Acta Mathematica et Informatica Universitatis Ostraviensis

István Járási

Computing all elements of given index in sextic fields with a cubic subfield

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 10 (2002), No. 1, 49--59

Persistent URL: http://dml.cz/dmlcz/120585

Acta Mathematica et Informatica Universitatis Ostraviensis 10 (2002) 49–59

Computing all elements of given index in sextic fields with a cubic subfield

István Járási

Abstract. There are no general methods for calculating elements of given index in sextic fields. This problem was investigated only in sextic fields having quadratic subfields.

In the present paper we give an algorithm to compute all elements of given index in sextic fields containing a cubic subfield. To illustrate the method we give a detailed example in the last section.

1. Introduction

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

$$I(\alpha) = (\mathbb{Z}_K : \mathbb{Z}[\alpha]).$$

It is a classical problem in algebraic number theory to determine all elements of $\mathbb{Z}_K$ of given index. It is obvious that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is an integral basis, if and only if $I(\alpha) = 1$. Such an integral basis is called *power integral basis*. If there exists such an $\alpha \in \mathbb{Z}_K$, then $\mathbb{Z}_K$ is called *monogene*.

Let $\{1, \omega_2, \ldots, \omega_n\}$ be an arbitrary integral basis in K. Then the discriminant of the linear form $l(x) = x_2\omega_2 + \ldots + x_n\omega_n$ can be written as

$$D(l(x)) = (I(x_2, \ldots, x_n))^2 \cdot D_K \tag{1.1}$$

where $I(x_2, \ldots, x_n)$ is the *index form* corresponding to the integral basis $\{1, \omega_2, \ldots, \omega_n\}$, and D_K is the discriminant of the field K. This index form has the property that for an arbitrary primitive element

$$\alpha = x_1 + x_2\omega_2 + \ldots + x_n\omega_n \in \mathbb{Z}_K$$

the equation

$$I(\alpha) = |I(x_2, \ldots, x_n)|$$

Received: January 31, 2002.
2000 *Mathematics Subject Classification:* 11Y50, 11D57.
Key words and phrases: index form equations, sextic fields, power integral bases.

holds. Consequently, the index of a primitive $\alpha \in \mathbb{Z}_K$ can be determined by

$$I(\alpha) = \frac{\prod_{1 \le i < j \le n} |\alpha^{(i)} - \alpha^{(j)}|}{\sqrt{|D_K|}} \tag{1.2}$$

where $\alpha^{(i)}$ $(1 \le i \le n)$ denote the conjugates of α. So the problem of determining all elements of $\mathbb{Z}_K$ of given index g is equivalent to solving the *index form equation*

$$I(x_2, \dots, x_n) = \pm g \quad (x_2, \dots, x_n \in \mathbb{Z}).$$

For an arbitrary $z \in \mathbb{Z}$ the indices of $\pm\alpha + z$ are the same. These numbers are called *equivalent*. In 1976 K.Győry [10] proved in an effective form that an index form equation has only finitely many solutions, that is up to equivalence there are only finitely many elements of $\mathbb{Z}_K$ of given index. For related results on power integral bases and algorithms for solving index form equations see Győry [11] and Gaál [6].

In this paper we consider sextic fields. There are no general effective algorithms for solving index form equations in sextic fields. The only case when algorithms for determining all elements of given index were formerly described is the case of sextic fields with a quadratic subfield, cf. I.Gaál [4],[5] and I.Gaál and M.Pohst [8]. In this case the index form equation implies a relative Thue equation over the quadratic subfield which makes the resolution easier.

Our purpose is to consider sextic fields having a cubic subfield. This case was partially investigated by the author in [12] where an algorithm is given to compute generators of power integral bases having "small" coordinates in an integral basis. In this case the index form equation is much more complicated than in the previously considered sextic fields but using the ideas of I.Gaál and K.Győry [7] and the method of Wildanger [13], [14] for the enumeration of the "small" values of the exponents in unit equations, it can be solved within reasonable time. In this paper we give a feasible algorithm for the *complete* resolution of index form equations in such fields. Using standard arguments we reduce the index form equation to unit equations in two variables. These unit equations are solved by using the reduction method and enumeration method described by Gaál and Pohst [9]. This enumeration method is based on K. Wildanger's ideas, cf. [13], [14]. Below we consider in detail the most difficult case when the sextic field is totally real and has the largest possible Galois group $S_4 \times C_2$.

