Publ. Math. Debrecen
42 / 3–4 (1993), 253–263

Power integral bases in orders of families of quartic fields

By ISTVÁN GAÁL (Debrecen)

Dedicated to Professor Lajos Tamássy on his 70th birthday

Abstract. We consider five infinite families of polynomials, namely

I $f_1(x) = x^4 + k \quad (k > 0,\ k \neq 4k_0^4)$
II $f_2(x) = x^4 + k^2x^2 - 2kx + 1$
III $f_3(x) = x^4 + x^3 + kx^2 + \varepsilon x + 1 \quad (k > 0,\ \varepsilon = \pm 1,\ k \neq 2 \text{ if } \varepsilon = 1)$
IV $f_4(x) = x^4 + 4kx^3 + 4k^2x^2 + 8x + 4(k^2 + 2k + 3)$
V $f_5(x) = x^4 + kx^2 + 1 \quad (k \geq 3)$

with an integer parameter k. We show, that all these polynomials are irreducible, a root ξ of any of them generates a totally complex quartic field $K = \mathbb{Q}(\xi)$, we describe the Galois group of K and compute all power integral bases in the order $\mathbb{Z}[\xi]$ of the ring of integers of K.

1. Introduction

In a series of papers [2], [3], [4] (see also [5]) the author together with Pethő and Pohst considered certain methods for the resolution of index form equations in certain types of quartic number fields. These methods depend on the Galois structure of the field. Recently they gave a method [6] that makes it possible to find in feasible time the "small" solutions of index form equations in *any* quartic field. (Under "small" solutions we mean the solutions that do not exceed a prescribed bound e.g. 10^{20} in absolute value.) In the totally complex case this method gives all solutions of the index form equations.

The author is grateful to the Alexander von Humboldt Stiftung for supporting his work and also to the Mathematisches Institut der Heinrich–Heine–Universität in Düsseldorf for its hospitality during the author's stay there as a Humboldt-fellow .

In the present paper we consider five infinite families of totally complex quartic fields $K = \mathbb{Q}(\xi)$, generated by a root ξ of one of the following polynomials

$$\begin{array}{rl} \text{I} & f_1(x) = x^4 + k \quad (k > 0,\ k \neq 4k_0^4) \\ \text{II} & f_2(x) = x^4 + k^2x^2 - 2kx + 1 \\ \text{III} & f_3(x) = x^4 + x^3 + kx^2 + \varepsilon x + 1 \ (k > 0,\ \varepsilon = \pm 1,\ k \neq 2 \text{ if } \varepsilon = 1) \\ \text{IV} & f_4(x) = x^4 + 4kx^3 + 4k^2x^2 + 8x + 4(k^2 + 2k + 3) \\ \text{V} & f_5(x) = x^4 + kx^2 + 1 \quad (k \geq 3) \end{array}$$

where k is a parameter taking any integer value with the above restrictions (in the family I k is not allowed to take a value of the form $4k_0^4$ where $k_0 \in \mathbb{Z}$).

We prove that in the above five families all polynomials are irreducible, the corresponding fields K are totally complex, we describe the Galois group of K, and determine all solutions of the index form equation of K corresponding to the basis $(1, \xi, \xi^2, \xi^3)$ of the order $\mathbb{Z}[\xi]$ of the ring of integers of K, that is we determine all $\alpha \in \mathbb{Z}[\xi]$ which generate a power integral basis $(1, \alpha, \alpha^2, \alpha^3)$ in $\mathbb{Z}[\xi]$.

The main purpose of the paper is to demonstrate that the method of [6] can be applied not only to single number fields, but also to *infinite families* of number fields. Our method is probably applicable also to some other families of totally complex quartic fields, however, the above families of fields have the following interesting features: I is the simplest possible family of fields ("pure quartic fields"), in families II–III the index form equation admits several non-trivial solutions, family II was also considered by Nagell [11], IV is a family of fields with Galois group A_4 that occur very seldom: there are only 90 fields of this type among the 81322 totally complex quartic fields with discriminant $< 10^6$. Family V was considered by several authors, cf. e.g. Cusick [1].

