ACTA ARITHMETICA
115.1 (2004)

Index form equations in sextic fields: a hard computation

by

Yuri Bilu (Bordeaux), István Gaál (Debrecen) and
Kálmán Győry (Debrecen)

The purpose of this paper is to compute all generators of power integral bases in a totally real sextic field with Galois group S_6. To perform this computation was hardly possible using the previously available tools. Some new ideas are involved that may also be useful for other types of diophantine equations.

1. Introduction. Let K be an algebraic number field of degree n with ring of integers $\mathbb{Z}_K$. It is a classical problem in algebraic number theory to decide if K admits *power integral bases*, that is, integral bases of the form $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$. A general survey of this area can be found in K. Győry [10]. For a recent monograph with a detailed description of (mainly) computational results and methods on power integral bases we refer to I. Gaál [4].

If $\{1, \omega_2, \dots, \omega_n\}$ is an integral basis of K, then

$$D_{K/\mathbb{Q}}(\omega_2 X_2 + \cdots + \omega_n X_n) = (I(X_2, \dots, X_n))^2 D_K$$

where D_K denotes the discriminant of the field K, and $I(X_2, \dots, X_n)$ is the *index form* corresponding to the above integral basis. As is known, $\alpha = x_1 + \omega_2 x_2 + \cdots + \omega_n x_n \in \mathbb{Z}_K$ generates a power integral basis of K if and only if $x_1 \in \mathbb{Z}$ and $(x_2, \dots, x_n)$ is a solution of the *index form equation*

$$I(x_2, \dots, x_n) = \pm 1 \quad \text{with } x_2, \dots, x_n \in \mathbb{Z}. \tag{1}$$

General effective finiteness results for the solutions of index form equations

2000 *Mathematics Subject Classification*: 11Y50, 11D57.

Key words and phrases: power integral bases, index form equations, reduction, enumeration.

Research of the second-named author supported in part by grants T 037367 and T 042985 from the Hungarian National Foundation for Scientific Research.

Research of the third-named author supported in part by the Netherlands Organization for Scientific Research, the Hungarian Academy of Sciences and grants T 029330, T 038225 and T 042985 from the Hungarian National Foundation for Scientific Research.

were obtained by K. Győry [8], which made it possible, at least in principle, to determine all solutions in concrete cases; for recent improvements, see [9], [10]. In the last decade considerable effort was made to develop efficient algorithms for finding explicitly the solutions, which was successful for lower degree fields ($n \leq 5$) and partially successful for higher degree fields; see [4].

I. Gaál and K. Győry [6] gave an algorithm for solving index form equations in arbitrary quintic fields. Despite the very short CPU times we had for cubic and quartic fields, in the quintic case (in the most interesting case of totally real fields with Galois group S_5) about 8 hours of CPU time were necessary (using a 1 GHz PC under Linux). In [6] the ideas of K. Győry [8], [9] were used in reducing the index form equation to appropriate unit equations in two variables and applying Baker's estimates. It was observed that if $K = \mathbb{Q}(\xi)$ is a totally real quintic field with a doubly transitive Galois group (which is satisfied in the most difficult cases), then the values of the linear factors of the index form are contained in fields of type $L_{i,j} = \mathbb{Q}(\xi^{(i)} + \xi^{(j)}, \xi^{(i)}\xi^{(j)})$ of degree 10 with 9 fundamental units. After having derived a Baker's type estimate for the corresponding 9 unknown exponents in the unit equation, the usual reduction algorithm and a suitably modified version (see I. Gaál and M. Pohst [7], I. Gaál [4]) of K. Wildanger's enumeration method [11] were still applicable. The critical part of the algorithm was the enumeration of the small exponent vectors.

Since that time we have been trying to extend the same method to sextic fields, when in the most interesting cases (totally real sextic field, with a doubly transitive Galois group) the corresponding fields $L_{i,j}$ are of degree 15 with 14 fundamental units. This unit rank is already beyond the applicability of the same enumeration procedures.

Despite this, some refinements of the enumeration method lead us to being able to compute all generators of power integral bases in a totally real sextic field with Galois group S_6. As we expected, the total CPU time was far longer than in the previous lower degree fields: about 5 months. In this paper we present the refined enumeration process and report on the computation.