2. The unit equation

Let K be a totally real sextic field with a cubic subfield M and with Galois group $S_4 \times C_2$. Denote by $\mathbb{Z}_K$ the ring of integers of K, and by D_K its discriminant. Similarly, let $\mathbb{Z}_M$ be the ring of integers of M, and D_M its discriminant. Let ϱ be a primitive integral element of M, and let ϑ be a primitive integral element of K. For simplicity we assume that any $\alpha \in \mathbb{Z}_K$ can be represented in the form of

$$\alpha = x_0 + x_1\varrho + x_2\varrho^2 + y_0\vartheta + y_1\varrho\vartheta + y_2\varrho^2\vartheta,$$

with $x_i, y_i \in \mathbb{Z}$. Note that otherwise in this representation a common denominator d appears. In such cases the same arguments work but instead of g we have $g \cdot d^{15}$ on the right side of (2.1).

Let $\varrho^{(i)}$ $(i = 1,2,3)$ denote the conjugates of ϱ. Similarly, we will use the notation $M^{(i)} = \mathbb{Q}(\varrho^{(i)})$, $i = 1,2,3$. Let $\vartheta^{(i1)}, \vartheta^{(i2)}$ denote the conjugates of ϑ over $M^{(i)}$ $(i = 1,2,3)$, respectively. Let $K^{(ip)} = \mathbb{Q}(\vartheta^{(ip)})$, $i = 1,2,3$, $p = 1,2$. Then the conjugates of α are

$$\alpha^{(ip)} = x_0 + x_1\varrho^{(i)} + x_2(\varrho^{(i)})^2 + y_0\vartheta^{(ip)} + y_1\varrho^{(i)}\vartheta^{(ip)} + y_2(\varrho^{(i)})^2\vartheta^{(ip)}$$

for $1 \le i \le 3, 1 \le p \le 2$. Here we note that since for $p = 1,2$ $M^{(i)} \subset K^{(ip)}$ holds, one can express an arbitrary $\alpha^{(ip)} \in \mathbb{Z}_{K^{(ip)}}$ in terms of powers of the $\vartheta^{(ip)}$-s and rational integers.

Our purpose is to determine all solutions of the equation

$$I(\alpha) = g \ (\alpha \in \mathbb{Z}_K) \tag{2.1}$$

for a fixed $g \in \mathbb{Z}$. For

$$1 \le i,j \le 3 \ , \ 1 \le p,q \le 2 \ , \ (i,p) \ne (j,q)$$

consider the linear forms

$$\begin{aligned} l^{(ip,jq)}&(x_1,x_2,y_0,y_1,y_2) = \\ &= (\varrho^{(i)} - \varrho^{(j)})x_1 + ((\varrho^{(i)})^2 - (\varrho^{(j)})^2)x_2 + \\ &+ (\vartheta^{(ip)} - \vartheta^{(jq)})y_0 + (\varrho^{(i)}\vartheta^{(ip)} - \varrho^{(j)}\vartheta^{(jq)})y_1 + ((\varrho^{(i)})^2\vartheta^{(ip)} - (\varrho^{(j)})^2\vartheta^{(jq)})y_2. \end{aligned}$$

Using (1.2) and this notation, (2.1) can be written as

$$\prod l^{(ip,jq)}(x_1,x_2,y_0,y_1,y_2) = \pm g\sqrt{|D_K|}, \tag{2.2}$$

where the product extends to the tuples (ip,jq) where $(i,p) \prec (j,q)$ in the lexicographical order. When we reduce an index form equation to unit equations, we use the above defined linear forms. In this case we assume a cubic subfield, so we can have several types of unit equations depending on the choice of the linear forms. For $\{i,j,k\} = \{1,2,3\}$ and $1 \le p,q,r \le 2$ Siegel's-identity gets the form

$$l^{(ip,jq)} + l^{(jq,kr)} + l^{(kr,ip)} = 0 \tag{2.3}$$

in the variables (x_1,x_2,y_0,y_1,y_2).