Finally, we remark that an analogous problem for the family $f_a(x) = x^4 - ax^3 - x^2 + ax + 1$ (with some restrictions on a) was recently considered with different methods by Mignotte, Pethő and Roth [10].

Notation. In the following we denote by a_1, a_2, a_3, a_4 the coefficients of any of the above polynomials, that is we write $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$.

2. Irreducibility

First we show that the polynomials under consideration are irreducible:

Lemma 1. *All polynomials in the families I–V are irreducible.*

Proof of Lemma 1. We have to show, that

– $f(x)$ has no integer roots
– $f(x)$ cannot be factorized in the form $(x^2+ax+b)(x^2+cx+d)$.

The first assertion follows from Lemma 4 of Section 3 where we prove that $f(x)$ has only complex (non–real) roots. Hence we only have to demonstrate, that the equation system

$$a+c=a_1 \tag{1}$$

$$d+ac+b=a_2 \tag{2}$$

$$ad+bc=a_3 \tag{3}$$

$$db=a_4 \tag{4}$$

has no integer solutions a,b,c,d.

I. If we had $a=0$, then by (1) $c=0$, by (2) $b=-d$ and by (4) $-d^2=k>0$ which is a contradiction. Assume that $a\neq 0$. Then by (1) $c=-a$, by (2) and (3) $d+b=a^2$, $d-b=0$ whence $d=b=a^2/2$ and by (4) $k=bd=a^4/4$. It follows that f_1 can be reducible only if $a=2k_0$ in which case $k=4k_0^4$ and $f_1(x)=(x^2+2k_0x+2k_0^2)(x^2-2k_0x+2k_0^2)$, but $k=4k_0^4$ is excluded.

II. By (1) $c=-a$, (4) implies $bd=1$ that is either $b=d=1$ or $b=d=-1$, and by (3) $-2k=ad+bc$ whence $-2k=(d-b)a=0$. Hence the equation system implies $k=0$ but x^4+1 is irreducible.

III. By (4) $bd=1$ that is $b=d=\pm 1$. Put $\eta=b=d$. By (1) we get $c=1-a$ and substituting b,d,c into (3) we get $b=\varepsilon$ that is $\varepsilon=\eta$. Finally, (2) gives $a^2-a+k-2\varepsilon=0$. This equation has negative discriminant for $k>2$. Checking the four polynomials corresponding to $k=1,2$ and $\varepsilon=\pm 1$ we find that they are irreducible except when $k=2$, $\varepsilon=1$.

IV. We express c from the first equation, and substitute it into (2), (3), (4); then we express d from the second equation and substitute it again into (3),(4) to get

$$a^3-4ka^2+4k^2a+b(4k-2a)=8 \tag{3'}$$

$$(4k^2+a^2-4ka-b)b=4(k^2+2k+3)\,. \tag{4'}$$

If in (3′) we had $a=2k$ then by (4′) we would obtain $-b^2=4(k^2+2k+3)>0$ which is impossible. Hence we can express b from (3′) and substitute into (4′) to conclude

$$a^6-12ka^5+56k^2a^4-128k^3a^3+16(9k^4-k^2-3)a^2+$$
$$64(-k^5+k^3+3k)a-64(k^4+3k^2+1)=0\,.$$

It follows that we must have $a = 2\bar{a}$. After dividing by 64 the above equation gives

$$\bar{a}^6 - 6k\bar{a}^5 + 14k^2\bar{a}^4 - 16k^3\bar{a}^3 + (9k^4 - k^2 - 3)\bar{a}^2 + 2(-k^5 + k^3 + 3k)\bar{a} - (k^4 + 3k^2 + 1) = 0\,.$$

Here the constant term is always odd, hence the equation can only hold if $\bar{a} = 2\hat{a} + 1$. Substituting it into the former equation and considering it modulo 2 we conclude

$$1 + 9k^4 - k^2 - 3 - k^4 - 3k^2 - 1 = 8k^4 - 4k^2 - 3 \equiv 1 \pmod 2$$

which is a contradiction.

