q}(\sqrt{c})$ hence it is a totally complex quartic field.

We prove:

Theorem 1. *Let $c\equiv 1\ (\mathrm{mod}4)$. Then for all $(c,k)\in S$ up to equivalence the only power integral basis in $L_{c,k}$ is generated by*

$$\vartheta=\frac{1}{2}\left(1+\sqrt{a_k+2\sqrt{c}}\right).$$

Theorem 2. *Let $c\equiv 2,3\ (\mathrm{mod}4)$. Then for all $(c,k)\in S$ up to equivalence the only power integral basis in $L_{c,k}$ is generated by*

$$\vartheta=\sqrt{a_k+\sqrt{c}}.$$

J.G.Huard, B.K.Spearman and K.S.Williams [8] showed that the above elements generate power integral bases. We completely solve the index form equation and prove that up to equivalence there are no other generators of power integral bases.

3 Auxiliary results

We showed [4] (see also [2]) that the index form equation in quartic fields (having three variables and degree 6) can be reduced to a cubic Thue equation and a corresponding system of equations with quadratic forms in three variables. We formulate this result for the order $\mathbb{Z}[\xi]$ since in our application this is just the full ring of integers of the number field.

Let $K = \mathbb{Q}(\xi)$ be a quartic number field and $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 \in \mathbb{Z}[x]$ the minimal polynomial of ξ.

Lemma 3. *The element $\alpha = a + x\xi + y\xi^2 + z\xi^3 \in \mathbb{Z}[\xi]$ (with $a, x, y, z \in \mathbb{Z}$) generates a power integral basis in $\mathbb{Z}[\xi]$ if and only if there is a solution $(u, v) \in \mathbb{Z}^2$ of the cubic equation*

$$F(u, v) = u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3 = \pm 1 \quad (1)$$

such that (x, y, z) satisfies

$$\begin{aligned} Q_1(x, y, z) &= x^2 - xya_1 + y^2a_2 + xz(a_1^2 - 2a_2) + yz(a_3 - a_1a_2) \\ &\quad + z^2(-a_1a_3 + a_2^2 + a_4) = u \ , \\ Q_2(x, y, z) &= y^2 - xz - a_1yz + z^2a_2 = v \quad . \end{aligned} \quad (2)$$

In [6] (see also [2]) we gave a general method for solving the system of equations with quadratic forms (2). We showd that it can be reduced to some quartic Thue equations. On the other hand, for totally complex quartic fields the resolution of this system of equations (2) can be made easy by constructing a positive definite quadratic form (cf. [4], [2]).

Lemma 4. *Let K be a totally complex quartic field. Then the polynomial $R(x) = F(x, 1)$ has three distinct real roots, $\lambda_1 < \lambda_2 < \lambda_3$. The form $T_\lambda(x, y, z) = Q_1(x, y, z) + \lambda \cdot Q_2(x, y, z)$ is positive definite if and only if $\lambda \in (-\lambda_2, -\lambda_1)$.*

4 Proof of Theorem 1

I. We have $a_k = 4k + 3, b_k = 2$ and set $c = 4\ell + 1 < -3$ ($\ell < -1$). The defining polynomial of ϑ is

$$f(x) = x^4 - 2x^3 - 2kx^2 + (2k + 1)x + k^2 + k - \ell.$$

Using the notation of Lemma 3 we have $a_1 = -2, a_2 = -2k, a_3 = 2k+1, a_4 = k^2 + k - \ell$. Equation (1) is of the form

$$F(u,v) = (u + (2k+1)v)(u^2 - uv - v^2(4k^2 + 6k + 1 - 4\ell)) = \pm 1$$

whence we obtain the system of equations

$$\begin{aligned} u + (2k+1)v &= i_1 \\ u^2 - uv - v^2(4k^2 + 6k + 1 - 4\ell) &= i_2 \end{aligned}$$

with $i_1, i_2 = \pm 1$. We express u from the first equation and insert it into the second equation. Then we obtain a second degree eguation for v.

For $i_1 = i_2 = 1$ we become

$$v = \frac{a_k \pm \sqrt{a_k^2 - 8c}}{2c}.$$

In this formula $a_k^2 < a_k^2 - 8c < (a_k + 1)^2$ because of $k > |\ell|$, hence we do not become integer value for v.

For $i_1 = 1, i_2 = -1$ we obtain the possible solutions $v = 0$ and $v = a_k/c$ if this is integer. We obtain $(u,v) = (\pm 1, 0), (-(2k+1)a_k/c + 1, a_k/c)$.