Since the Galois group of the cubic subfield M is not cyclic (this is satisfied in our case, otherwise the Galois group of K has at most 24 elements), there is an automorphism of the Galois group of M interchanging $\varrho^{(i)}$ and $\varrho^{(j)}$ $(i \ne j)$. In view of the arguments of the Proof of Theorem 1 of [12], this can be extended to an automorphism of the Galois group of K, interchanging $\vartheta^{(ip)}$ and $\vartheta^{(jq)}$. This isomorphism leaves $L^{(ip,jq)} = \mathbb{Q}(\vartheta^{(ip)} + \vartheta^{(jq)}, \vartheta^{(ip)}\vartheta^{(jq)})$ fixed, hence it is a proper subfield of $K^{(ip)}K^{(jq)}$ which is also a proper subfield of the normal closure of K of degree $\#(S_4 \times C_2) = 48$. Hence the degree of $L^{(ip,jq)}$ cannot exceed 12, so its unit rank is ≤ 11. (Note that in the totally real case under consideration this maximum is reached.) This idea was first used by Gaál and Győry [7].

Let $\alpha = x_0 + x_1\varrho + x_2\varrho^2 + y_0\vartheta + y_1\varrho\vartheta + y_2\varrho^2\vartheta$ be a solution of (2.1), and

$$\delta^{(ip,jq)} = \frac{\alpha^{(ip)} - \alpha^{(jq)}}{\vartheta^{(ip)} - \vartheta^{(jq)}}.$$

It is easy to see that there is an integer $d \in \mathbb{Z}$ such that arbitrary $\alpha \in \mathbb{Z}_K$ can be represented in the form of

$$\alpha = \frac{z_0 + z_1\vartheta + z_2\vartheta^2 + z_3\vartheta^3 + z_4\vartheta^4 + z_5\vartheta^5}{d}$$

where $z_i \in \mathbb{Z}$ for $i = 0, \ldots, 5$. (If $I(\vartheta) = 1$ then $d = 1$). Hence $d\delta^{(ip,jq)}$ will be an integer in $L^{(ip,jq)}$.

Using this notations (2.2) can be written as

$$\prod d\delta^{(ip,jq)} = \frac{\pm g d^{15}}{I(\vartheta)}, \tag{2.4}$$

where the product is taken for the same tuples (ip, jq) as (2.2). Again using the arguments of the Proof of Theorem 1 of [12] it is easy to see that there exists an automorphism of the Galois group of K mapping $\vartheta^{(ip)}$ to $\vartheta^{(kr)}$ and simultaneously $\vartheta^{(jq)}$ to $\vartheta^{(ls)}$, if $1 \leq k, l \leq 3, k \neq l, 1 \leq r, s \leq 2$. (For this observe that k or l is equal to i or j and recall that the Galois group of M is not cyclic.) This automorphism maps $\delta^{(ip,jq)}$ to $\delta^{(kr,ls)}$. Thus equation (2.4) is a norm equation in $L^{(ip,jq)}$, so there exist an integer $\gamma^{(ip,jq)}$ of norm $\frac{\pm g d^{15}}{I(\vartheta)}$ and a unit $\eta^{(ip,jq)} \in L^{(ip,jq)}$ such that

$$d\delta^{(ip,jq)} = \eta^{(ip,jq)}\gamma^{(ip,jq)}.$$

Note that the following computations must be performed for a complete set of non-associate integral elements γ of $L^{(ip,jq)}$ of norm $\frac{\pm g d^{15}}{I(\vartheta)}$, which can be determined e.g. by KASH [2]. Let

$$\beta^{(ip,jq,kr)} = \frac{\gamma^{(ip,jq)}\left(\vartheta^{(ip)} - \vartheta^{(jq)}\right)}{\gamma^{(ip,kr)}\left(\vartheta^{(ip)} - \vartheta^{(kr)}\right)}.$$

