Relative power integral bases in infinite families of quartic extensions of quadratic 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

January 21, 2013

Abstract

We consider infinite parametric families of octic fields, that are quartic extensions of quadratic fields. We describe all relative power integral bases of the octic fields over the quadratic subfields.

1 Introduction

Let K be an algebraic number field of degree n with ring of integers $\mathcal{O} = \mathbb{Z}_K$. The index of $\alpha \in \mathcal{O}$ (assumed α is a primitive element that is $K = \mathbb{Q}(\alpha)$) is defined by

$$I(\alpha) = (\mathcal{O}^+ : \mathbb{Z}[\alpha]^+)$$

*Research supported in part by K75566 and K100339 from the Hungarian National Foundation for Scientific Research

2010 *Mathematics Subject Classification*: Primary 11R33; Secondary 11D25,11Y50

Key words and phrases: power integral basis, monogenity, relative extensions

that is the index of the additive group of $\mathbb{Z}[\alpha]$ in the additive group of $\mathcal{O}$. The ring $\mathcal{O}$ is called *monogenic* if it is generated by a single element ϑ over $\mathbb{Z}$, that is $\mathcal{O} = \mathbb{Z}[\vartheta]$. In this case the index of ϑ, is equal to 1 and obviously $1, \vartheta, \ldots, \vartheta^{n-1}$ is an integral basis of $\mathcal{O}$ called *power integral basis*.

There is an extensive literature of monogenic number fields (cf. [2]) involving also algorithms for determining all possible generators of power integral bases. We also succeeded to determine all possible generators of power integral bases also in some infinite parametric families of number fields, see [7], [4].

The index and the notion of power integral basis was extended also to the *relative case*, for relative extensions of number fields. Relative cubic extensions were considered by I.Gaál and M.Pohst [3] and relative quartic extensions by I.Gaál and M.Pohst [8] (cf. also [2]).

Let M be a number field and K an extension field of M of relative degree n. Denote the rings of integers of M and K by $\mathbb{Z}_M$ and $\mathcal{O} = \mathbb{Z}_K$, respectively. If $\alpha \in \mathcal{O}$ is a primitive element of K over M (that is $K = M(\alpha)$), then the *relative index* of α over M is defined by

$$I_{K/M}(\alpha) = (\mathcal{O}^+ : \mathbb{Z}_M[\alpha]^+),$$

that is the index of the additive group of $\mathbb{Z}_M[\alpha]$ in the additive group of $\mathcal{O}$. The relative index is equal to 1 if and only if $1, \alpha, \ldots, \alpha^{n-1}$ is a *relative power integral basis* of $\mathcal{O}$ over $\mathbb{Z}_M$.

The method of [8] to determine relative power integral bases in quartic relative extensions was a direct generalization of our method [6] for quartic fields, however its application is much more complicated technically.

2 Results

We are going to consider three infinite parametric families of octic fields $K = M(\xi)$ over their quadratic subfield M. Our purpose is to describe the relative power integral bases of either $\mathcal{O} = \mathbb{Z}_K$ over $\mathbb{Z}_M$ (if the integer basis of K is known in a parametric form) or of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$ (otherwise). Note that in the later case ξ itself is a generator of a power integral basis but it is important to ask if there exist any other generators of power integral bases.

The elements of $\mathcal{O}$ that only differ by unit factors and by translation by elements of $\mathbb{Z}_M$ are called *equivalent*. Equivalent elements have the same relative indices. There are only finitely many non-equivalent generators of relative power integral bases. We intend to determine all generators of power integral bases up to equivalence.

3 Results

We shall consider three infinite families of relative quartic extensions over quadratic fields.

I. Let $D > 0$ be a square-free integer, $M = \mathbb{Q}(\sqrt{-D})$, $t \in \mathbb{Z}_M$ a parameter and let ξ be a root of

$$f(x) = x^4 - t^2x^2 + 1 \in \mathbb{Z}_M[x]. \tag{1}$$

Let $K = M(\xi)$ and consider the relative power integral bases of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$.