V. (1) implies $c = -a$ whence by (3) we have $a(d - b) = 0$. If $a = 0$ then by (2) and (4) $d + b = k, db = 1$ which cannot hold because of $k \geq 3$. If $b = d$ then by (4) $d = \pm 1$ whence by (2) $k = \pm 2 - a^2$ which is again impossible. □

3. Signature

First we formulate the following assertion concerning the discriminants of the polynomials:

Lemma 2. *The polynomials in families* I–V *have the following discriminants:*

I	$D(f_1) = 256k^3$
II	$D(f_2) = 16(k^4 + 16)$
III	$D(f_3) = k(k + 4)(-9 + 4k)^2$ *if* $\varepsilon = 1$
	$D(f_3) = (k^2 - 4k + 8)(7 + 4k)^2$ *if* $\varepsilon = -1$
IV	$D(f_4) = 2^{12}(9 + 3k^2 + k^4)^2$
V	$D(f_5) = 16(k^2 - 4)^2$.

The proof of the lemma is direct calculation.

Remark. It is important to remark, that for any value of k, according to the original conditions, in families I–V all discriminants are positive. It follows, that the corresponding discriminants of the number fields K are also positive.

In the sequel we need certain polynomials related to $f(x)$. Although some of them we apply only in the following sections, we take here the opportunity to introduce all of them and point out the relation between them. Let

$$F(x, y) = x^3 - a_2x^2y + (a_1a_3 - 4a_4)xy^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)y^3. \tag{5}$$

The polynomial $R(x) = F(x, 1)$ is sometimes used as a resolvent polynomial of $f(x)$. However, to determine the roots of $f(x)$ it can be more

helpful to substitute $x = y - a_1/4$ in $f(x)$ in order to eliminate the term of degree 3 to get a polynomial $f_0(y) = y^4 + b_2y^2 + b_3y + b_4$ and then to define

$$r(z) = z^3 - 2b_2z^2 + (b_2^2 - 4b_4)z + b_3^2 \ .$$

The correspondence of $F(x, y)$, $R(x)$ and $r(z)$ and the way of determining the roots of $f(x)$ by using the roots of $r(z)$ is shown in the following lemma.

Lemma 3. *Denote by* ξ_i, $i = 1, \dots, 4$ *the roots of* $f(x)$.

(a) *The roots of* $R(x)$ *are* $\xi_i\xi_j + \xi_k\xi_l$ *for* $(i, j, k, l) = (1, 2, 3, 4)$, $(1, 3, 2, 4)$, $(1, 4, 2, 3)$.

(b) *The roots of* $r(z)$ *are* $(y_i + y_j)(y_k + y_l)$ *(for the same indices as before) where* $y_i = \xi_i + a_1/4$, $i = 1, \dots, 4$.

(c) $r(z) = -R(-z + a_2 - a_1^2/4)$.

(d) *For the roots* $y_i = \xi_i + a_1/4$ *of* $f_0(y)$ *we have*

$$\begin{aligned} 2y_1 &= \sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3} \\ 2y_2 &= \sqrt{-\theta_1} - \sqrt{-\theta_2} - \sqrt{-\theta_3} \\ 2y_3 &= -\sqrt{-\theta_1} + \sqrt{-\theta_2} - \sqrt{-\theta_3} \\ 2y_4 &= -\sqrt{-\theta_1} - \sqrt{-\theta_2} + \sqrt{-\theta_3} \ . \end{aligned}$$

where $\theta_1, \theta_2, \theta_3$ *are the roots of* $r(z)$.