Using this and (2.3) we have

$$\beta^{(ip,jq,kr)}\frac{\eta^{(ip,jq)}}{\eta^{(ip,kr)}} + \beta^{(kr,jq,ip)}\frac{\eta^{(kr,jq)}}{\eta^{(kr,ip)}} = 1. \tag{2.5}$$

Since the η-s are conjugated to each other, and they lie in a totally real field of degree 12, the number of unknown exponents in this unit equation is 11.(Here note again that in this paper we deal with the most difficult case i.e. when the degree of $L^{(ip,jq)}$) is exactly 12 and it is also a totally real field, so it has 11 fundamental units. Generaly there are less then 11 fundamental units, because the degree of $L^{(ip,jq)}$) is at most 12)

Denote by $\{\varepsilon_1, \ldots, \varepsilon_{11}\}$ a set of fundamental units of $L^{(ip,jq)}$. Let $\{i, j, k\} = \{1, 2, 3\}$ and $1 \leq p, q, r \leq 2$. Then there are rational integers $a_1, \ldots, a_{11}$ such that

$$\eta^{(ip,jq)} = \pm\left(\varepsilon_1^{(ip,jq)}\right)^{a_1} \cdot \ldots \cdot \left(\varepsilon_{11}^{(ip,jq)}\right)^{a_{11}}.$$

Introducing

$$\nu_h^{(ip,jq,kr)} = \frac{\varepsilon_h^{(ip,jq)}}{\varepsilon_h^{(ip,kr)}} \qquad (h = 1, \dots, 11),$$

$$\mu^{(ip,jq,kr)} = \prod_{h=1}^{11} \left(\nu_h^{(ip,jq,kr)}\right)^{a_h}$$

and

$$\xi^{(ip,jq,kr)} = \beta^{(ip,jq,kr)}\mu^{(ip,jq,kr)},$$

by (2.5) we have

$$\beta^{(ip,jq,kr)}\left(\nu_1^{(ip,jq,kr)}\right)^{a_1} \cdot \dots \cdot \left(\nu_{11}^{(ip,jq,kr)}\right)^{a_{11}} +$$
$$+ \beta^{(kr,jq,ip)}\left(\nu_1^{(kr,jq,ip)}\right)^{a_1} \cdot \dots \cdot \left(\nu_{11}^{(kr,jq,ip)}\right)^{a_{11}} = 1,$$

or simply

$$\xi^{(ip,jq,kr)} + \xi^{(kr,jq,ip)} = 1.$$

and this unit equation can be solved using Baker's method, reduction procedures and Wildanger's enumeration method. This procedure was first described by Gaál and Pohst [9].

After solving this equation in the variables $a_1, \dots, a_{11}$ one has to consider the system of linear equations

$$(2.6)\quad l^{(ip,jq)}(x_1, x_2, y_0, y_1, y_2) = \pm(\vartheta^{(ip)} - \vartheta^{(jq)})\gamma^{(ip,jq)}\left(\varepsilon_1^{(ip,jq)}\right)^{a_1} \cdot \dots \cdot \left(\varepsilon_{11}^{(ip,jq)}\right)^{a_{11}}$$

for all possible indices, and solving this it is easy to calculate x_1, x_2, y_0, y_1, y_2.