Theorem 1. *For* $|t| > 245$ *all non-equivalent generators of power integral bases of* $\mathcal{O}$ *over* $\mathbb{Z}_M$ *are given by*

$$\alpha = \xi, -t^2\xi+\xi^3, (1-t^4)\xi+t\xi^2+t^2\xi^3, (1-t^4)\xi-t\xi^2+t^2\xi^3, t\xi^2+\xi^3, -t\xi^2+\xi^3.$$

Moreover for $D = -3$ *we also have*

$$\alpha = (1-\omega_3^2 t)\xi + \omega_3\xi^2 + \omega_3^2\xi^3$$

with $\omega_3 = (1+i\sqrt{3})/2$.

II. Let $D > 0$ be a square-free integer, $M = \mathbb{Q}(\sqrt{-D})$, $t \in \mathbb{Z}_M$ a parameter and let ξ be a root of

$$f(x) = x^4 - 4tx^3 + (6t+2)x^2 + 4tx + 1 \in \mathbb{Z}_M[x]. \tag{2}$$

Let $K = M(\xi)$ and consider the relative power integral bases of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$.

Theorem 2. *For $|t| > 1544803$ all non-equivalent generators of power integral bases of $\mathcal{O}$ over $\mathbb{Z}_M$ are given by*

$$\alpha = \xi, (6t+2)\xi - 4t\xi^2 + \xi^3.$$

Note that the arguments to prove the above two theorems apply results on the solutions of parametric relative Thue equations that were only proved for large parameters. This makes necessary the assumptions on the parameters.

III. Let $M = \mathbb{Q}(i)$, and let $t \in \mathbb{Z}_M$ be a parameter such that the polynomial

$$f(x) = x^4 - itx^2 + 1 \in \mathbb{Z}_M[x] \tag{3}$$

is irreducible over M. Denote by ξ a root of $f(x)$.

For this family of relative quartic extensions we shall separately consider the Gaussian integer ($t \in \mathbb{Z}_M$) and rational integer ($t \in \mathbb{Z}$) parameters. The reason is that if $t \in \mathbb{N}$ and $t^2 + 4$ is square free, then the integral basis of K is known by B.K.Spearman and K.S.Williams [11].

First consider Gaussian integer parameters. Let $t \in \mathbb{Z}_M \backslash \mathbb{Z}$ be a parameter such that $f(x)$ is irreducible over M. Let $K = M(\xi)$, set $\mathcal{O} = \mathbb{Z}_M[\xi]$ and consider the relative power integral bases of $\mathcal{O}$ over $\mathbb{Z}_M$.

Theorem 3. *For the above parameters $t \in \mathbb{Z}_M \setminus \mathbb{Z}$ with $|t| < 50$ all non-equivalent generators*

$$\alpha = x\xi + y\xi^2 + z\xi^3$$

of power integral bases of $\mathcal{O}$ over $\mathbb{Z}_M$, with $x, y, z \in \mathbb{Z}_M$, $\max(|x|, |y|, |z|) \leq 30$ are given by

$$\alpha = \xi, -it\xi + \xi^3.$$

Next consider rational integer parameters. By the results of B.K.Spearman and K.S.Williams [11] for $t \in \mathbb{N}$, $t^2 + 4$ square free the polynomial $f(x)$ is irreducible over M and if ξ is a root of $f(x)$, $K = M(\xi)$ then ξ itself generates power integral basis over M. Therefore we take $\mathcal{O} = \mathbb{Z}_K$ and consider the relative power integral bases of $\mathcal{O}$ over $\mathbb{Z}_M$.

Theorem 4. *For $t \in \mathbb{N}$, t^2+4 square free, $t \leq 100$, all non-equivalent generators*

$$\alpha = x\xi + y\xi^2 + z\xi^3$$

of power integral bases of $\mathcal{O}$ over $\mathbb{Z}_M$, with $x, y, z \in \mathbb{Z}_M$, $\max(|x|, |y|, |z|) \leq 30$ *are given by*

$$\alpha = \xi, -it\xi + \xi^3.$$

Moreover, for $t = 1$ the following elements and their equivalents also generate power integral bases of $\mathcal{O}$ over $\mathbb{Z}_M$:

$$\alpha = 3\xi+(1+i)\xi^2+2i\xi^3, 3\xi-(1+i)\xi^2+2i\xi^3, i\xi+(1+i)\xi^2+\xi^3, i\xi-(1+i)\xi^2+\xi^3.$$

In the last two theorems we made direct calculation for the solutions of the relative Thue equations involved. The solutions in general are not known, that is why we only have results for small parameters.