Proof of Lemma 3. (a) and (b) can be checked directly, for (b) see also [8]. (c) follows from Lemma 2 of [6]. For (d) see again [8]. □

The main purpose of this Section is to prove:

Lemma 4. *The polynomials in the families I–V have only complex (=non-real) roots.*

Proof of Lemma 4.. By the remark after Lemma 2 $D(f)$ is always positive, which implies that either all the roots are real or all of them are complex (=non-real). Obviously ξ_i is non-real if and only if y_i is non-real, hence we only have to show that there exists a non-real y_i. Further, by (d) of Lemma 3 we can express all the $\sqrt{-\theta_i}$ by the y_i-s, hence if all the y_i-s were real, then we would obtain, that also all the $\sqrt{-\theta_i}$-s are real. This means, that it is sufficient to demonstrate that there exists a θ_i which is positive. Finally, by (c) of Lemma 2 this is equivalent with the fact, that there exists a root $\mu_i = -\theta_i + a_2 - a_1^2/4$ of $R(x)$ with $-\mu_i + a_2 - a_1^2/4 > 0$.

I. $R(x) = x(x^2 - 4k)$ $a_1 = a_2 = 0$, and for the root $\mu_1 = -2\sqrt{k}$ we have $-\mu_1 > 0$.

II. $R(x) = x(x^2 - xk^2 - 4)$ $a_1 = 0, a_2 = k^2$ for the root $\mu_1 = 0$ we have $-\mu_1 + k^2 > 0$ if $k \neq 0$, but for $k = 0$ the polynomial $x^4 + 1$ is totally complex.

III. $\varepsilon = 1$. $R(x) = (x-2)(x^2 - xk + 2x + 1 - 2k)$ $a_1 = 1, a_2 = k$, for the root $\mu_1 = 2$ we have $-\mu_1 + k - 1/4 > 0$, if $k > 2$, the case $k = 1$ can be checked directly, $k = 2$ is excluded.

III. $\varepsilon = -1$. $R(x) = (x+2)(x^2 - xk - 2x - 1 + 2k)$ $a_1 = 1, a_2 = k$, for the root $\mu_1 = -2$ we have $-\mu_1 + k - 1/4 > 0$.

IV. $R(x) = x^3 - 4k^2x^2 - 16k^2x - 48x - 64$, $a_1 = 4k, a_2 = 4k^2$ that means $a_2 - a_1^2/4 = 0$. It is sufficient to show that $R(x)$ has at least one negative root. We have $R(-7) = -71 - 84k^2$, $R(-4) = 64$, $R(0) = -64$ which implies that $R(x)$ has exactly two negative and one positive roots.

V. $R(x) = (x-2)(x+2)(x-k)$, $a_1 = 0, a_2 = k$, for the root $\mu_1 = -2$ we have $-\mu_1 + k = 2 + k > 0$. □

4. Galois groups

In order to describe the Galois group of $f(x)$ we apply the following lemma:

Lemma 5 (Kappe and Warren [7], Theorem 1). *Suppose that* $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ *is irreducible over* $\mathbb{Q}$, *has discriminant* D, *and its resolvent polynomial* $R(x) = x^3 - a_2x^2 + (a_1a_3 - 4a_4)x + (4a_2a_4 - a_3^2 - a_1^2a_4)$ *has splitting field* E.

(i) $Gal(f) = S_4$ *if and only if* $R(x)$ *is irreducible over* $\mathbb{Q}$ *and* D *is not a square.*

(ii) $Gal(f) = A_4$ *if and only if* $R(x)$ *is irreducible over* $\mathbb{Q}$ *and* D *is a square.*

(iii) $Gal(f) = V_4$ *if and only if* $R(x)$ *splits into linear factors over* $\mathbb{Q}$

(iv) $Gal(f) = C_4$ *if and only if* $R(x)$ *has exactly one root* t *in* $\mathbb{Q}$ *and* $g(x) = (x^2 - tx + a_4)(x^2 + a_1x + a_2 - t)$ *splits over* E

(v) $Gal(f) = D_8$ *if and only if* $R(x)$ *has exactly one root* t *in* $\mathbb{Q}$ *and* $g(x)$ *does not split over* E.