3. Baker's method

Taking logarithms for each possible indices we have

$$a_1 \log\left|\nu_1^{(ip,jq,kr)}\right| + \dots + a_{11} \log\left|\nu_{11}^{(ip,jq,kr)}\right| = \log\left|\mu^{(ip,jq,kr)}\right|$$

One can consider the above equations (for each possible indices) as a system of linear equations in $a_1, \dots, a_{11}$. The matrix of this system of linear equations has linearly independent columns, cf. [7]. Hence one can select eleven tuples (ip, jq, kr) of indices such that the coefficient matrix M of the left hand side will have rank 11. Let (i_0p, j_0q, k_0r) be the index for which $\left|\log|\mu^{(ip,jq,kr)}|\right|$ attains its maximum. Then by multiplication by the inverse of M one can express the variables $a_1, \dots, a_{11}$, and we conclude

$$A = \max_{1 \le h \le 11} |a_h| \le c_1 \left|\log\left|\mu^{(i_0p,j_0q,k_0r)}\right|\right|,$$

where c_1 denotes the row norm of M^{-1}, that is, the maximum sum of the absolute values of the elements in the rows of M^{-1}. Note that M should be chosen such that c_1 becomes as small as possible. Now if $|\mu^{(i_0p,j_0q,k_0r)}| < 1$ then $\log|\mu^{(i_0p,j_0q,k_0r)}| \le -A/c_1$, and if $|\mu^{(i_0p,j_0q,k_0r)}| > 1$ then the same holds for $\mu^{(i_0p,k_0q,j_0r)} = 1/\mu^{(i_0p,j_0q,k_0r)}$. Hence we conclude that

$$(3.1)\qquad \left|\mu^{(i_0p,j_0q,k_0r)}\right| < \exp(-\frac{A}{c_1})$$

for a certain index. Set $c_2 = |\beta^{(i_0p,j_0q,k_0r)}|$. Then using the inequality $|\log x| \leq 2|x-1|$ holding for $|x-1| < 0.795$, we have

$$\begin{aligned}
&\left|\log|\beta^{(k_0r,j_0q,i_0p)}| + a_1 \log|\nu_1^{(k_0r,j_0q,i_0p)}| + \cdots + a_{11} \log|\nu_{11}^{(k_0r,j_0q,i_0p)}|\right| = \\
&\quad = \left|\log|\beta^{(k_0r,j_0q,i_0p)}\mu^{(k_0r,j_0q,i_0p)}|\right| \leq \\
&\quad \leq 2\left|1 - |\beta^{(k_0r,j_0q,i_0)}\mu^{(k_0r,j_0q,i_0p)}|\right| \leq \\
&\quad \leq 2\left|1 - \beta^{(k_0r,j_0q,i_0p)}\mu^{(k_0r,j_0q,i_0p)}\right| = \\
&\quad = 2\left|\beta^{(i_0p,j_0q,k_0r)}\mu^{(i_0p,j_0q,k_0r)}\right| \leq \\
&\quad \leq 2c_2 \exp(-A/c_1),
\end{aligned}$$

provided that the right hand side is $< 0,795$, but in the opposite case we get a much better estimate for A. In our example the terms in the above linear form in logarithms were linearly independent over $\mathbb{Q}$, so we can apply the estimates of Baker and Wüstholz [1] to derive a lower estimate

$$\left|\log|\beta^{(k_0r,j_0q,i_0p)}| + a_1 \log|\nu_1^{(k_0r,j_0q,i_0p)}| + \cdots + a_{11} \log|\nu_{11}^{(k_0r,j_0q,i_0p)}|\right| > \\ > \exp(-C_0 \log A),$$

with a large constant C_0. This inequality compared with (3.1) implies an upper bound A_0 for A. In our example we got $A_0 = 10^{104}$.

4. LLL reduction of Baker's bound

For a fixed index (ip, jq, kr) consider the lattice L spanned by the columns of the 13 by 12 matrix

$$\begin{pmatrix}
1 & 0 & \cdots & 0 \\
0 & 1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 1 \\
C\log|\beta^{(kr,jq,ip)}| & C\log|\nu_1^{(kr,jq,ip)}| & \cdots & C\log|\nu_{11}^{(kr,jq,ip)}|
\end{pmatrix}$$

where the constant C will be specified later. Denote by b_1 the first vector of the LLL reduced basis of L. Now Lemma 1 of Gaál and Pohst [9] cf. also Gaál [6] yields the following:

Lemma 1. *If* $A = \max|a_h| < A_0$ *and*

$$|b_1| > \sqrt{13} \cdot 2^{11/2} A_0$$

then for all solutions of the inequality

$$\left|\log|\beta^{(kr,jq,ip)}| + a_1 \log|\nu_1^{(kr,jq,ip)}| + \cdots + a_{11} \log|\nu_{11}^{(kr,jq,ip)}|\right| < 2c_2 \exp(-A/c_1)$$

we have

$$A < c_1(\log C + \log(2c_2) - \log A_0).$$

Note that one has to perform this reduction for all possible tuples of indices. After getting Baker's bound we can use this very efficient lemma to reduce A. One should apply the lemma in 4-5 steps, taking the previous bound (initially Baker's bound) as A_0. To ensure the condition of the lemma a suitable choice of the constant C is described in Section 7.

The lemma is very efficient in the first and second steps, when the new bound is about the logarithm of the previous one, but after 4-5 steps the new bound will not improve the previous one. In our example the final reduced bound was 164. The first step was hard to perform, because we had to use 1500 digits of accuracy.

5. Wildanger's method for the enumeration of the solutions of the unit equation

In this section we use the construction of Gaál and Pohst [9] which is in fact a variant of Wildanger's method [14]. Note that in [9] the relative extension is of degree $n \geq 3$ so in our case we have to use a modified version of Lemma 2 of [9].

For all possible tuples $I = (ip, jq, kr)$ set

$$\xi^{(I)} = \xi^{(ip,jq,kr)}, \ \beta^{(I)} = \beta^{(ip,jq,kr)}$$

and

$$\nu_h^{(I)} = \nu_h^{(ip,jq,kr)} \text{ for } h = 1, \ldots, 11$$

Let $I^* = \{I_1, \ldots, I_t\}$ be a nonempty set of indices with the following properties:

1: if $(ip, jq, kr) \in I^*$ then either $(kr, ip, jq) \in I^*$ or $(kr, jq, ip) \in I^*$

2: if $(ip, jq, kr) \in I^*$ then either $(jq, kr, ip) \in I^*$ or $(jq, ip, kr) \in I^*$

3: the vectors

$$\underline{e}_h = \begin{pmatrix} \log|\nu_h^{(I_1)}| \\ \vdots \\ \log|\nu_h^{(I_t)}| \end{pmatrix} \text{ for } h = 1, \ldots, 11$$

are linearly independent.

Set

$$\underline{g} = \begin{pmatrix} \log|\beta^{(I_1)}| \\ \vdots \\ \log|\beta^{(I_t)}| \end{pmatrix}, \ \underline{b} = \begin{pmatrix} \log|\xi^{(I_1)}| \\ \vdots \\ \log|\xi^{(I_t)}| \end{pmatrix}.$$

Using this notation we have

$$\underline{b} = \underline{g} + a_1\underline{e}_1 + \cdots + a_{11}\underline{e}_{11}.$$

Let A_r be the reduced bound obtained in the previous section, and let

$$\log S_0 = \max_{I \in I^*} \left(\left|\log|\alpha^I|\right| + A_r \left|\log|\nu_1^{(I)}|\right| + \cdots + A_r \left|\log|\nu_{11}^{(I)}|\right| \right). \tag{5.1}$$

From this it is easy to see that

$$\frac{1}{S_0} \leq |\xi^{(I)}| \leq S_0 \text{ for all } I \in I^* \tag{5.2}$$

The following lemma will help us to replace S_0 by a smaller constant in (5.2). Note that it is a variant of Lemma 2 of Gaál and Pohst [9], cf. also Gaál [6]:

Lemma 2. *Let $1 < s < S$ be given constants and assume that*

$$\frac{1}{S} \le |\xi^{(I)}| \le S \text{ for all } I \in I^*$$

Then either

$$\frac{1}{s} \le |\xi^{(I)}| \le s \text{ for all } I \in I^*$$

or there is an $I \in I^*$ with

$$|\xi^{(I)} - 1| \le \frac{1}{s-1}.$$

Proof. Note that the proof of Lemma 2 in [9] based on the multiplicative and additive relations between the $\beta^{(I)}$-s for which $I \in I^*$. In our construction I^* is defined so that the $\xi^{(I)}$-s for which $I \in I^*$ have the same properties. □

