Simultaneous representation of integers by a pair of ternary quadratic forms – with an application to index form equations in quartic number fields

István Gaál, *
Kossuth Lajos University, Mathematical Institute
H–4010 Debrecen Pf.12.

Attila Pethő †
University Medical School of Debrecen, Laboratory for Computer Science
Nagyerdei krt. 98, H–4028 Debrecen

and Michael Pohst ‡
Heinrich–Heine–Universität, Mathematisches Institut
Universitätsstrasse 1, D–4000 Düsseldorf 1

November 28, 2009

*The author is greatful 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.

†Research supported in part by Hungarian National Foundation for Scientific Research Grant 1641/90

‡Research supported in part by the Deutsche Forschungsgemeinschaft

Abstract

Let $Q_1, Q_2 \in \mathbb{Z}[X, Y, Z]$ be quadratic forms, $u_1, u_2 \in \mathbb{Z}$. In the present paper we consider the problem of solving the system of equations

$$\begin{aligned} Q_1(x, y, z) &= u_1 \\ Q_2(x, y, z) &= u_2 \text{ in } x, y, z \in \mathbb{Z} \ . \end{aligned} \tag{1}$$

Using a method of Mordell [10] the coprime solution of $Q_0(x, y, z) = u_1 Q_2(x, y, z) - u_2 Q_1(x, y, z) = 0$ are given by finitely many expressions of the form $x = f_x(p, q), \quad y = f_y(p, q), \quad z = f_z(p, q)$ where $f_x, f_y, f_z \in \mathbb{Z}[P, Q]$ are quadratic forms and p, q are integer parameters. Substituting these expressions into $Q_1(x, y, z) = u_1$ or $Q_2(x, y, z) = u_2$ we obtain a quartic homogeneous equation in two variables. In case it is irreducible, then it is a quartic Thue equation, otherwise it can be dealt with easier. The solutions p, q of this equation allow us to determine the solutions x, y, z of (1).

We apply these results to index form equations in quartic fields. In [7] we showed, that the problem of solving index form equations in quartic number fields can be reduced to the resolution of a cubic equation $F(u, v) = i$ and a corresponding system of quadratic equations $Q_1(x, y, z) = u, Q_2(x, y, z) = v$ where F is a binary cubic form and $Q_1, \ Q_2$ are ternary quadratic forms. We show, that in this case the application of the above method for the resolution of (1) leads to quartic Thue equations that split over the same quartic field.

1 Introduction

Let $Q_1, Q_2 \in \mathbb{Z}[X, Y, Z]$ be quadratic forms, u_1, u_2 given integers. In this paper we consider the problem of representation of u_1 by the quadratic form Q_1 and u_2 by the quadratic form Q_2 *simultaneously*, by the same $x, y, z \in \mathbb{Z}$, that is we want to solve the system of equations

$$\begin{aligned} Q_1(x, y, z) &= u_1 \\ Q_2(x, y, z) &= u_2 \text{ in } x, y, z \in \mathbb{Z} \ . \end{aligned} \tag{2}$$

We assume without restricting the generality, that $(x, y, z) = 1$ and the forms Q_1 and Q_2 are not proportional (specially, non of them is identically 0). We build the quadratic form

$$Q_0(X, Y, Z) = u_1 Q_2(X, Y, Z) - u_2 Q_1(X, Y, Z) \ . \tag{3}$$

Obviously, if (x, y, z) is a solution of (2) then as a consequence we obtain

$$Q_0(x, y, z) = 0 \ . \tag{4}$$

Using an idea of Mordell [10] we can represent all coprime solutions of (4) in a parametric form. More precisely, there are finitely many quadratic forms $f_x, f_y, f_z \in \mathbb{Z}[P, Q]$ in two variables such that if the parameters p, q run through the coprime integers, then $f_x(p, q)$, $f_y(p, q)$, $f_z(p, q)$ run through the coprime solutions of (4). If we substitute the parametric forms of x, y, z into the first or second equation of (2), according as $u_1 \neq 0$ or $u_2 \neq 0$ then we obtain a homogeneous quartic equation in two variables of the form

$$F_i(p, q) = Q_i(f_x(p, q), f_y(p, q), f_z(p, q)) = u_i \text{ in } p, q \in \mathbb{Z} \tag{5}$$

where $i = 1$ or 2. This equation is either a quartic Thue equation if F_i is irreducible, or F_i is reducible, in both cases we can solve (5) by using known methods. Its solutions allow us to determine the solutions of the original system of equations (2).

As an application of the above method we give an algorithm for the complete resolution of index form equations in arbitrary quartic number fields. In a series of papers [1], [2], [4], [5], [6] the authors have considered methods for the resolution of index form equations in certain types of quartic fields. These methods depent highly on the Galois structure of the field. In [7] we showed, that the index form equation in any quartic field K can be reduced to a cubic equation

$$F(u, v) = i \text{ in } u, v \in \mathbb{Z} \tag{6}$$

and a corresponding system of quadratic equations

$$\begin{aligned} Q_1(x, y, z) &= u \\ Q_2(x, y, z) &= v \end{aligned} \tag{7}$$

where F is a binary cubic form and $Q_1,\ Q_2$ are ternary quadratic forms. Equation (6) is either a cubic Thue equation, or (if F is reducible) it is trivial to solve. We show, that in this case the application of the above method for the resolution of (7) leads to quartic Thue equations that split over the same quartic field K. Thus, we obtain a general algorithm for the complete resolution of index form equation in arbitrary quartic fields, which *reduces the problem to the resolution of a cubic equation (6) and some quartic Thue equations.* This way we establish a basically *new approach* to index form equations in quartic fields, entirely different from the known methods, of Nagell [9] or of [8]. We have to emphasize, that from an *algorithmical point of view* our approach is much more preferable, because there exist already easily applicable computational methods for the resolution of Thue equations, which is not the case e.g. for unit equations (cf. [8]).