By using the above lemma we show, that

Lemma 6.

I. The polynomial f_1 *has Galois group* D_8 *if* k *is not a square, and* V_4 *if* k *is a square.*

II. The polynomial f_2 *has Galois group* D_8 *if* $k \neq 0$ *and* V_4 *if* $k = 0$.

III. The polynomial f_3 *has Galois group* D_8 *with the exception of the following cases:* C_4 *if* $k = 1, \varepsilon = 1$, V_4 *if* $k = 2, \varepsilon = -1$.

IV. The polynomial f_4 *has Galois group* A_4.

V. The polynomial f_5 *has Galois group* V_4.

PROOF OF LEMMA 6.

I. We have $R(x) = x(x^2 - 4k)$. If k is a square, then $R(x)$ factorizes into linear factors and the Galois group is V_4. If k is not a square, then $R(x)$ has the only root $t = 0$ in $\mathbb{Q}$, it splits over $E = \mathbb{Q}(\sqrt{k})$ but $g(x) = (x^2+k)x^2$ does not split over E.

II. We have $R(x) = x(x^2-k^2x-4)$ and the discriminant of the second degree factor of $R(x)$ is $k^4 + 16$ which can only be a square for $k = 0$, in which case $R(x)$ splits over $\mathbb{Q}$ and the Galois group is V_4. For $k \neq 0$ $R(x)$ splits over $E = \mathbb{Q}(\sqrt{k^4 + 16})$ but $g(x) = (x^2 + 1)(x^2 + k^2)$ has non–real roots.

III. $\varepsilon = 1$. We have $R(x) = (x - 2)(x^2 - kx + 2x + 1 - 2k)$. The discriminant of the second factor is $k^2 + 4k$ which is never a square, it splits over $E = \mathbb{Q}(\sqrt{k^2 + 4k})$. Further, $g(x) = (x - 1)^2(x^2 + x + k - 2)$ where the discriminant of the second factor is $9 - 4k$ which is negative for $k > 2$, that is g splits over a complex quadratic field. In these cases the Galois group is D_8 because E is real. For $k = 1$ we have $E = \mathbb{Q}(\sqrt{5})$ over which g also splits, that means the Galois group is C_4. $k = 2$ is excuded.

III. $\varepsilon = -1$. We have $R(x) = (x + 2)(x^2 - kx - 2x - 1 + 2k)$ where the discriminant of the second factor is $(k - 2)^2 + 4$ being square only for $k = 2$ when the Galois group is V_4. For any other k R splits over the real quadratic field $E = \mathbb{Q}(\sqrt{(k - 2)^2 + 4})$ but $g(x) = (x + 1)^2(x^2 + x + k + 2)$ splits over the complex quadratic field $\mathbb{Q}(\sqrt{-4k - 7})$.

IV. We have $R(x) = x^3 - 4k^2x^2 - 16k^2x - 48x - 64$. If we substitute $x = 4y$ and divide by 64 we obtain $\bar{R}(y) = y^3 - k^2y^2 - y(k^2 + 3) - 1$. This polynomial is irreducible (cf. also [12]). Further, by Lemma 2 the discriminant is a full square, hence the Galois group is A_4.

V. In this case we have $R(x) = (x - 2)(x + 2)(x - k)$ which implies the assertion. □

5. The index form equations

After having made the above preparations we arrive at the most important part of our discussion, namely we want to describe all power integral bases $(1, \alpha, \alpha^2, \alpha^3)$ in the order $\mathbb{Z}[\xi]$ of the field $K = \mathbb{Q}(\xi)$ generated by a root ξ of $f(x)$.