Summarizing, the constant S can be replaced by the smaller constant s if for each t_0 $(1 \le t_0 \le t)$ we enumerate directly the set H_{t_0} of those exponents $a_1, \ldots, a_{11}$ for which

$$\frac{1}{S} \le |\xi^{(I)}| \le S \text{ for all } I \in I^* \text{ and } |\xi^{(I_{t_0})} - 1| \le \frac{1}{s-1}$$

Such exponent vectors are contained in an ellipsoid. To enumerate the points of this ellipsoid we use the algorithm of Fincke and Pohst [3]. This is the critical step of the algorithm, for details see [6] and [9].

6. Sieving

As one can see in the last section, the enumeration method gives a very large number of exponent vectors $(a_1, \ldots, a_{11})$. To reduce this we insert a modular test to eliminate as much vectors as possible.

7. Numerical example

Using our algorithm we computed all power integral basis in a totally real sextic field having a cubic subfield with Galois group $S_4 \times C_2$. The method was implemented in Maple and was executed on a 333MHz Pentium PC. The defining polynomials, integral basis and fundamental units were computed by the KANT package [2]. Here we summarize our computational experiences.

Consider the totally real sextic field $K = \mathbb{Q}(\vartheta)$ where the minimal polynomial of ϑ is

$$x^6 - 17x^4 + 25x^3 + 3x^2 - 6x + 1.$$

The field has a cubic subfield $M = \mathbb{Q}(\varrho)$ where the minimal polynomial of ϱ is

$$x^3 - 4x - 1,$$

and has Galois group $S_4 \times C_2$. The ϱ has index 1 in M and $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ is an integral basis in K. The field $L^{(11,21)} = \mathbb{Q}(\vartheta^{(11)} + \vartheta^{(21)}, \vartheta^{(11)}\vartheta^{(21)})$ is generated by $\vartheta^{(11)}\vartheta^{(21)}$. In this case both $\vartheta^{(11)} + \vartheta^{(21)}$ and $\vartheta^{(11)}\vartheta^{(21)}$ generate a field of degree 12,

hence they generate the same field. The element $\vartheta^{(11)}\vartheta^{(21)}$ has a simpler defining polynomial, namely

$$x^{12}+4x^{11}-50x^{10}-57x^9+302x^8+348x^7-433x^6-450x^5+278x^4+181x^3-80x^2-8x+1$$

Baker's method gave the initial bound $A_0 = 10^{104}$ for A which was reduced to 164, using Lemma 1, by the following steps:

Step	Previous bound	Reduced bound	C
I	$A_0 = 10^{104}$	$A_1 = 2982$	A_0^{11}
II	$A_1 = 2982$	$A_2 = 199$	A_1^{20}
III	$A_2 = 199$	$A_3 = 167$	A_2^{25}
IV	$A_3 = 167$	$A_4 = 164$	A_3^{25}

The first step took about 8.3 hours, and we had to use 1500 digits of accuracy. The following steps took only a few minutes, and it was sufficient to use 150 digits of accuracy.

The final reduced bound was 164 and it gave $S_0 = 10^{1679}$ for the final enumeration (cf. (5.1)).

For the final enumeration we used the set of 18 ellipsoids defined by

$$I^* = \{(2p, 1q, 3r), (3p, 1q, 2r), (1p, 3q, 2r) \mid (p, q, r) \in \Gamma\}$$

where (p, q, r) runs through the set

$$\Gamma = \{(1,2,1), (1,1,2), (2,2,2), (1,2,2), (2,1,2), (2,2,1)\}.$$

In the table 1 we summarize the final enumeration using Wildanger's method. cf. Lemma 2. We display S, s the approximate number of exponent vectors $(a_1, \ldots, a_{11})$ enumerated in the 18 ellipsoids, the number of the exponent vectors surviving the modular tests and in the last column we display the CPU time. The last line represents the enumeration of the single ellipsoid containing the exponent vectors with coordinates ≤ 3 in absolute value (cf. [9]).