2 Simultaneous quadratic forms

Let $Q_1, Q_2 \in \mathbb{Z}[X,Y,Z]$ be non–proportional quadratic forms, $u_1, u_2 \in \mathbb{Z}$ be given integers, and consider the solutions of

$$\begin{aligned} Q_1(x,y,z) &= u_1 \\ Q_2(x,y,z) &= u_2 \ \text{ in } \ x,y,z \in \mathbb{Z} \ \text{ with } \ (x,y,z)=1. \end{aligned} \tag{8}$$

Set

$$Q_0(X,Y,Z) = u_1 Q_2(X,Y,Z) - u_2 Q_1(X,Y,Z) \quad . \tag{9}$$

If x,y,z is a solution of (8), then obviously it is also a solution of

$$Q_0(x,y,z) = 0 \ \text{ in } \ x,y,z \in \mathbb{Z} \quad . \tag{10}$$

To parametrize all solutions of (10) we use Theorem 4 of Chapter 7 of [10]:

Lemma 1 *If $Q_0(X,Y,Z)$ is a quadratic form with integer coefficients, then there exist finitely many quadratic forms $f_x(P,Q), f_y(P,Q), f_z(P,Q)$ with integer coefficients, such that all solutions with $(x,y,z)=1$ of (10) can be represented in the form*

$$x = f_x(p,q) \tag{11}$$

$$y = f_y(p,q) \tag{12}$$

$$z = f_z(p,q) \tag{13}$$

where $p,q \in \mathbb{Z}$ are parameters with $(p,q)=1$.

In order to determine the forms f_x, f_y, f_z we need to find a non–trivial solution of (10). For this purpose one can reduce the quadratic form $Q_0(X,Y,Z)$ to the sum of three squares and apply Theorems 3 or 5 of Chapter 7 of [10]:

Lemma 2 *Let a, b, c be square–free integers with $(a, b) = 1$, $(b, c) = 1$,$(c, a) = 1$. Assume, that a, b, c do not have the same sign and consider the form*

$$ax^2 + by^2 + cz^2 = 0 \quad . \tag{14}$$

(i) (14) has a non–trivial integer solution if and only if $-bc$ is a quadratic residue modulo a, $-ac$ is a quadratic residue modulo b, $-ab$ is a quadratic residue modulo c and moreover the congruence

$$ax^2 + by^2 + cz^2 = 0 \pmod 8$$

has a non–trivial solution.

(ii) If (14) is solvable, then it has a non–trivial integer solution with

$$|x| \leq \sqrt{|bc|}, \quad |y| \leq \sqrt{|ac|}, \quad |z| \leq \sqrt{|ab|} \quad .$$

Using Lemma 2 we can decide if (10) has a non–trivial solution, and if so, we can find such a solution (x_Q, y_Q, z_Q):

$$Q_0(x_Q, y_Q, z_Q) = 0 \quad . \tag{15}$$

Following the proof given in [10] of Lemma 1 we write now x, y, z in a parametric form. Depending on the non–zero values among x_Q, y_Q, z_Q we perform one of the following transformations:

$$\text{if } x_Q \neq 0 \text{ then } \begin{cases} x &= rx_Q \\ y &= ry_Q + p \\ z &= rz_Q + q \end{cases} \tag{16}$$

$$\text{if } y_Q \neq 0 \text{ then } \begin{cases} x &= rx_Q + p \\ y &= ry_Q \\ z &= rz_Q + q \end{cases} \tag{17}$$

$$\text{if } z_Q \neq 0 \text{ then } \begin{cases} x &= rx_Q + p \\ y &= ry_Q + q \\ z &= rz_Q \end{cases} \tag{18}$$

with some rational parameters r, p, q. If among x_Q, y_Q, z_Q there are more non–zero values, then we have more choices. In the following we make some remarks on how we can make a better choice at this point.

Our purpose is now to represent x, y, z as quadratic forms with integer coefficients in two coprime integer variables. We may assume, that in (16), (17), (18) $r \neq 0$, since otherwise we should get a linear form representation of x, y, z

and we could proceed easier (we get two quadratic equations in p, q). We substitute x, y, z of (16), (17) or (18) into (10) and we conclude

$$r^2 Q_0(x_Q, y_Q, z_Q) - r(c_1 p + c_2 q) + (c_3 p^2 + c_4 pq + c_5 q^2) = 0 \qquad (19)$$

with some rational integers $c_1, \ldots, c_5$ the values of which are easily calculated.

Since $Q_0(x_Q, y_Q, z_Q) = 0$ from (19) we get a linear equation for r. We have to test separately the case, when the coefficient $(c_1 p + c_2 q)$ of r disappears. In all these cases we get a linear representation of x, y, z in two parameters and we reach our purpose much easier.

As a consequence of (19) we obtain

$$r = \frac{c_3 p^2 + c_4 pq + c_5 q^2}{c_1 p + c_2 q} \quad .$$

We substitute now this expression into the original formula (16), (17) or (18) and multiply with the common denominator. In addition, we can also change p and q with coprime integer parameters by multiplying with their common denominator. These new parameters we denote again by p, q for simplicity. Then we have represented a multiple of x, y, z as quadratic forms $f_x(p,q), f_y(p,q), f_z(p,q)$ in coprime integer parameters p and q and with coefficients $c_{ij} \in \mathbb{Z}$:

$$\begin{aligned} k \cdot x &= f_x(p,q) = c_{11} p^2 + c_{12} pq + c_{13} q^2 \\ k \cdot y &= f_y(p,q) = c_{21} p^2 + c_{22} pq + c_{23} q^2 \\ k \cdot z &= f_z(p,q) = c_{31} p^2 + c_{32} pq + c_{33} q^2 \end{aligned} \qquad (20)$$

Denote by C the matrix with entries $(c_{ij})_{1 \le i,j \le 3}$.