2. Preliminaries. We use the same notation as in [6], giving here only the basic definitions.

Let $K = \mathbb{Q}(\xi)$ be a totally real sextic field with a doubly transitive Galois group. As in [6] this covers the most difficult (hence most interesting) cases. In our example the field has Galois group S_6. Let $d \in \mathbb{Z}$ be a common denominator such that each $\vartheta \in \mathbb{Z}_K$ can be written in the form

$$\vartheta = \frac{y_0 + y_1\xi + \cdots + y_5\xi^5}{d} \tag{2}$$

with $y_0, y_1, \dots, y_5 \in \mathbb{Z}$. In the following assume that ϑ is a generator of a power integral basis, that is, the index of ϑ is 1,

$$I(\vartheta) = 1. \tag{3}$$

As in [6] we let

$$l_{ij}(\underline{Y}) = (\xi^{(i)} - \xi^{(j)})Y_1 + \cdots + ((\xi^{(i)})^5 - (\xi^{(j)})^5)Y_5$$

and

$$\delta^{(i,j)} = \frac{d(\vartheta^{(i)} - \vartheta^{(j)})}{\xi^{(i)} - \xi^{(j)}}$$

for $1 \le i < j \le 6$. Equation (3) implies

$$\prod_{1 \le i < j \le 6} \delta^{(i,j)} = \frac{d^{15}}{I(\xi)} = d_0$$

with $d_0 \in \mathbb{Z}$. Hence $\delta^{(1,2)}$ is an integer in $L_{1,2} = \mathbb{Q}(\xi^{(1)} + \xi^{(2)}, \xi^{(1)}\xi^{(2)})$ of norm d_0, whence it can be represented in the form

$$\delta^{(1,2)} = \gamma^{(1,2)}\eta^{(1,2)}$$

where $\gamma^{(1,2)}$ is an integer in $L_{1,2}$ of norm d_0 (the finitely many non-associated possible values of $\gamma^{(1,2)}$ can be determined by using Kash [2]) and

$$\eta^{(1,2)} = \pm(\varepsilon_1^{(1,2)})^{a_1} \cdots (\varepsilon_{14}^{(1,2)})^{a_{14}}$$

is a representation of the unit $\eta^{(1,2)}$ in a system of fundamental units $\varepsilon_1^{(1,2)}, \dots$ $\dots, \varepsilon_{14}^{(1,2)}$ of $L_{1,2}$ with rational integer exponents $a_1, \dots, a_{14}$. Let $A = \max_{1 \le i \le 14} |a_i|$. We are going to determine $a_1, \dots, a_{14}$, from which $y_1, \dots, y_6$ and thus ϑ can be calculated.

Denote by $\lambda^{(i,j)}$ the conjugate of any $\lambda = \lambda^{(1,2)} \in L_{1,2}$ corresponding to $\xi^{(i)} + \xi^{(j)}$, $\xi^{(i)}\xi^{(j)}$ $(1 \le i < j \le 6)$ and for simplicity let $\lambda^{(j,i)} = \lambda^{(i,j)}$.

3. Application of Baker's method. For any distinct integers i, j, k with $1 \le i, j, k \le 6$, Siegel's identity

$$l_{ij}(\underline{Y}) + l_{jk}(\underline{Y}) + l_{ki}(\underline{Y}) = 0$$

can be written in the form

$$\beta^{(ijk)} + \beta^{(kji)} = 1 \tag{4}$$

where

$$\beta^{(ijk)} = \alpha^{(ijk)}\mu^{(ijk)}, \qquad \alpha^{(ijk)} = \frac{\gamma^{(i,j)}(\xi^{(i)} - \xi^{(j)})}{\gamma^{(i,k)}(\xi^{(i)} - \xi^{(k)})},$$

$$\mu^{(ijk)} = \prod_{h=1}^{14} (\nu_h^{(ijk)})^{a_h}, \qquad \nu_h^{(ijk)} = \frac{\varepsilon_h^{(i,j)}}{\varepsilon_h^{(i,k)}} \quad (h = 1, \dots, 14).$$

Observe that our notation implies

$$\beta^{(ijk)} = \frac{\vartheta^{(i)} - \vartheta^{(j)}}{\vartheta^{(i)} - \vartheta^{(k)}}. \tag{5}$$

Just as in [6] we can apply Baker's type estimates, that is, we can calculate positive constants c_1, c_2 and C_0 (this latter constant is a huge one given for example by the estimates of A. Baker and G. Wüstholz [1]) such that for certain distinct indices i, j, k,

$$\begin{aligned} &\exp(-C_0 \log A) \\ &\quad \le \left|\log|\alpha^{(kji)}| + a_1 \log|\nu_1^{(kji)}| + \cdots + a_{14} \log|\nu_{14}^{(kji)}|\right| \le 2c_2 \exp(-A/c_1), \end{aligned} \tag{6}$$

which implies an upper bound A_B for A. In our example we had $A_B = 10^{122}$.