4 Preliminaries

Our main tool throughout will be the application the method of [8] that we detail here. This reduces the relative index form equation to a relative cubic equation (Thue equation if irreducible) and some relative quartic Thue equations. In our three families the cubic equation will be reducible. To solve the quartic Thue equations we shall apply results on infinite parametric families of relative Thue equations.

Let K be a quartic extension of the number field M of degree m, generated by a root ξ with relative minimal polynomial $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 \in \mathbb{Z}_M[x]$. Let $\mathcal{O}$ be either $\mathbb{Z}_K$ or $\mathbb{Z}_M[\xi]$. We represent any $\alpha \in \mathcal{O}$ in the form

$$\alpha = \frac{1}{d}\left(a + x\xi + y\xi^2 + z\xi^3\right) \qquad (4)$$

with coefficients $x, y, z \in \mathbb{Z}_M$ $(1 \leq i \leq 4)$ and with a common denominator $d \in \mathbb{Z}$. Let $i_0 = I_{K/M}(\xi) = (\mathcal{O}^+ : \mathbb{Z}_M[\xi]^+)$,

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

a binary cubic form over $\mathbb{Z}_M$ and

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

ternary quadratic forms over $\mathbb{Z}_M$.

Lemma 5. *([8]) If α of (4) satisfies*

$$I_{K/M}(\alpha) = 1,$$

then there is a solution $(u, v) \in \mathbb{Z}_M$ of

$$N_{M/\mathbb{Q}}(F(u, v)) = \pm \frac{d^{6m}}{i_0} \tag{5}$$

such that

$$\begin{aligned} u &= Q_1(x, y, z), \\ v &= Q_2(x, y, z). \end{aligned} \tag{6}$$

For a given solution u, v of (5) we have to solve the system of equations (6). For this purpose we use a method of L.J.Mordell [10] to parametrize the solutions of the quadratic form equation $Q_0(x, y, z) = uQ_2(x, y, z) - vQ_1(x, y, z) = 0$ which is also explained in general in [8]. These detailes will be completely described in our proofs.

5 Proofs

5.1 Proof of Theorem 1

In our Lemma we substitute $a_1 = 0, a_2 = -t^2, a_3 = 0, a_4 = 1$. Equation (5) is of the form

$$F(u, v) = (u - 2v)(u + 2v)(u + t^2 v) = \varepsilon$$

where ε is a unit in M. Therefore all factors of $F(u, v)$ must also be units in M which implies $v = 0$ and u a unit in M. The equation $Q_0 = 0$ implies $Q_2 = 0$, that is

$$y^2 - xz - z^2 t^2 = 0. \tag{7}$$

A non-trivial solution of it is $x_0 = -t^2, y_0 = 0, z_0 = 1$. Hence the solutions of (7) can be parametrized in the form

$$\begin{aligned} x &= -t^2 r + p \\ y &= q \\ z &= r \end{aligned} \tag{8}$$

with $p, q, r \in M, r \neq 0$ (cf. [10], [8]). Substituting these expressions into (7) we obtain $rp = q^2$. We multiply all equations of (8) by p and replace rp by q^2, whence

$$\begin{aligned} kx &= -t^2q^2 + p^2 \\ ky &= pq \\ kz &= q^2 \end{aligned} \tag{9}$$

with some $k \in M$. In case $\mathbb{Z}_M$ has unique factorization, we multiply these equations by the square of the common denominators of p, q and divide them by the square of the gcd of p, q. This way we can replace the parameters k, p, q by parameters in $\mathbb{Z}_M$. (Remark that if $\mathbb{Z}_M$ has no unique factorization, then principally the same argument is followed involving ideals of $\mathbb{Z}_M$. The detailed procedure can be found in [8].)

Considering the coefficients of p^2, pq, q^2 in the representation of kx, ky, kz in (9) and calculating the determinant of the corresponding 3x3 matrix we confer that k must also be a unit (cf. [8]). Finally, substituting the representation (9) into $Q_1(x, y, z) = u$ we obtain

$$p^4 - t^2p^2q^2 + q^4 = k^2u.$$

(The second equation $Q_2(x, y, z) = v$ vanishes on both sides.)

Applying the results of Theorem 2 of V.Ziegler [12] we can describe the solutions of this relative quartic Thue equation, hence also x, y, z in (9) which gives the result of our Theorem 1. Note that Theorem 2 of V.Ziegler [12] is only valid for $|t| > 245$.