Lemma 3 *Let*

$$Q_0(X, Y, Z) = a_1 X^2 + a_2 Y^2 + a_3 Z^2 + a_4 XY + a_5 YZ + a_6 ZX \quad .$$

For the determinant of the matrix C we have

$$\begin{aligned} |det\,(C)| &= |x_Q|^3 A \quad \textit{in case of substitution (16)} \\ |det\,(C)| &= |y_Q|^3 A \quad \textit{in case of substitution (17)} \\ |det\,(C)| &= |z_Q|^3 A \quad \textit{in case of substitution (18)} \end{aligned}$$

where

$$A = |a_1 a_5^2 + a_2 a_6^2 + a_3 a_4^2 - 4 a_1 a_2 a_3 - a_4 a_5 a_6|.$$

The proof of the lemma is direct calculation, using (15). Lemma 3 implies that C is a regular matrix if and only if $A \neq 0$. If C is singular, then it means, that one of x, y, z depends linearly on the other two, whence from (2) we get a system of two quadratic equations in two variables. In this case we can proceed easier. In the following we assume, that C is regular.

We remark, that in case all entries of the matrix C have a non–trivial greatest common divisor d, then at this step we can divide all entries of C with it, by changing k with k/d.

Consider (20) as a system of linear equations in p^2, pq, q^2. Let $C^{-1} = (\bar{c}_{ij}/\det(C))_{1 \leq i,j \leq 4}$ with some integer $\bar{c}_{ij}$. Solving this equation system by Cramer's rule we obtain

$$\begin{aligned} \det(C) \cdot p^2 &= k \cdot (\bar{c}_{11}x + \bar{c}_{12}y + \bar{c}_{13}z) \\ \det(C) \cdot q^2 &= k \cdot (\bar{c}_{31}x + \bar{c}_{32}y + \bar{c}_{33}z) \ . \end{aligned}$$

We obtain, that k divides both terms on the left sides above, and using that p, q are integers with $(p, q) = 1$ we conclude, that $k | \det(C)$.

In the following we have to consider all possible values for k. We remark, that if there are more non–zero values among x_0, y_0, z_0, then in view of Lemma 3 we have to choice that substitution, which makes the determinant of C smaller in absolute value.

In order to reduce the number of possibilities for k, we can check, if the system

$$\begin{aligned} c_{11}p^2 + c_{12}pq + c_{13}q^2 &\equiv 0 \pmod{k} \\ c_{21}p^2 + c_{22}pq + c_{23}q^2 &\equiv 0 \pmod{k} \\ c_{31}p^2 + c_{32}pq + c_{33}q^2 &\equiv 0 \pmod{k} \end{aligned} \tag{21}$$

is solvable in p, q such that the gcd of the residue classes of p and q modulo k is coprime to k.

Now for all possible values of k we substitute the representation (20) obtained for x, y, z into the first or second equation of (2) according as $u_1 \neq 0$ or $u_2 \neq 0$, respectively. Then we get

$$F_i(p, q) = Q_i(f_x(p, q), f_y(p, q), f_z(p, q)) = k^2 u_i \ \text{ in } \ p, q \in \mathbb{Z} \ , \tag{22}$$

where $i = 1$ or 2. This is a homogeneous quartic equation in p, q. F_i can be one of the following types:

- If F_i is irreducible, then (22) is a quartic Thue equation, that can be solved by the known methods (see.e.g.[11], [12]).

- If it is a product of two irreducible quadratic forms, then it can be reduced to a system of two quadratic equations in two variables
- If F_i has one or more linear factors, then (22) can be solved trivial

For all solution p, q of (22) we calculate the corresponding values of x, y, z and we test if (2) holds. We remark, that it can also happen, that (2) admits infinitely many solutions.

3 Index form equations in quartic fields

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. Let $\omega_1 = 1,\ \omega_2,\ \omega_3,\ \omega_4$ be an integral basis of K and denote by $l_i(X, Y, Z)\ \ (i = 1, \ldots, 4)$ the conjugates of the linear form $l(X, Y, Z) = X\omega_2 + Y\omega_3 + Z\omega_4$ over $\mathbb{Q}$. The discriminant of this linear form can be written as

$$D_{K/Q}(X\omega_2+Y\omega_3+Z\omega_4) = \prod_{1\le i<j\le 4} (l_i(X, Y, Z) - l_j(X, Y, Z))^2 = (I(X, Y, Z))^2 D_K$$

where D_K is the discriminant of K and $I(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ is the *index form* corresponding to the integral basis $\omega_1, \ldots, \omega_4$.

As an application of the method described in Section 2, our purpose is now to determine all solutions of the index form equation

$$I(x_0, y_0, z_0) = \pm m \qquad (x_0, y_0, z_0 \in \mathbb{Z}) \tag{23}$$

where m is a positive integer. The smallest m, for which (23) is solvable, is the *minimal index* of K, and the solutions of (23) make it possible to determine all integers in K with index m. In case the minimal index is 1, this way we get all *power integral bases* of K.

The problem of the resolution of index form equations in quartic fields we have already considered in a series of papers [1], [2], [4], [5], [6]. The applicability of these methods depend on the Galois group of the field.

We assume as in [7], that the integral basis of K is presented in the form

$$\omega_i = \frac{1}{d}\sum_{j=1}^{4} w_{ij}\xi^{j-1} \ \ (i = 1, \ldots, 4)$$

with $\omega_1 = 1,\ \ \omega_{ij}, d \in \mathbb{Z}$.

Suppose, that (x_0, y_0, z_0) is a solution of (23). We rewrite $\alpha = x_0\omega_2 + y_0\omega_3 + z_0\omega_4$ in the form

$$\alpha = \frac{a_\alpha + x_1\xi + y_1\xi^2 + z_1\xi^3}{d}$$

where $a_\alpha, x_1, y_1, z_1 \in \mathbb{Z}$ are determined by

$$\begin{pmatrix} a_\alpha \\ x_1 \\ y_1 \\ z_1 \end{pmatrix} = \begin{pmatrix} w_{11} & w_{21} & w_{31} & w_{41} \\ w_{12} & w_{22} & w_{32} & w_{42} \\ w_{13} & w_{23} & w_{33} & w_{43} \\ w_{14} & w_{24} & w_{34} & w_{44} \end{pmatrix} \begin{pmatrix} 0 \\ x_0 \\ y_0 \\ z_0 \end{pmatrix} \tag{24}$$