4. Reduction. The reduction of this bound A_B is performed by using an appropriate version of Lemma 2.2.2 of [4].

For a triple (k, j, i) of distinct indices $1 \le k, j, i \le 6$, consider the lattice $\mathcal{L}$ spanned by the columns of the 15 by 14 matrix

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \\ C \cdot \log|\alpha^{(kji)}| & C \cdot \log|\nu_1^{(kji)}| & \dots & C \cdot \log|\nu_{14}^{(kji)}| \end{pmatrix}$$

where C is a large constant. Denote by b_1 the first vector of an LLL reduced basis of $\mathcal{L}$.

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

$$|b_1| > 512 \cdot A_0 \tag{7}$$

then for all solutions of the inequality

$$\left|\log|\alpha^{(kji)}| + a_1 \log|\nu_1^{(kji)}| + \cdots + a_{14} \log|\nu_{14}^{(kji)}|\right| \le 2c_2 \exp(-A/c_1)$$

we have

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

Note that if in the above linear form the terms are linearly dependent over $\mathbb{Q}$ then we can reduce the number of variables. We have to perform the reduction procedure for all possible triples (k, j, i). Since (k, j, i) and (k, i, j) give the same linear form, this yields 60 cases to consider. In each case we perform several consecutive reduction steps. In our example the final reduced bound A_R for A was 336.

5. Enumeration. We have to introduce considerable changes in the enumeration process. First, as in [6] we calculate an S_0^* with

$$\frac{1}{S_0^*} \le |\beta^{(ijk)}| \le S_0^*$$

for any i, j, k. This is obtained by

$$\log S_0^* = \max_{i,j,k} \big(\big|\log|\alpha^{(ijk)}|\big| + A_R\big|\log|\nu_1^{(ijk)}|\big| + \cdots + A_R\big|\log|\nu_{14}^{(ijk)}|\big|\big). \tag{8}$$

In our example we had $S_0^* = 10^{3125}$.

Our procedure is based on the following statement. In the lemma a *triple* will mean a 3-element ordered subset of $\{1, \dots, n\}$.

LEMMA 2. *Let $\gamma_1, \dots, \gamma_n$ be pairwise distinct complex numbers and let*

$$D = \prod_{1 \le i < j \le n} |\gamma_i - \gamma_j|. \tag{9}$$

Let $s > 1$ be a real number. Then either

$$\left|\log|\gamma_i - \gamma_j| - \frac{2}{n(n-1)}\log D + \frac{\log s}{n}\right| \le \log s \tag{10}$$

for all $1 \le i < j \le n$, or there exists a triple (i_1, j_1, k_1) such that

$$\left|\frac{\gamma_{j_1} - \gamma_{i_1}}{\gamma_{k_1} - \gamma_{i_1}}\right| \le \left(\frac{3}{s}\right)^{(n-1)/(n-2)}. \tag{11}$$

Proof. Replacing each γ_i by $\gamma_i D^{-2/(n(n-1))}$, we may assume that $D = 1$ and (10) transforms to

$$\left|\log|\gamma_i - \gamma_j| + \frac{\log s}{n}\right| \le \log s \quad (1 \le i < j \le n). \tag{12}$$

Put

$$\delta = \min_{1 \le i < j \le n} |\gamma_i - \gamma_j|, \qquad \Delta = \max_{1 \le i < j \le n} |\gamma_i - \gamma_j|.$$