Our main tool is the following assertion:

Lemma 7 (GAÁL, PETHŐ and POHST [6]). *According to the above notation let $f(x) = x^4+a_1x^3+a_2x^2+a_3x+a_4$ be the defining polynomial of ξ and let $F(u, v) = u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3$. An element $\alpha = a + x\xi + y\xi^2 + z\xi^3$ $(a, x, y, z \in \mathbb{Z})$ generates a power*

integral basis in the order $\mathbb{Z}[\xi]$ *of the field* $K = \mathbb{Q}(\xi)$ *if and only if there exists a solution* $(u, v) \in \mathbb{Z}^2$ *of the equation*

$$F(u, v) = \pm 1 \tag{6}$$

such that u, v *can be represented as*

$$Q_1(x, y, z) = x^2 - xya_1 + y^2a_2 + xz(a_1^2 - 2a_2) + yz(a_3 - a_1a_2) + \\ + z^2(-a_1a_3 + a_2^2 + a_4) = u \tag{7}$$

$$Q_2(x, y, z) = y^2 - xz - a_1yz + z^2a_2 = v \tag{8}$$

with the coefficients x, y, z *of* α.

Further, if K *is totally complex, then the quadratic form*

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

is positive definite if and only if $\lambda \in (\lambda_1, \lambda_2)$ *where* $\lambda_1 < \lambda_2 < \lambda_3$ *denote the three distinct real roots of* $R(x) = F(x, 1)$.

Proof of Lemma 7. In order to prove the first part of the assertion apply the proof of Theorem 1 of [6] with $d = m = n = i_m = 1$ (according to the notation of [6]). The second part follows from Theorem 2 of [6]. □

Remark. The essence of the method of [6] for determining the suitable triples (x, y, z) (a is arbitrary) in totally complex quartic fields is first to find all solutions (u, v) of (6), then to build a positive definite quadratic form $T_\lambda(x, y, z) = Q_1(x, y, z) + \lambda Q_2(x, y, z)$, for each solution (u, v) (with $u + \lambda v \geq 0$) to enumerate the solutions of $T_\lambda(x, y, z) = u + \lambda v$ and to check (7), (8).

Our main result is the following

Theorem 1. *Let* ξ *be a root of one of the polynomials in the families I–V. The element* $\alpha = a + x\alpha + y\alpha^2 + z\alpha^3$ $(a, x, y, z \in \mathbb{Z})$ *generates a power integral basis* $(1, \alpha, \alpha^2, \alpha^3)$ *of the order* $\mathbb{Z}[\xi]$ *of the field* $K = \mathbb{Q}(\xi)$, *if and only if* $a \in \mathbb{Z}$ *and* (x, y, z) *is equal to one of the following triples or their negatives:*

I. $(1, 0, 0)$, $(0, 0, 1)$ *if* $k = 1$, $(1, 0, 0)$ *if* $k \geq 2$

II. $(1, 0, 0)$, $(k^2, 0, 1)$, $(k^4 + 1, k, k^2)$, *further, if* $k = 2l$ $(l \in \mathbb{Z})$, *then also* $(8l^4 + 1, l, 2l^2)$.

III.
$(1, 0, 0)$, $(1, 1, 1)$, $(1, 1, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ $(1, 0, 1)$ *if* $k = 1$, $\varepsilon = 1$,
$(1, 0, 0)$, $(3, 1, 1)$, $(2, 0, 1)$, $(1, 1, 0)$, $(0, 1, 0)$ *if* $k = 3$, $\varepsilon = 1$,
$(1, 0, 0)$, $(k, 1, 1)$ *for any other allowed pair* k, ε.

IV. $(1, 0, 0)$ *for any* $k \in \mathbb{Z}$

V. $(1,0,0)$, $(k,0,1)$ *for any allowed* k.

Proof of Theorem 1.

I. The solutions of $F(u,v) = u(u^2 - 4kv^2) = \pm 1$ are $u = \pm 1, v = 0$. It follows from

$$Q_1 + Q_2 = \left(x - \frac{z}{2}\right)^2 + y^2 + \left(k - \frac{1}{4}\right) z^2 = 1$$

that only $u = 1$ is possible and $z = 0$ if $k \geq 2$. In this case the possible solutions are $(1,0,0)$ and $(0,1,0)$ but the second one does not satisfy (8). If $k = 1$, the possibilities are $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(1,0,1)$ but the second and the fourth one fail in testing (7) and (8).