We make use of Theorem 1 of [7]:

Lemma 4 *Let $i_m = d^6 m/n$, where $n = I(\xi)$. The element $\alpha = x_0\omega_2 + y_0\omega_3 + z_0\omega_4$ is a solution of (23) if and only if there is a solution (u, v) of the cubic equation*

$$F(u,v) = u^3 - a_2u^2v + (a_1a_3 - 4a_4)uv^2 + (4a_2a_4 - a_3^2 - a_1^2a_4)v^3 = \pm i_m \tag{25}$$

such that (x_1, y_1, z_1) of (24) satisfy

$$\begin{aligned} Q_1(x_1,y_1,z_1) &= x_1^2 - x_1y_1a_1 + y_1^2a_2 + x_1z_1(a_1^2 - 2a_2) + y_1z_1(a_3 - a_1a_2) \\ &\quad + z_1^2(-a_1a_3 + a_2^2 + a_4) = u \\ Q_2(x_1,y_1,z_1) &= y_1^2 - x_1z_1 - a_1y_1z_1 + z_1^2a_2 = v \quad . \end{aligned} \tag{26}$$

The form $F(U, V)$ of (25) can be either reducible (if the Galois group of K is solvable, that is C4, V4 or D8, see the remarks in [7]) or irreducible (if the Galois group is S4 or A4). In the reducible case the resolution of (25) is trivial, in the irreducible case (25) is a cubic Thue equation that can be solved easily (cf. e.g. the methods in [11], [12]).

For every solution (u, v) of (25) we want to determine the corresponding solutions (x_1, y_1, z_1) (26). The method described in Section 2 is applicable only if in (26) the variables x_1, y_1, z_1 are coprime. For this purpose we set $d_1 = (x_1, y_1, z_1)$. It follows from (25) and (26) that d_1^2 divides (u, v) and further it d_1^6 divides i_m. Usually there are only very few possible values of d_1. The following procedures should be performed for all these values. Put

$$\begin{aligned} x_2 &= \frac{x_1}{d_1} \\ y_2 &= \frac{y_1}{d_1} \\ z_2 &= \frac{z_1}{d_1} \quad . \end{aligned} \tag{27}$$

Now we have $(x_2, y_2, z_2) = 1$ for the new variables, and by (26)

$$\begin{aligned} Q_1(x_2, y_2, z_2) &= \frac{u}{d_1^2} \\ Q_2(x_2, y_2, z_2) &= \frac{v}{d_1^2} \end{aligned} \tag{28}$$

hold. We build the quadratic form

$$Q_0(X, Y, Z) = uQ_2(X, Y, Z) - vQ_1(X, Y, Z) \tag{29}$$

where

$$\begin{aligned} Q_0(X, Y, Z) &= (-v)X^2 + (-a_2v + u)Y^2 + (a_1a_3v - a_2^2v - a_4v + a_2u)Z^2 \\ &\quad +(a_1v)XY + (-a_3v + a_1a_2v - a_1u)YZ + (-a_1^2v + 2a_2v - u)ZX \quad . \end{aligned}$$

Obviously, we have

$$Q_0(x_2, y_2, z_2) = 0 \ . \tag{30}$$

Following the method of Section 2 we find a non–trivial solution (x_Q, y_Q, z_Q) of (30), that is

$$Q_0(x_Q, y_Q, z_Q) = 0, \tag{31}$$

and depending on the non–zero values among x_Q, y_Q, z_Q we perform one of the following substitutions:

$$\text{if } x_Q \neq 0 \text{ then } \begin{cases} x_2 &= rx_Q \\ y_2 &= ry_Q + p \\ z_2 &= rz_Q + q \end{cases} \tag{32}$$

$$\text{if } y_Q \neq 0 \text{ then } \begin{cases} x_2 &= rx_Q + p \\ y_2 &= ry_Q \\ z_2 &= rz_Q + q \end{cases} \tag{33}$$

$$\text{if } z_Q \neq 0 \text{ then } \begin{cases} x_2 &= rx_Q + p \\ y_2 &= ry_Q + q \\ z_2 &= rz_Q \end{cases} \tag{34}$$

with some rational parameters r, p, q, to get the analogue of (19), that is

$$r(c_1p + c_2q) = c_3p^2 + c_4pq + c_5q^2 \ . \tag{35}$$

As in Section 2 we must consider separately the case when $c_1p + c_2q = 0$. Otherwise we express r from (35) and replace p, q with coprime integer parameters, and we obtain (cf. (20))

$$\begin{aligned} k \cdot x_2 &= f_x(p, q) = c_{11}p^2 + c_{12}pq + c_{13}q^2 \\ k \cdot y_2 &= f_y(p, q) = c_{21}p^2 + c_{22}pq + c_{23}q^2 \\ k \cdot z_2 &= f_z(p, q) = c_{31}p^2 + c_{32}pq + c_{33}q^2 \end{aligned} \tag{36}$$

where k, c_{ij} are integers. Denote by C the matrix with entries $(c_{ij})_{1 \leq i,j \leq 3}$. The analogue of Lemma 2 in this case is

Lemma 5 *For the determinant of the matrix C we have*

$$\begin{aligned} |det\,(C)| &= |x_Q|^3\, i_m \quad \textit{in case of substitution (32)} \\ |det\,(C)| &= |y_Q|^3\, i_m \quad \textit{in case of substitution (33)} \\ |det\,(C)| &= |z_Q|^3\, i_m \quad \textit{in case of substitution (34)} \end{aligned}$$

where i_m is the constant of Lemma 4.

An important consequence of this lemma is that $\det(C) \neq 0$.

As it is shown in Section 2, $k|\det(C)$, moreover, k must survive the test (21). Now for all possible values of k and of d_1 from (26) (27) and (36) we obtain the equations

$$F_1(p,q) = Q_1(f_x(p,q), f_y(p,q), f_z(p,q)) = u_1 \tag{37}$$
$$F_2(p,q) = Q_2(f_x(p,q), f_y(p,q), f_z(p,q)) = v_1 \ . \tag{38}$$

with integer right hand sides

$$u_1 = \frac{k^2 u}{d_1^2}, \qquad v_1 = \frac{k^2 v}{d_1^2}.$$

We want to determine the possible values of $p, q \in \mathbb{Z}$. In case $u \neq 0$ and $v \neq 0$ the two equations (37), (38) are equivalent in view of (29). If $v = 0$, we solve equation (37), otherwise equation (38).