There exists a triple (i_1, j_1, k_1) such that $|\gamma_{j_1} - \gamma_{i_1}| = \delta$ and $|\gamma_{k_1} - \gamma_{i_1}| \ge \Delta/2$. Since

$$\left|\frac{\gamma_{j_1} - \gamma_{i_1}}{\gamma_{k_1} - \gamma_{i_1}}\right| \le \frac{2\delta}{\Delta},$$

it remains to show that if (12) fails, then

$$\frac{2\delta}{\Delta} \le \left(\frac{3}{s}\right)^{(n-1)/(n-2)}. \tag{13}$$

If $|\gamma_l - \gamma_m| = \Delta$ then for every $i \ne l, m$ we have either $|\gamma_i - \gamma_l| \ge \Delta/2$ or $|\gamma_i - \gamma_m| \ge \Delta/2$. Hence the product in (9) has, besides $|\gamma_l - \gamma_m|$, at least $n-2$ factors exceeding $\Delta/2$. Therefore the product can be estimated from below by $(\Delta/2)^{n-1}\delta^{(n-1)(n-2)/2}$ and trivially from above by $\delta\Delta^{n(n-1)/2-1}$.

Thus

$$(\Delta/2)^{n-1}\delta^{(n-1)(n-2)/2} \le 1 \le \delta\Delta^{n(n-1)/2-1},$$

which implies that

$$\frac{2}{n-2}\log\frac{\Delta}{2} \le \log\delta^{-1} \le \left(\frac{n(n-1)}{2}-1\right)\log\Delta,$$

which in turn yields the inequality

$$\log\frac{\Delta}{2\delta} \ge \max\left\{\frac{n}{n-2}\log\frac{\Delta}{2}, \frac{n(n-1)}{(n-2)(n+1)}\log\delta^{-1} - \log 2\right\}. \tag{14}$$

Now, if (12) fails, then either

$$\log\Delta \ge ((n-1)/n)\log s \quad \text{or} \quad \log\delta^{-1} \ge ((n+1)/n)\log s.$$

Any of these inequalities, combined with (14), implies (13). ∎

Equation (3) can be written as

$$\prod_{1\le i<j\le 6} |\vartheta^{(i)} - \vartheta^{(j)}| = \sqrt{|D_K|}.$$

Let $s > 1$ be a real number. Applying Lemma 2 we deduce that either for all $1 \le i < j \le 6$ we have

$$\left|\log|\vartheta^{(i)} - \vartheta^{(j)}| - \frac{\log|D_K|}{15} + \frac{\log s}{6}\right| \le \log s \tag{15}$$

or there are distinct i, j, k with

$$\left|\frac{\vartheta^{(i)} - \vartheta^{(j)}}{\vartheta^{(i)} - \vartheta^{(k)}}\right| \le \left(\frac{3}{s}\right)^{5/4} = \left(\frac{s}{3}\right)^{-5/4}. \tag{16}$$

Our enumeration process is divided into several steps similar to those in [6]. Instead of Lemma 2 in [6] we shall use the following consequence of our Lemma 2 above:

LEMMA 3. *Let $3 < s < S$ be positive constants and let*

$$Q = \left(\frac{s}{3}\right)^{5/4}.$$

Assume that for all distinct $1 \le i, j, k \le 6$ we have

$$\frac{1}{S^2} \le |\beta^{(ijk)}| \le S^2. \tag{17}$$

Then either for all distinct $1 \le i, j, k \le 6$ we have

$$\frac{1}{s^2} \le |\beta^{(ijk)}| \le s^2, \tag{18}$$

or there are distinct indices $1 \le i_0, j_0, k_0 \le 6$ such that

$$\left|\log|\beta^{(k_0 j_0 i_0)}|\right| \le \log\frac{Q}{Q-1}. \tag{19}$$

Further, for all $l = \{1, \dots, 6\} \setminus \{i_0, j_0, k_0\}$ *we have either*

$$\big|\log|\beta^{(lj_0i_0)}|\big| \le \log\frac{\sqrt{Q}}{\sqrt{Q}-1} \quad \text{or} \quad \big|\log|\beta^{(k_0li_0)}|\big| \le \log\frac{\sqrt{Q}}{\sqrt{Q}-1}. \tag{20}$$

Proof. Apply Lemma 2 with $n = 6$, $\gamma_i = \vartheta^{(i)}$, $1 \le i \le 6$ and $D = D_K$. Then there are two possibilities.