5.2 Proof of Theorem 2

In our Lemma we substitute $a_1 = -4t, a_2 = 6t + 2, a_3 = 4t, a_4 = 1$. Equation (5) is of the form

$$F(u, v) = (u + 2v)(u - (2 - 2t)v)(u - (2 + 8t)v) = \varepsilon$$

where ε is a unit in M. Therefore all factors of $F(u, v)$ must also be units in M which implies $v = 0$ and u a unit in M. Again $Q_0 = 0$ implies $Q_2 = 0$, that is

$$y^2 - xz + 4tyz + (6t + 2)z^2 = 0. \tag{10}$$

A non-trivial solution of it is $x_0 = 6t+2, y_0 = 0, z_0 = 1$. Hence the solutions of (10) can be parametrized in the form

$$\begin{aligned} x &= (6t+2)r + p \\ y &= q \\ z &= r \end{aligned} \tag{11}$$

with $p, q, r \in M, r \neq 0$. Substituting these expressions into (10) we obtain $q^2 = r(p - 4tq)$. We multiply all equations of (11) by $p - 4tq$ and replace $r(p - 4tq)$ by q^2, whence

$$\begin{aligned} kx &= p^2 - 4tpq + (6t+2)q^2 \\ ky &= pq - 4tq^2 \\ kz &= q^2 \end{aligned} \tag{12}$$

with some $k \in M$. Similarly as in I we replace the parameters k, p, q by parameters in $\mathbb{Z}_M$. Again we confer that k must also be a unit. Finally, substituting the representation (12) into $Q_1(x, y, z) = u$ we obtain

$$p^4 - 4tp^3q + (6t+2)p^2q^2 + 4tpq^3 + q^4 = k^2u.$$

(The second equation $Q_2(x, y, z) = v$ again vanishes on both sides.)

Applying the results of Theorem 2 of B.Jadrijevič and V.Ziegler [9] we can describe the solutions of this relative quartic Thue equation, hence also x, y, z in (12) which gives the result of our Theorem 2. Note that Theorem 2 of B.Jadrijevič and V.Ziegler [9] is only valid for $|t| > 1544803$.

5.3 Proofs of Theorem 3 and Theorem 4

In this proof we use the result of B.K.Spearman and K.S.Williams [11]. They consider octic fields generated by a root of the polynomial $x^8 + (t^2+2)x^4 + 1 = (x^4 - itx^2 + 1)(x^4 + itx^2 + 1)$. We set $M = \mathbb{Q}(i)$, $t \in \mathbb{Z}_M$ a parameter such that $f(x) = x^4 - itx^2 + 1$ is irreducible over M. Let ξ be a root of $f(x)$ and $K = M(\xi)$.

We take $t \in \mathbb{Z}_M \setminus \mathbb{Z}$, $\mathcal{O} = \mathbb{Z}_M[\xi]$ for the purposes of Theorem 3. However, if $t \in \mathbb{N}$, $t^2 + 4$ squarefree, the result of B.K.Spearman and K.S.Williams [11] implies, that ξ itself generates power integral basis of K over M, that is why in Theorem 4 we take $\mathcal{O} = \mathbb{Z}_K$.

In the following we consider the two cases (according to Theorem 3 and Theorem 4, respectively) together. In our Lemma we substitute $a_1 = 0, a_2 = -it, a_3 = 0, a_4 = 1$. Equation (5) is of the form

$$F(u,v) = (u + itv)(u - 2v)(u + 2v) = \varepsilon$$

where ε is a unit in M. Therefore all factors of $F(u,v)$ must also be units in M which implies $v = 0$ and u a unit in M. By $Q_0 = 0$ we again get $Q_2 = 0$, that is

$$y^2 - xz - itz^2 = 0. \tag{13}$$

A non-trivial solution of it is $x_0 = 1, y_0 = 0, z_0 = 0$. Hence the solutions of (13) can be parametrized in the form

$$\begin{aligned} x &= r \\ y &= p \\ z &= q \end{aligned} \tag{14}$$

with $p, q, r \in M, r \neq 0$. Substituting these expressions into (13) we obtain $rq = p^2 - itq^2$. We multiply all equations of (14) by q and replace rq by $p^2 - itq^2$, whence

$$\begin{aligned} kx &= p^2 - itq^2 \\ ky &= pq \\ kz &= q^2 \end{aligned} \tag{15}$$

with some $k \in M$. Similarly as before we replace the parameters k, p, q by parameters in $\mathbb{Z}_M$. Again we confer that k must also be a unit. Finally, substituting the representation (15) into $Q_1(x, y, z) = u$ we obtain

$$p^4 - itp^2q^2 + q^4 = k^2u. \tag{16}$$

(The second equation $Q_2(x, y, z) = v$ again vanishes on both sides.)