The main goal of the following considerations is to show, that the equations we get are *quartic Thue equations over the same field K*. That means, by the resolution of several quartic Thue equations (corresponding to different values of k, d_1) we do not have to deal with different quartic fields, it sufficies to know the basic data (integral basis, fundamental units) of the original field K. We remark, that these quartic Thue equations can be solved by applying the Baker–Davenport method (see e.g. [11]) or the method described in [12].

Substitute $X = Y - a_1$ in the polynomial $f(X)$ and build a quadratic form from it to get

$$g(Y,Z) = Z^4 f(Y - a_1) = N_{K/Q}(Y - a_1 Z - \xi Z) \ . \tag{39}$$

This form has played an important role already in [7]. Our proof bases on the observation, that in case $v = 0$ the form $F_1(p,q)$ and in case $v \neq 0$ the form $F_2(p,q)$ divides the form $G(p,q) = g(f_y(p,q), f_z(p,q))$ in $\mathbb{Q}[p,q]$. We first discuss some lemmas that we need in our proof, then we consider the cases $v = 0$ and $v \neq 0$ separately.

3.1 Some lemmas

Lemma 6 *If* $(x_Q, y_Q, z_Q) \neq (0,0,0)$ *then* $Q_1(x_Q, y_Q, z_Q)$ *and* $Q_2(x_Q, y_Q, z_Q)$ *can not both vanish.*

Proof. Assume indirect, that both of them vanish. If $z_Q = 0$ then $Q_2(x_Q, y_Q, z_Q) = 0$ implies $y_Q = 0$ and from that by $Q_1(x_Q, y_Q, z_Q) = 0$ we get $x_Q = 0$ which is a contradiction. If $z_Q \neq 0$ then by $Q_2(x_Q, y_Q, z_Q) = 0$

$$x_Q = \frac{y_Q^2 - a_1 y_Q z_Q + a_2 z_Q^2}{z_Q} \quad . \tag{40}$$

Substituting it into $Q_1(x_Q, y_Q, z_Q) = 0$ we obtain

$$y_Q^4 - 3a_1 y_Q^3 z_Q + (a_2 + 3a_1^2) y_Q^2 z_Q^2 + (a_3 - 2a_1 a_2 - a_1^3) y_Q z_Q^3 + (a_1^2 a_2 + a_4 - a_1 a_3) z_Q^4 = 0$$

which yields

$$f\left(\frac{y_Q}{z_Q} - a_1\right) = 0$$

which is agian a contradiction, because f has no rational roots. □

We shall also make use of the following consequences of the above lemma:

Lemma 7 *Assume that* (u, v) *is a solution of (25) and* (x_Q, y_Q, z_Q) *is a non–trivial solution of (31).*
(i) If $y_Q = 0$ *and* $z_Q = 0$ *then* $v = 0$.
(ii) If $v \neq 0$ *then* $Q_2(x_Q, y_Q, z_Q) \neq 0$.

Proof of (i). Under the conditions $y_Q = 0$ and $z_Q = 0$ we have $Q_2(x_Q, y_Q, z_Q) = 0$ whence $Q_1(x_Q, y_Q, z_Q) \neq 0$ by Lemma 6. These imply at once $v = 0$ by (31) which can be written as

$$uQ_2(x_Q, y_Q, z_Q) = vQ_1(x_Q, y_Q, z_Q) \quad .$$

Proof of (ii) If we had $v \neq 0$ and $Q_2(x_Q, y_Q, z_Q) = 0$ then by (31) (see the above equation) we would have $Q_1(x_Q, y_Q, z_Q) = 0$ which is a contradiction by Lemma 6. □

3.2 The case v=0

Now we proceed to the easier case, when in (26) we have $v = 0$.

Theorem 1 *Assume that in (26) $v = 0$ and we use substitution (32), (33) or (34) to obtain the forms $f_x(p, q)$, $f_y(p, q)$, $f_z(p, q)$ as described in (36). Then equation (37) is a quartic Thue equation over K.*

Proof. For simplicity we prove our assertion in case of the substitution (34). It can be proved similarly also for (32), or (33).

Using substitution (34) in case $v = 0$ we obtain

$$f_y(p, q) - a_1 f_z(p, q) - \xi f_z(p, q) = -uq(z_Q p - (y_Q + z_Q \xi)q) \quad .$$

Let now

$$h(p, q) = z_Q p - (y_Q + z_Q \xi)q$$

and compute

$$H(p, q) = N_{K/Q}(h(p, q)) \quad .$$

Using the connection between the roots of $f(x)$ and its coefficients we can express the coefficients of $H(p, q)$ by $y_Q, z_Q, a_1, \ldots, a_4$.

On the other hand consider

$$F_1(p, q) = Q_1(f_x(p, q), f_y(p, q), f_z(p, q)).$$

In case $v = 0$ (31) reduces to $Q_2(x_Q, y_Q, z_Q) = 0$ (obviously $u \neq 0$). Express now x_Q in the form (40) and substitute it into $F_1(p, q)$. We obtain

$$\frac{z_Q^2}{u^2} F_1(p, q) = H(p, q) \quad .$$

Finally, remark that a root of $H(p, 1) = 0$ is $\xi + y_Q/z_Q$ which is a primitive element of K, that means, the form $F_1(p, q)$ is irreducible and has a root in K, that is (37) is a Thue equation over K. □

3.3 The general case $v \neq 0$

For simplicity we restrict ourselves in the following to the substitutions (33), (34). If both $y_Q = 0$ and $z_Q = 0$ then by Lemma 7 (i) we have $v = 0$ and the problem reduces to the easier case of Theorem 1.