Firstly, if (15) is satisfied for all pairs of indices, then we infer that for any distinct i, j, k,

$$\begin{aligned}\log|\beta^{(ijk)}| &= \left|\frac{\vartheta^{(i)}-\vartheta^{(j)}}{\vartheta^{(i)}-\vartheta^{(k)}}\right| \\ &\le \left(\log s + \frac{\log|D_K|}{15} - \frac{\log s}{6}\right) - \left(-\log s + \frac{\log|D_K|}{15} - \frac{\log s}{6}\right) \\ &= 2\log s.\end{aligned}$$

The same inequality can be derived for $\beta^{(kji)} = 1/\beta^{(ijk)}$, hence we have

$$\big|\log|\beta^{(ijk)}|\big| \le 2\log s,$$

which implies (18).

Secondly, consider the case when (16) holds for some distinct i, j, k. Note that for any $Q > 1$ and $\beta \in \mathbb{R}$,

$$\text{if } |\beta - 1| \le \frac{1}{Q} \text{ then } \big|\log|\beta|\big| \le \log\frac{Q}{Q-1}. \tag{21}$$

Then, putting $Q = (s/3)^{5/4}$, we deduce from (16) that

$$|\beta^{(kji)} - 1| = |\beta^{(ijk)}| \le \left(\frac{s}{3}\right)^{-5/4} = \frac{1}{Q},$$

whence, by inequality (21), we obtain (19) with $k_0 = k$, $j_0 = j$, $i_0 = i$.

Further, for any $l \in \{1, \dots, 6\} \setminus \{i_0, j_0, k_0\}$ observe that

$$\beta^{(ijk)} = \frac{\vartheta^{(i)}-\vartheta^{(j)}}{\vartheta^{(i)}-\vartheta^{(k)}} = \frac{\vartheta^{(i)}-\vartheta^{(j)}}{\vartheta^{(i)}-\vartheta^{(l)}} \cdot \frac{\vartheta^{(i)}-\vartheta^{(l)}}{\vartheta^{(i)}-\vartheta^{(k)}} = \beta^{(ijl)} \cdot \beta^{(ilk)}.$$

By $|\beta^{(ijk)}| < 1/Q$ this implies that either

$$|\beta^{(ijl)}| \le \frac{1}{\sqrt{Q}}, \quad \text{or} \quad |\beta^{(ilk)}| \le \frac{1}{\sqrt{Q}},$$

whence using inequality (21) we obtain (20). ∎

Let $S_0 > S_1 > \cdots > S_k$. We now apply Lemma 3 repeatedly for $S = S_i$, $s = S_{i+1}$, $i = 0, \dots, k-1$. Initially (17) is satisfied for $S = S_0 = \sqrt{S_0^*}$. In each step we assume that (17) holds. Then either (18) is satisfied for all indices i, j, k, in which case there is nothing to do, or we have (19) for a triple i_0, j_0, k_0 and, further, for all $l = \{1, \dots, 6\} \setminus \{i_0, j_0, k_0\}$ one of the inequalities of (20) is satisfied.

By $\big|\log|\beta^{(ijk)}|\big| = \big|\log|\beta^{(ikj)}|\big|$ we have altogether $6 \cdot 5 \cdot 4/2 = 60$ triples i, j, k. Arrange these triples i, j, k into a sequence $I_1, \dots, I_{60}$ where each I_m yields a triple i, j, k. Let

$$\lambda_1 = \frac{1}{2\log S}, \quad \lambda_2 = \frac{1}{\log \dfrac{Q}{Q-1}}, \quad \lambda_3 = \frac{1}{\log \dfrac{\sqrt{Q}}{\sqrt{Q}-1}}$$

and set

$$\lambda_{I_m} = \begin{cases} \lambda_2 & \text{if (19) is satisfied for } I_m, \\ \lambda_3 & \text{if (20) is satisfied for } I_m, \\ \lambda_1 & \text{otherwise.} \end{cases}$$