From the surviving exponent vectors we calculated the coordinates in the basis $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ of the corresponding elements of K by (2.6) and tested if they really generate power integral basis. We got the following solutions:

$$(x_1, x_2, y_0, y_1, y_2) = (0,0,1,0,0), (1,0,7,0,-2).$$

We note that if α generates power integral basis, then for arbitrary $z \in \mathbb{Z}$ the element $\pm\alpha + z$ generates also power integral basis.

Step	S	s	Enumerated	Survived	CPU Time
I	10^{1879}	10^{100}	0	0	1.5h
II	10^{100}	10^{50}	0	0	0.3h
III	10^{50}	10^{20}	1	0	0.1h
IV	10^{20}	10^{15}	30	0	0.1h
V	10^{15}	10^{12}	1300	0	0.1h
VI	10^{12}	10^{10}	14200	0	0.2h
VII	10^{10}	10^{9}	22700	0	0.2h
VIII	10^{9}	10^{8}	78300	0	0.6h
IX	10^{8}	10^{7}	246000	0	1.6h
X	10^{7}	10^{6}	650000	0	3.7h
XI	10^{6}	$5 \cdot 10^{5}$	366000	0	1.7h
XII	$5 \cdot 10^{5}$	10^{5}	1033000	2	4.8h
XIII	10^{5}	$5 \cdot 10^{4}$	328000	2	2.7h
XIV	$5 \cdot 10^{4}$	10^{4}	1971000	12	6.5h
XV	10^{4}	$5 \cdot 10^{3}$	711000	16	2.7h
XVI	$5 \cdot 10^{3}$	10^{3}	1688000	38	5.9h
XVII	10^{3}	$5 \cdot 10^{2}$	500000	42	1.5h
XVIII	$5 \cdot 10^{2}$	10^{2}	902000	76	3.3h
XIX	10^{2}	10^{1}	278000	149	1.8h
XX	10^{1}	3	1800	128	0.03h
XXI	3	0	3	3	0.01h

TABLE 1

References

[1] A.Baker and G.Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math., **442** (1993), 19–62.

[2] M.Daberkow, C.Fieker, J.Klüners, M.Pohst, K.Roegner and K.Wildanger, *KANT V4*, J. Symbolic Comput., **24** (1997), 267–283.

[3] U.Fincke and M.Pohst *Improved methods for calculating vectors of short lenght in a lattice, including a complexity analysis*, Math. Comput., **44** (1985), 463–471.

[4] I.Gaál, *Computing elements of given index in totally complex cyclic sextic fields*, J.Symbolic Comput., **20** (1995), 61–69.

[5] I.Gaál, *Computing all power integral bases in orders of totally real cyclic sextic number fields*, Math. Comput., **65** (1996), 801–822.

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

[7] I.Gaál and K.Győry, *On the resolution of index form equations in quintic fields*, Acta Arith., **89** (1999), 379–396.

[8] I.Gaál and M.Pohst, *On the resolution of index form equations in sextic fields with an imaginary quadratic subfield*, J.Symbolic Comput., **22** (1996), 425–434.

[9] I.Gaál and M.Pohst, *On the resolution of relative Thue equations*, Math. Comput., **71** (2002), 429–440.

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

[11] K.Győry, *Discriminant form and index form equations*, In: Algebraic number theory and diophantine analysis, Proc. Conf. Graz 1998, Walter de Gruyter 2000, 191–214.

[12] I.Járási, *Power integral bases in sextic fields with a cubic subfield*, Acta Sci. Math. Szeged, to appear.

[13] K.Wildanger, *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganzen Punkte einer Mordellschen Kurve*, Dissertation, Technical University, Berlin, (1997).

[14] K.Wildanger, *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern*, J.Number Theory, **82** (2000), 188–224.

University of Debrecen, Institute of Mathematics and Informatics, H-4010 Debrecen Pf.12

E-mail address: ijarasi@math.klte.hu