Theorem 2 *Assume that in (26) $v \neq 0$ and we use substitution (33) or (34) to obtain the forms $f_x(p,q)$, $f_y(p,q)$, $f_z(p,q)$ as described in (36). Then equation (38) is a quartic Thue equation over K.*

Proof We prove the assertion in case of the substitution (34). The case (33) can be dealt with similarly.

I. First we prove that a root of $F_2(p,q)$ is in K. Consider again

$$f_y(p,q) - a_1 f_z(p,q) - \xi f_z(p,q) = t_2 p^2 + t_1 pq + t_0 q^2 \tag{41}$$

where in the present case

$$\begin{aligned} t_2 &= v(y_Q - z_Q a_1 - z_Q \xi) \\ t_1 &= -2vx_Q + 2va_2 z_Q - uz_Q + va_1 z_Q \xi \\ t_0 &= va_1 x_Q - va_2 y_Q + uy_Q - va_3 z_Q + uz_Q \xi - va_2 z_Q \xi \end{aligned}$$

We remark, that here obviously $t_2 \neq 0$. Our purpose is to factorize the above form (41) over K. We have to show, that the discriminant of the second degree equation in (41) is a square in K. The discriminant is

$$D = t_1^2 - 4t_2 t_0 \quad .$$

By adding $4vQ_0(x_Q, y_Q, z_Q) = 0$ to D we can eliminate from it not only the term containing x_Q^2, but also all other terms containing x_Q or y_Q or y_Q^2 and we obtain

$$D = z_Q^2((v^2 a_1^2 - 4v^2 a_2 + 4uv)\xi^2 + (2uva_1 - 4v^2 a_3)\xi + u^2 - 4v^2 a_4) \quad .$$

Add now $4v^2 z_Q^2 f(\xi) = 0$ to D to have

$$D = (z_Q(2v\xi^2 + va_1\xi + u))^2$$

as we wanted to show. We conclude, that the form in (41) can be factorized over K as

$$t_2 p^2 + t_1 pq + t_0 q^2 = t_2(p - \rho_1 q)(p - \rho_2 q) \tag{42}$$

where

$$\rho_1 = \frac{-t_1 - \sqrt{D}}{2t_2} \quad \rho_2 = \frac{-t_1 + \sqrt{D}}{2t_2} \quad .$$

Let now

$$h(p,q) = \frac{1}{v} t_2(p - \rho_1 q) = \frac{1}{v}\left(t_2 p + \frac{t_1 + \sqrt{D}}{2} q\right) =$$

$$= z_Q q\xi^2 + (-z_Q p + z_Q a_1 q)\xi + y_Q p - z_Q a_1 p - x_Q q + z_Q a_2 q \quad .$$

Our next purpose is to demonstrate, that the form

$$H(p,q) = N_{K/Q}(h(p,q))$$

is up to a constant factor the same as $F_2(p,q)$ in (38). Using the connection between the roots and the coefficients of $f(x)$ we calculate the coefficients of $H(p,q)$. These coefficients do not depend on u, v only on $x_Q, y_Q, z_Q, a_1, \ldots, a_4$.

On the other hand consider $F_2(p,q)$. By Lemma 7 (ii) in case $v \neq 0$ we have $Q_2(x_Q, y_Q, z_Q) \neq 0$, hence from (31) we can express v in the form

$$v = u\frac{Q_1(x_Q, y_Q, z_Q)}{Q_2(x_Q, y_Q, z_Q)} \quad .$$

Substitute it into $F_2(p,q)$, multiply it with $Q_2(x_Q, y_Q, z_Q)$ and divide by v^2. The result is just $H(p,q)$. That means, $F_2(p,q)$ has a root in K.

II. Finally, we have to show, that the root ρ_1 of $F_2(p,q)$ is a primitive element of K, which would imply that $F_2(p,q)$ is irreducible, that is (38) is a Thue equation over K.

We have

$$\rho_1 = \frac{x_Q - z_Q a_2 - z_Q a_1 \xi - z_Q \xi^2}{y_Q - z_Q a_1 - z_Q \xi} \quad .$$

This element can not be rational, because then ξ would be a root of a second degree polynomial, which is impossible. We also have to exclude the possibility, that it were a second degree element.

Assume indirect, that it is a second degree element. Then there must be rational numbers b, c such that

$$\rho_1^2 + b\rho_1 + c = 0 \quad .$$

Multiplying with the square of the dominator of ρ_1 we get a polynomial equation of degree 4 for ξ. We can eliminate the coefficient of ξ^4 by using $f(\xi) = 0$. Then the remainding cubic polynomial in ξ must be trivial, that is all coefficients must be 0. We eliminate the variable b by using the coefficient of ξ^3 and c by

using the coefficient of ξ^2. There remaind two more equations, the coefficient C_1 of ξ and the constant term C_0 must also vanish. C_1 is a quadratic form, C_0 is a cubic form in x_Q, y_Q, z_Q, that depend also on the coefficients $a_1, \ldots, a_4$ of $f(x)$. Moreover, we can also make use of the equation (31).

In the following we denote by $R(f_1, f_2, X)$ the resultant of two polynomials f_1, f_2 with respect to the variable X.

We build $T_1 = R(C_1, C_0, x_Q)$, $T_2 = R(C_1, Q_0, x_Q)$, finally $T_3 = R(T_1, T_2, y_Q)$. Factorizing the result we obtain

$$T_3 = -z_Q^{20}(-a_1^3 - 8a_3 + 4a_1a_2)^4 D(f)F(u,v) \quad .$$

Here $z_Q \neq 0$, the discriminant $D(f)$ of $f(x)$ and $F(u,v)$ are also obviously non–zero.