For $i_1 = -1, i_2 = 1$ the expression under the square root cannot be a square, similarly as for $i_1 = i_2 = 1$.

For $i_1 = i_2 = -1$ we obtain the possible solutions $v = 0$ and $v = -a_k/c$ if this is integer. We obtain $(u,v) = (\pm 1, 0), ((2k+1)a_k/c - 1, -a_k/c)$.

II. Next we calculate the roots of $R(x) = F(x,1)$. We obtain

$$\begin{aligned} x_1 &= \frac{1}{2}(1 - a_k) = -2k - 1 \\ x_2 &= \frac{1}{2}\left(1 + \sqrt{a_k^2 - 4c}\right) = 2k + 2 + \rho_2 \\ x_3 &= \frac{1}{2}\left(1 - \sqrt{a_k^2 - 4c}\right) = -2k - 1 - \rho_3 \end{aligned}$$

where ρ_2, ρ_3 are positive numbers, since $c < 0$. Therefore we have

$$\lambda_1 = x_3 < \lambda_2 = x_1 < \lambda_3 = x_2.$$

III. For $a_1 = -2, a_2 = -2k, a_3 = 2k+1, a_4 = k^2 + k - \ell$ the quadratic forms involved in Lemma 3 are

$$\begin{aligned} Q_1(x,y,z) &= x^2 + 2xy - 2y^2k + xz(4 + 4k) + yz(-2k + 1) + z^2(5k + 2 + 5k^2 - \ell), \\ Q_2(x,y,z) &= y^2 - xz + 2yz - 2z^2k. \end{aligned}$$

To construct a positive definite quadratic form we should take a $\lambda \in (-\lambda_2, -\lambda_1) = (-x_1, -x_3) = (2k+1, 2k+1+\rho_3)$. Therefore we can take $\lambda = 2k+1+\varepsilon$ with an arbitrary small positive ε. We obtain

$$Q_1(x,y,z) + \lambda Q_2(x,y,z) = u + \lambda v$$

that is

$$\left(x+y+z\left(\frac{3}{2}+k-\frac{\varepsilon}{2}\right)\right)^2+\varepsilon\left(y+\frac{3z}{2}\right)^2+z^2\left(-\ell-\frac{1}{4}-\varepsilon k-\frac{3\varepsilon}{4}-\frac{\varepsilon^2}{4}\right)=u+\lambda v \tag{3}$$

where $u+\lambda v$ is either 1 or $1+\varepsilon a_k/c$ or $-1-\varepsilon a_k/c$, the last being impossible for sufficiently small ε.

IV.1. If $u+\lambda v = 1$ then by $\ell < -1$ for sufficiently small ε the coefficient of z^2 in (3) is greater than 1, hence we obtain $z=0$ and (3) implies

$$(x+y)^2 + \varepsilon y^2 = 1.$$

For a small value of ε the left hand side is only integer for $y=0$, hence $x = \pm 1$.

IV.2. If $u+\lambda v = 1+\varepsilon a_k/c$ then by $\ell < -1$ we obtain for sufficiently small ε that $0.9 < 1+\varepsilon a_k/c < 1$. The coefficient of z^2 in (3) is greater than 1, hence we obtain $z=0$. Equation (3) implies

$$(x+y)^2 + \varepsilon y^2 = 1 + \varepsilon a_k/c$$

that is

$$(x+y)^2 - 1 = \varepsilon\left(\frac{a_k}{c} - y^2\right).$$

We have $\varepsilon > 0$,$a_k/c < 0$ and $-y^2 \le 0$ hence the right hand side is negativ. This can only happen with the left hand side if $x+y=0$. The we obtain

$$\varepsilon\left(y^2 - \frac{a_k}{c}\right) = 1$$

which is impossible e.g. if ε is irrational.

Therefore only ϑ generates a power integral basis. $\square$

5 Proof of Theorem 2

I. The proof of our Theorem 2 is similar to Theorem 1. In this case we have $a_k = 2k + c + 1, b_k = 1$ and $c \equiv 2, 3 \pmod 4$. The element ϑ is defined by the polynomial

$$f(x) = x^4 - 2a_k x^2 + a_k^2 - c.$$

By Lemma 3 we have now $a_1 = 0, a_2 = -2a_k, a_3 = 0, a_4 = a_k^2 - c$. The cubic equation (1) gets the form

$$F(u, v) = (u + 2a_k v)(u^2 + 4v^2(c - a_k^2)) = \pm 1$$

which implies the system of equations

$$\begin{aligned} u + 2a_k v &= i_1 \\ u^2 + 4v^2(c - a_k^2) &= i_2 \end{aligned}$$

with $i_1, i_2 = \pm 1$. Substituting u from the first equation into the second equation we become a quadratic equation for v.