There are 60 possibilities for the indices i_0, j_0, k_0 in (19). Further, for each $l = \{1, \dots, 6\} \setminus \{i_0, j_0, k_0\}$ there are two possibilities according to which part of (20) holds. This makes altogether 480 possible distributions of the weights $\lambda_1, \lambda_2, \lambda_3$. As in [6], we define

$$\varphi(\underline{b}) = \begin{pmatrix} \lambda_1 \log|\beta^{(I_1)}| \\ \vdots \\ \lambda_{60} \log|\beta^{(I_{60})}| \end{pmatrix}, \quad \varphi(\underline{g}) = \begin{pmatrix} \lambda_1 \log|\alpha^{(I_1)}| \\ \vdots \\ \lambda_{60} \log|\alpha^{(I_{60})}| \end{pmatrix}$$

and

$$\varphi(\underline{e}_h) = \begin{pmatrix} \lambda_1 \log|\nu_h^{(I_1)}| \\ \vdots \\ \lambda_{60} \log|\nu_h^{(I_{60})}| \end{pmatrix} \quad \text{for } h = 1, \dots, 14.$$

The vectors $\varphi(\underline{e}_1), \dots, \varphi(\underline{e}_{14})$ are linearly independent and we have

$$\varphi(\underline{b}) = \varphi(\underline{g}) + a_1\varphi(\underline{e}_1) + \cdots + a_{14}\varphi(\underline{e}_{14}).$$

By the definition of the weights, in view of (19), (20) we have

$$\|\varphi(\underline{g}) + a_1\varphi(\underline{e}_1) + \cdots + a_{14}\varphi(\underline{e}_{14})\|_2^2 = \|\varphi(\underline{b})\|_2^2 = \sum_{m=1}^{60} \lambda_{I_m}^2 \log^2|\beta^{(I_m)}| \le 60. \tag{22}$$

This inequality defines an *ellipsoid* that can be enumerated by using the method of U. Fincke and M. Pohst [3], as in [6].

This enumeration relies on the ideas of K. Wildanger [11]. It is important that here we have altogether four large weights in the coordinates. Since the 14 variables are already too many for this enumeration method (it is efficient at most up to unit rank 11 or 12, see [4] or [5]), our first idea was to eliminate three of the variables and then to have only 11 variables and one large weight. After making several computational experiments, we found that this method is less efficient than the present algorithm involving 14 variables and four

large weights. Also, to have all the possible coordinates here (all 60 possible triples) reduces the number of enumerated vectors $(a_1, \dots, a_{14})$ considerably (at the price of enumerating more ellipsoids). The reason for this is that for the enumerated points, almost all initial inequalities are satisfied, and thus having more initial inequalities reduces the number of enumerated vectors.

In the last step

$$\|\varphi(\underline{g}) + a_1\varphi(\underline{e}_1) + \cdots + a_{14}\varphi(\underline{e}_{14})\|_2^2 = \|\varphi(\underline{b})\|_2^2 = \sum_{m=1}^{60} \lambda_{I_m}^2 \log^2 |\beta^{(I_m)}| \le 60 \cdot (2 \log S_k)^2 \tag{23}$$

also defines an ellipsoid.

We carried out several tests in order to choose the sequence $S_0 > S_1 > \cdots > S_k$ appropriately. The constant S_0 is determined by (8). We made several tests to see how large we could make S_k so that the lattice points in the ellipsoid (23) could be enumerated. In our example we could enumerate these lattice points within a couple of minutes with $S_k = 10$, but $S_k = 15$ was not successful (even with 12 days of CPU time on a 1 GHz PC). Then the interval (S_k, S_0) was divided into several parts (also after making several experiments) so that each intermediate step can be performed.

6. Sieve. We only remark that, as in [6], we also used sieving modulo a suitable prime number (see Section 6 of [6]) in enumerating the vectors $(a_1, \dots, a_{14})$. This was used to get rid of the majority of possible vectors.

7. The example. Let $f(x) = x^6 - 5x^5 + 2x^4 + 18x^3 - 11x^2 - 19x + 1$ and let ξ be a root of $f(x)$. Then $K = \mathbb{Q}(\xi)$ is a totally real sextic field with discriminant $D_K = 592661$, integral basis $\{1, \xi, \xi^2, \xi^3, \xi^4, \xi^5\}$ and Galois group S_6. (Hence we have $d = 1$ in the representation (2).) The fields $\mathbb{Q}(\xi^{(1)} + \xi^{(2)})$, $\mathbb{Q}(\xi^{(1)}\xi^{(2)})$ are in this case the same. The minimal polynomial of $\xi^{(1)}\xi^{(2)}$ is

$$\begin{aligned} F(x) = {} & x^{15} - 2x^{14} - 79x^{13} + x^{12} + 2311x^{11} \\ & + 3943x^{10} - 23190x^9 - 77373x^8 - 22532x^7 + 145057x^6 \\ & + 110573x^5 - 36269x^4 + 996x^3 + 344x^2 - 11x - 1, \end{aligned}$$

the field $L_{1,2} = \mathbb{Q}(\xi^{(1)}\xi^{(2)})$ has discriminant 123374497805640685368241. In the example we have $d_0 = 1$. The fundamental units in $L_{1,2}$ were computed by Kash [2]; it would be far too long to include their explicit forms here.