II. We have $F(u,v) = u(u^2 - k^2uv - 4v^2) = \pm 1$, whence $u = \pm 1$ and $v = 0$ or $v = \mp k^2/4$, the second being possible only if k is even. In order to avoid complicated formulas, in both cases we use the positive semidefinite quadratic form

$$Q_1 = (x - zk^2)^2 + (yk - z)^2 = 1 \quad . \tag{9}$$

It follows that only $u = 1$ is possible and either (i) $x - zk^2 = \pm 1$ and $yk = z$, or (ii) $x = zk^2$ and $yk - z = \pm 1$.

Consider first the solution $(u,v) = (1,0)$. Combining $Q_2 = y^2 - xz + z^2k^2 = 0$ with (i) we obtain $(1,0,0)$ and (k^4+1, k, k^2), and for (ii) we get $(k^2, 0, 1)$.

Consider now the even values of k, that is $k = 2l$ and the solution $(u,v) = (1, -k^2/4) = (1, -l^2)$. The above equation pairs (i) and (ii) we combine now with $Q_2 = y^2 - xz + 4l^2z^2 = -l^2$ and we obtain the additional solution $(8l^4+1, l, 2l^2)$ for (i). For (ii) our equation system can be reduced to $y^2 = -l^2$ whence $l = 0$, $v = 0$ and we have already found the corresponding solution for $k = 0$.

III. In this case

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

has solutions $(u,v) = (\pm 1, 0)$ for any allowed k and ε. Further, for $k = 1$, $\varepsilon = 1$ the pair $(u,v) = (\pm 1, \pm 1)$, and for $k = 3$, $\varepsilon = 1$ the pair $(u,v) = (\pm 3, \pm 1)$ is also a solution.

First consider $(u,v) = (\pm 1, 0)$. We have

$$Q_1 = \left(x - \frac{y}{2} + \left(\frac{1}{2} - k\right) z\right)^2 + \frac{4}{4k-1}\left(\left(k - \frac{1}{4}\right) y + \left(\frac{\varepsilon}{2} - k + \frac{1}{4}\right) z\right)^2 + \frac{4k-2}{4k-1} z^2 = 1$$

which implies that only $u = 1$ is possible and $|z| \leq 1$.

If $z = 0$ then by (8) we have $0 = v = y^2$ whence $y = 0$ and $x = 1$.

For $|z| = 1$, we assume that $z = 1$, then we can rewrite the above equation $Q_1 = 1$ as

$$(4k-1)(2x - y + (1-2k))^2 + ((4k-1)y + (2\varepsilon - 4k + 1))^2 = 4 \ .$$

In case $k \geq 2$ this equation can only hold if the first term is 0 and the second one is 4, whence $x = k, y = 1, z = 1$. In case $k = 1$ we obtain $(1, 1, 1)$ in the same way. For $k = 1$ it is also possible, that the first term above is 3 and the second one is 1 which gives the solution $(1, 0, 1)$ for $k = 1, \varepsilon = 1$.

In case $k = 1$, $\varepsilon = 1$ for $(u, v) = (\pm 1, \pm 1)$ we obtain the further solutions $(0, 0, 1)$, $(1, 1, 0)$, $(0, 1, 0)$.

In case $k = 3$, $\varepsilon = 1$ for $(u, v) = (\pm 3, \pm 1)$ we obtain the further solutions $(2, 0, 1)$, $(1, 1, 0)$, $(0, 1, 0)$.