For $i_1 = i_2 = 1$ we obtain the possible solutions $v = 0$ and $v = -a_k/c$. If $c \equiv 2 \pmod 4$ then a_k is odd, if $c \equiv 3 \pmod 4$ then a_k is even, hence $v = -a_k/c$ is not an integer.

For $i_1 = -1, i_2 = 1$ we obtain the possible solutions $v = 0$ and $v = a_k/c$, the later is not possible similarly as for $i_1 = i_2 = 1$.

For $i_1 = 1, i_2 = -1$ and $i_1 = i_2 = -1$ there are no solutions because of the congruence condition.

Hence we only obtain $(u, v) = (1, 0)$.

II. Next we calculate the roots of $R(x) = F(x, 1)$. We obtain

$$\begin{aligned} x_1 &= -2a_k \\ x_2 &= -2\sqrt{a_k^2 - c} = -2a_k - \rho_2 \\ x_3 &= 2\sqrt{a_k^2 - c} = 2a_k + \rho_3 \end{aligned}$$

where ρ_2, ρ_3 are positive numbers, since $c < 0$. Therefore we have

$$\lambda_1 = x_2 < \lambda_2 = x_1 < \lambda_3 = x_3.$$

III. For $a_1 = 0, a_2 = -2a_k, a_3 = 0, a_4 = a_k^2 - c$ the quadratic forms involved in Lemma 3 are

$$\begin{aligned} Q_1(x, y, z) &= x^2 - 2y^2 a_k + 4xza_k + z^2(5a_k^2 - c), \\ Q_2(x, y, z) &= y^2 - xz - 2z^2 a_k. \end{aligned}$$

To construct a positive definite quadratic form we should take a $\lambda \in (-\lambda_2, -\lambda_1) = (-x_1, -x_2) = (2a_k, 2a_k + \rho_2)$. We again take $\lambda = 2a_k + \varepsilon$ with an arbitrary small positive ε. Hence

$$Q_1(x, y, z) + \lambda Q_2(x, y, z) = u + \lambda v$$

that is

$$\left(x + z\left(a_k - \frac{\varepsilon}{2}\right)\right)^2 + \varepsilon y^2 + z^2\left(-c - \varepsilon a_k - \frac{\varepsilon^2}{4}\right) = u + \lambda v \qquad (4)$$

where $u + \lambda v$ is 1.

IV. If $u + \lambda v = 1$ then by $c < 0$ the coefficient of z^2 in (4) is greater than 1 for sufficiently small ε, hence we obtain $z = 0$ and (4) implies

$$x^2 + \varepsilon y^2 = 1.$$

For a small value of ε the left hand side is only integer for $y = 0$, hence $x = \pm 1$.

Therefore ϑ is the only generator of a power integral bases. □

References

[1] I.Gaál, *Power integral bases in orders of families of quartic fields*, Publ. Math. (Debrecen), **42** (1993), 253–263.

[2] I.Gaál, Diophantine Equations and Power Integral Bases, Birkhäuser Boston, 2002.

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

[4] I.Gaál, A.Pethő and M.Pohst, *On the resolution of index form equations in quartic number fields*, J. Symbolic Comput., **16** (1993), 563–584.

[5] 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.

[6] I.Gaál, A.Pethő and M.Pohst, *Simultaneous representation of integers by a pair of ternary quadratic forms – with an application to index form equations in quartic number fields*, J.Number Theory, **57**(1996), 90–104.

[7] I.Gaál and M.Pohst, *Power integral bases in a parametric family of totally real quintics*, Math. Comput., **66**(1997), 1689–1696.

[8] J.G.Huard, B.K.Spearman and K.S.Williams, *Integral bases for quartic fields with quadratic subfields*, J. Number Theory **51**(1995), 87–102.

[9] G.Nyul, *Power integral bases in mixed biquadratic number fields*, Acta Acad. Paed. Agriensis, Sect. Math. **28**(2001) 79–86

[10] E.Thomas, *Complete solutions to a family of cubic diophantine equations*, J.Number Theory, **34**(1990), 235250.

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