Unfortunately the solutions of this parametric relative Thue equation are not known in general. We could only test "small" solutions of the equation for "small" parameters t.

For the case of Theorem 3 we let $t \in \mathbb{Z}_M \setminus \mathbb{Z}$ run through the range $t \leq 50$ (such that $f(x)$ is irreducible over M), and tested the solutions of equation (16) for $|q|^2 \leq 1000$ with the possible right hand sides $\pm 1, \pm i$.

(The range $|q|^2 \leq 1000$ covers the range $\max(|x|,|y|,|z|) \leq 30$ by (15).) For given t, q and right hand side we calculated the roots p of the equation and tested if it is in $\mathbb{Z}_M$. In this range we only found trivial solutions, that is $(p,q) = (1,0), (0,1)$ and their associates. Up to unit factors these solutions imply $(x,y,z) = (1,0,0), (-it,0,1)$ by (15).

For the case of Theorem 4 we let $t \in N$ run thought the values from $1 \leq t \leq 100$ with t^2+4 squarefree. For $|q|^2 \leq 1000$ and the possible right hand sides $\pm 1, \pm i$ we calculated the corresponding roots of equation (16) and tested if it is in $\mathbb{Z}_M$. (The range $|q|^2 \leq 1000$ again corresponds to the range $\max(|x|,|y|,|z|) \leq 30$ by (15).) In addition to the trivial solutions $(p,q) = (1,0), (0,1)$ we only found additional solutions for $t = 1$, namely $(p,q) = (1, 1+i), (-1, 1+i), (1+i, 1), (1+i, -1)$ which give the solutions listed in Theorem 4 by (15).

Remark 1. There are usually several posible parametrization of the solutions of the quadratic form equation $Q_0(x,y,z) = 0$. It is not always straitforward to find a suitable parametrization leading to a known family of parametric Thue equations.
Remark 2. The direct calculations involved in Theorems 3 and 4 were performed in Maple on a simple PC. The CPU time took a couple of hours.
Remark 3. Our experience supports the conjecture that the assertions of Theorems 3 and 4 are true in general (not only for small parameters t and small values of x, y, z).

References

[1] M. Daberkow, C.Fieker, J.Klüners, M.Pohst, K.Roegner and K.Wildanger, *KANT V4* , J. Symbolic Comput. **24** (1997), 267–283. http://www.math.tu-berlin.de/~kant/

[2] I.Gaál, *Diophantine equations and power integral bases*, Boston, Birkhäuser, 2002.

[3] I.Gaál, *Power integral bases in cubic relative extensions*, Experimental Math., **10**(2001), 133–139.

[4] I.Gaál and G.Lettl, *A parametric family of quintic Thue equations II.*, Monatsh. Math., **131**(2000), 29–35.

[5] I.Gaál, A.Pethő and M.Pohst, *On the resolution of index form equations in quartic number fields*, J. Symb. Comput. **16**(1993), No.6, 563-584.

[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 cyclic quintics*, Math. Comp. **66**(1997), 1689-1696.

[8] I.Gaál and M.Pohst, *On the resolution of index form equations in relative quartic extensions*, J.Number Theory, **85**(2000), 201–219.

[9] B.Jadrijevič, V.Ziegler, *A system of relative Pellian equations and a related family of relative Thue equations*, Int. J. Number Theory **2**(2006), No. 4, 569-590.

[10] L.J.Mordell, Diophantine equations, Pure and Applied Mathematics, 30. London-New York: Academic Press, 1969.

[11] B.K.Spearman and K.S.Williams, *The simplest D_4–octics*, Int. J. Algebra **2**(2008), 79–89.

[12] V.Ziegler, *On a family of relative quartic Thue inequalities*, J. Number Theory **120**(2006), No. 2, 303-325.