IV. In this case the equation to be solved is

$$F(u, v) = u^3 - 4k^2u^2v - 16(k^2 + 3)uv^2 - 64v^3 = \pm 1.$$

Substituting $v_1 = 4v$ we rewrite the above equation as

$$F_1(u, v_1) = u^3 - k^2u^2v_1 - (k^2 + 3)uv_1^2 - v_1^3 = \pm 1.$$

This family of cubic Thue equations (corresponding to the "simplest cubic fields" of SHANKS [12]) was considered by THOMAS [13] whose results were completed by MIGNOTTE [9]. Their works imply, that the only solution (u, v_1) of this equation, for which v_1 is divisible by 4 is $(\pm 1, 0)$, that yields $(u, v) = (\pm 1, 0)$. We build

$$Q_1 + Q_2 = \left(x - 2ky + \left(4k^2 - \frac{1}{2}\right)z\right)^2 + \\ + (y + (4 - 3k)z)^2 + \left(3k^2 - \frac{17}{4}\right)z^2 = 1$$

whence only $u = 1$ is possible. For $|k| \geq 2$ the above form is positive definite and z can only be 0. The two candidates we obtain are $(1, 0, 0)$ and $(2k, 1, 0)$ but the last one fails to satisfy (8).

For $k = 0, \pm 1$ we consider $Q_1 + 2Q_2 = 1$, yielding $(x - z)^2 + 2(y + 2z)^2 + 3z^2 = 1$ for $k = 0$, $(x - 2y + 3z)^2 + 2(y - z)^2 + 5z^2 = 1$ for $k = 1$ and $(x + 2y + 3z)^2 + 2(y + 5z)^2 + 5z^2 = 1$ for $k = -1$, all of them having only the trivial solution $(1, 0, 0)$.

V. In this case we have

$$F(u, v) = (u - 2v)(u + 2v)(u - kv) = \pm 1 \ .$$

It can be easily seen, that the only solutions are $(u, v) = (\pm 1, 0)$. Further, the form Q_1 is positive definite,

$$Q_1 = (x - kz)^2 + ky^2 + z^2 = 1$$

which implies $y = 0$ because of $k \geq 3$. If $x - kz = 1, z = 0$ then we get the trivial solution $(1, 0, 0)$, if $x - kz = 0, z = 1$, we obtain the solution $(k, 0, 1)$ which satisfies also the other equation $Q_2 = 0$. □

References

[1] T. W. Cusick, The diophantine equation $x^4 - kx^2y^2 + y^4 = 1$, *Arch. Math.* **59** (1992), 345–347.

[2] I. Gaál, A. Pethő and M. Pohst, On the resolution of index form equations in biquadratic number fields, I, *J. Number Theory* **38** (1991), 18–34.

[3] I. Gaál, A. Pethő and M. Pohst, On the resolution of index form equations in biquadratic number fields, II, *J. Number Theory* **38** (1991), 35–51.

[4] 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* (*to appear*).

[5] I. Gaál, A. Pethő and M. Pohst, On the resolution of index form equations, Proc. of the 1991 International Symposium on Symbolic and Algebraic Computation, ed. by Stephen M. Watt, *ACM Press*, 1991, pp. 185–186.

[6] I. Gaál, A. Pethő and M. Pohst, On the resolution of index form equations in quartic fields (*to appear*).

[7] L. C. Kappe and B. Warren, An elementary test for the Galois group of a quartic polynomial, *Amer. Math. Monthly* **96** (1989), 133–137.

[8] R. Kochendörfer, Einführung in die Algebra, *Berlin*, 1966.

[9] M. Mignotte, Verification of a conjecture of E. Thomas (*to appear*).

[10] M. Mignotte, A. Pethő and R. Roth, Complete solutions of quartic Thue and index form equations (*to appear*).

[11] T. Nagell, Sur les representations de l'unite par les formes binaires biquadratiques du premier rang, *Ark. Mat.* **5** (1964), 477–521.

[12] D. Shanks, The simplest cubic fields, *Math. Comp.* **28** (1974), 1137–1152.

[13] E. Thomas, Complete solutions to a family of cubic diophantine equations, *J. Number Theory* **34** (1990), 235–250.

I. GAÁL
KOSSUTH LAJOS UNIVERSITY
MATHEMATICAL INSTITUTE
H–4010 DEBRECEN, PF. 12
HUNGARY

(Received November 17, 1992)