We still have to consider the case, when

$$a_3 = \frac{-a_1^3 + 4a_1a_2}{8} \tag{43}$$

We remark, that in this case

$$F(u,v) = 2^{-6}(4u + va_1^2 - 4va_2)(16u^2 - 4a_1^2uv + 4a_1^2a_2v^2 - a_1^4v^2 - 64a_4v^2) \tag{44}$$

which, in view of our remarks in [7] yields, that K has a quadratic subfield. In this case, proceeding in the same way as above we get

$$C_1 = (3a_1z_Q - 4y_Q)(3a_1^2z_Q - 4a_2z_Q - 4a_1y_Q + 8x_Q) = 0 \quad . \tag{45}$$

(A) Now if in (45) the first factor is 0, that is

$$y_Q = \frac{3a_1z_Q}{4}$$

then

$$R(C_0, Q_0, x_Q) = 2^{-12}z_Q^6(16a_1^2a_2 - 5a_1^4 - 256a_4)(16u^2 - 4a_1^2uv + 4a_1^2a_2v^2 - a_1^4v^2 - 64a_4v^2)$$

Here the last factor is the second factor of (44) which is non–zero. If

$$a_4 = \frac{16a_1^2a_2 - 5a_1^4}{256}$$

then this condition together with (43) results a reducible polynomial f, which is impossible.

(B) Now if in (45) the second factor is 0, that is

$$x_Q = \frac{4a_1y_Q + 4a_2z_Q - 3a_1^2z_Q}{8}$$

then $C_0 = 0$ implies

$$a_4 = \frac{a_1^4 + 16a_2^2 - 8a_1^2a_2}{64}$$

which together with (43) gives again a reducible polynomial f, which is impossible. □

Remarks

(i) In the proofs of Theorem 1 and Theorem 2 we used the computer algebra system MAPLE. Especially in the proof of Theorem 2 it would have been hardly possible to compute the resultants T_1, T_2, T_3 and to factorize T_3 without MAPLE.

(ii) The assertion of Theorem 2 holds very probably also in case (32), but the formulas became much more complicated. Part I of the above proof can also be performed in case of (32), but in Part II it is impossible even with MAPLE to build the final resultant T_3 because of the complicated formulas.

4 Numerical examples

We illustrate our method by computing the minimal index and all elements of minimal index in some quartic fields. In [7] we have already given extensive lists of minimal indices and elements of minimal index in quartic fields of different signatures. Our purpose here is to make an impresson on what kind of Thue equations are to be solved by applying our method described in Section 3. In our examples we deal with totally real fields with Galois group S_4 or A_4, as they are considered as the most interesting examples.

In the following we make use of the field index $I(K)$ of K, which is the greatest common divisor of the indices of all primitive integral elements in K. $I(K)$ is easy to calculate (cf. [3]) and the minimal index must be divisible by it, which makes the calculations often faster.

In our examples we list the discriminant D_K of the field $K = \mathbb{Q}(\xi)$, the defining polynomial $f(x)$ of ξ, the signature, the Galois group, the integral basis of K, the index n of ξ and the field index $I(K)$ of K. Then we consider the values of m divisable by $I(K)$. The minimal index is the smallest value of m for which we obtain solutions of the index form equation (23). For each m we give the cubic equation $F(u, v) = i_m$ (25) and for all solutions (u, v) of it we list a non–trivial solution (x_Q, y_Q, z_Q) of (31). We indicate which substitution of (32), (33), (34) we applied, and we display the determinant $\det(C)$ (cf. Lemma 5). Then follows either the form $F_1(p, q)$ or $F_2(p, q)$ ((37) or (38)), the possible values of k and d_1 (cf. (27)). For all possible pair k, d_1 we give the

right hand side u_1 or v_1 of (37) or (38), respectively, and we list the solutions of the equation together with the corresponding solutions of (23) in the form $(p, q) : (x_0, y_0, z_0)$.

References

[1] 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.

[2] 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.

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

[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 in biquadratic number fields, IV. The dihedral case*, to appear.

[6] 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.

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

[8] K.Győry, *Sur les polynomes á coefficients entiers et de discriminant donné, III.*, Publ. Math. (Debrecen), **23**(1976), 141–165.

[9] T.Nagell, *Sur les discriminants des nombres algébriques*, Arkiv för Math., **7** (1967), 265–282.

[10] L.J.Mordell, Diophantine Equations, Academic Press, New York–London, 1969.

[11] A.Pethő und R.Schulenberg, *Effectives Lösen von Thue Gleichungen*, Publ. Math. (Debrecen), **34** (1987), 189–196.

[12] N.Tzanakis and B.M.M.de Weger, *On the practical solution of the Thue equation*, J.Number Theory, **31** (1989), 99–132.

EXAMPLE 1

$D_K = 1957, f(x) = x^4 - 4x^2 - x + 1$, totally real, Galois group S_4
integral basis $\{1, \xi, \xi^2, \xi^3\}, n = 1, I(K) = 1$
$m = 1, F(u,v) = u^3 + 4u^2v - 4uv^2 - 17v^3 = \pm 1$
$(u,v) = (1,0), (x_Q, y_Q, z_Q) = (1,0,0)$, substitution (16), $\det(C) = 1$
$F_1(p,q) = p^4 - 4p^2q^2 - pq^3 + q^4$
possible values: $k = 1, d_1 = 1$
$k = 1, d_1 = 1, u_1 = \pm 1$ (1,0):(1,0,0), (–1,1):(–3,–1,1), (0,1):(–4,0,1), (2,1):(0,2,1)
$(u,v) = (-4,1), (x_Q, y_Q, z_Q) = (0,-1,0)$, substitution (17), $\det(C) = 1$
$F_2(p,q) = p^4 + 8p^3q + 18p^2q^2 + 7pq^3 - 3q^4$
possible values: $k = 1, d_1 = 1$
$k = 1, d_1 = 1, v_1 = \pm 1$ (1,0):(0,1,0), (–4,1):(–4,1,1), (–1,1):(–1,–2,1), (–7,2):(–14,–3,4), (1,4):(4,33,16)
$(u,v) = (-2,1), (x_Q, y_Q, z_Q) = (2,1,-1)$, substitution (17), $\det(C) = 1$
$F_2(p,q) = p^4 + 15p^3q + 76p^2q^2 + 154pq^3 + 101q^4$
possible values: $k = 1, d_1 = 1$
$k = 1, d_1 = 1, v_1 = \pm 1$ (1,0):(–4,–1,1), (–3,1):(3,0,–1), (–7,2):(–2,–1,1), (–10,3):(8,–1,–2)
$(u,v) = (2,1), (x_Q, y_Q, z_Q) = (5,0,-1)$, substitution (18), $\det(C) = 1$
$F_2(p,q) = p^4 - p^3q - 12p^2q^2 + 6pq^3 + 37q^4$
possible values: $k = 1, d_1 = 1$
$k = 1, d_1 = 1, v_1 = \pm 1$ (1,0):(–5,0,1), (–2,1):(8,1,–2), (3,1):(–12,1,3), (–7,3):(4,9,-5)

EXAMPLE 2

$D_K = 2777, f(x) = x^4 - x^3 - 4x^2 + x + 2$, totally real, Galois group S_4
integral basis $\{1, \xi, \xi^2, \xi^3\}, n = 1, I(K) = 1$
$m = 1, F(u,v) = u^3 + 4u^2v - 9uv^2 - 35v^3 = \pm 1$
$(u,v) = (1,0), (x_Q, y_Q, z_Q) = (1,0,0)$, substitution (16), $\det(C) = 1$
$F_1(p,q) = p^4 + 3p^3q - p^2q^2 - 6pq^3 - q^4$
possible values: $k = 1, d_1 = 1$
$k = 1, d_1 = 1, u_1 = \pm 1$ (1,0):(1,0,0), (–2,1):(–2,–2,1), (0,1):(–4,0,1), (–5,2):(–1,–10,4)
$(u,v) = (-4,1), (x_Q, y_Q, z_Q) = (0,-1,0)$, substitution (17), $\det(C) = 1$
$F_2(p,q) = p^4 + 8p^3q + 19p^2q^2 + 13pq^3 + 2q^4$
possible values: $k = 1, d_1 = 1$
$k = 1, d_1 = 1, v_1 = \pm 1$ (1,0):(–1,1,0), (–3,1):(–6,–3,2), (–1,1):(0,–1,0)
$(u,v) = (-3,1), (x_Q, y_Q, z_Q) = (1,-1,-1)$, substitution (16), $\det(C) = 1$
$F_2(p,q) = -p^4 + 3p^3q + 9p^2q^2 - 38pq^3 + 31q^4$
possible values: $k = 1, d_1 = 1$

$k = 1, d_1 = 1, v_1 = \pm 1$ (1,0):(1,2,–1), (2,1):(–3,–1,1), (5,2):(–3,–2,1), (8,3):(1,–1,–1)

$(u, v) = (3, 1), (x_Q, y_Q, z_Q) = (5, 1, -1)$, substitution (17), $\det(C) = 1$

$F_2(p, q) = 2p^4 + 47p^3q + 393p^2q^2 + 1372pq^3 + 1697q^4$

possible values: $k = 1, d_1 = 1$

$k = 1, d_1 = 1, v_1 = \pm 1$ (–8,1):(5,1,–1), (–4,1):(21,1,–5)

$(u, v) = (-33, 8), (x_Q, y_Q, z_Q) = (0, -4, 1)$,substitution (18),$\det(C) = 1$

$F_2(p, q) = 8(71p^4 + 185p^3q + 144p^2q^2 + 31pq^3 + 2q^4)$

possible values: $k = 1, d_1 = 1$

$k = 1, d_1 = 1, v_1 = \pm 8$ (–1,1):(6,–2,–1), (–1,7):(0,4,–1)

EXAMPLE 3

$D_K = 15188, f(x) = x^4 - x^3 - 7x^2 + x + 2$, totally real, Galois group S_4

integral basis $\{1, \xi, \xi^2, (\xi + \xi^3)/2\}, n = 2, I(K) = 1$

$m = 1, F(u, v) = u^3 + 7u^2v - 9uv^2 - 59v^3 = \pm 32$

$(u, v) = (-14, 2), (x_Q, y_Q, z_Q) = (0, -1, 0)$, substitution (17), $\det(C) = 4$

$F_2(p, q) = p^4 + 14p^3q + 52p^2q^2 + 22pq^3 - q^4$

possible values: $k = 1, 2, 4, d_1 = 1$

$k = 1, d_1 = 1, v_1 = \pm 2$ no solutions

$k = 2, d_1 = 1, v_1 = \pm 8$ (–7,1):(–12,–1,3)

$k = 4, d_1 = 1, v_1 = \pm 32$ no solutions

$(u, v) = (-6, 2), (x_Q, y_Q, z_Q) = (3, 2, -1)$, substitution (18), $\det(C) = 4$

$F_2(p, q) = 2(p^4 + 11p^3q + 33p^2q^2 + 19pq^3 - 26q^4)$

possible values: $k = 1, 2, d_1 = 1$

$k = 1, d_1 = 1, v_1 = \pm 2$ (1,0):(–4,–1,1), (–5,2):(2,1,–1)

$k = 2, d_1 = 1, v_1 = \pm 8$ (–2,1):(no corresponding solution)

$(u, v) = (6, 2), (x_Q, y_Q, z_Q) = (3, -4, 1)$, substitution (18), $\det(C) = 4$

$F_2(p, q) = 2(11p^4 + 119p^3q + 447p^2q^2 + 649pq^3 + 248q^4)$

possible values: $k = 1, 2, d_1 = 1$

$k = 1, d_1 = 1, v_1 = \pm 2$ (–37,10):(1,–2,1)

$k = 2, d_1 = 1, v_1 = \pm 8$ (–4,1):(no corresponding solution)

EXAMPLE 4

$D_K = 157609, f(x) = x^4 - 13x^2 - 2x + 19$, totally real, Galois group A_4

integral basis $\{1, \xi, (1 + \xi + \xi^2)/2, (1 + \xi^3)/2\}, n = 4, I(K) = 2$

$m = 2, F(u, v) = u^3 + 13u^2v - 76uv^2 - 992v^3 = \pm 32$

$(u, v) = (-26, 2), (x_Q, y_Q, z_Q) = (0, -1, 0)$,substitution (17),$\det(C) = 4$