Using the estimates for the linear form in the logarithms in (6) we have $c_1 = 2.394, c_2 = 21.4$ and finally we obtain the upper bound $A_B = 10^{122}$ for $A = \max_{1 \le i \le 14} |a_i|$.

The table below gives a summary of the reduction procedure. In each step C is the constant used in Lemma 1, and "digits" shows the accuracy used.

Step	$A <$	$\|b_1\| >$	C	Digits	New bound for H	CPU time
I	10^{122}	$5.12 \cdot 10^{124}$	10^{1300}	1500	6502	300 min
II	6502	$3.39 \cdot 10^6$	10^{90}	120	484	7 min
III	484	$2.47 \cdot 10^5$	10^{65}	85	352	5 min
IV	352	180224	10^{62}	85	336	4 min

The most interesting (and time consuming) part of the computation was the enumeration process. By (8) we had $S_0^* = 10^{3125}$, hence we put $S_0 = 10^{1563}$. In the following table we describe the steps of the enumeration process. Note that while enumerating the ellipsoids we also used sieving modulo 5869. We display $S = S_i$, $s = S_{i+1}$, the approximate number of the enumerated vectors in all the 480 ellipsoids, the number of vectors that survived the sieve, the accuracy and the CPU time (the total for the 480 ellipsoids). Note that the CPU times refer to a 1 GHz PC running under Linux. The last line refers to the last ellipsoid (23).

Step	S	s	Enumerated	Survived	Digits	CPU time
I	10^{1563}	10^{50}	0	0	200	12 hours
II	10^{50}	10^{10}	0	0	100	9 hours
III	10^{10}	10^7	0	0	100	6.2 hours
IV	10^7	10^5	$0.004 \cdot 10^6$	3	100	4 hours
V	10^5	10^4	$0.12 \cdot 10^6$	112	100	2.2 hours
VI	10000	7000	$0.048 \cdot 10^6$	79	50	7 hours
VII	7000	5000	$0.12 \cdot 10^6$	121	50	6 hours
VIII	5000	3000	$0.26 \cdot 10^6$	308	50	4.5 hours
IX	3000	2000	$0.52 \cdot 10^6$	488	50	2.5 hours
X	2000	1000	$2.8 \cdot 10^6$	2069	50	7 hours
XI	1000	500	$8.6 \cdot 10^6$	6787	50	16 hours
XII	500	400	$6.2 \cdot 10^6$	4963	50	16 hours
XIII	400	300	$10.56 \cdot 10^6$	8440	50	22 hours
XIV	300	200	$26.4 \cdot 10^6$	18353	50	36 hours
XV	200	150	$29.7 \cdot 10^6$	22228	50	53 hours
XVI	150	100	$67.2 \cdot 10^6$	46101	50	96 hours
XVII	100	50	$278.4 \cdot 10^6$	190300	50	384 hours
XVIII	50	20	$120.0 \cdot 10^6$	850644	50	1632 hours
XIX	20	10	$883.2 \cdot 10^6$	758542	50	1128 hours
XX	10		$50.6 \cdot 10^6$	34412	50	0.5 hours

Altogether there were 1943950 vectors that survived the sieve out of $1484.7 \cdot 10^6$ enumerated vectors. The total CPU time for the enumeration (involving the first sieve) was 3443.9 hours (that is, 143 days or 4.8 months). These routines were running on a machine with six parallel 1 GHz processors under Linux, so the real time was about one month. Note that the CPU time for the enumeration of the last ellipsoid (23) with $S = 10$ was short. The enumeration of this last ellipsoid with $S = 15$ was not successful within two weeks. Hence we could not diminish the critical CPU times in steps XVII, XVIII.

The following processes took just a couple of minutes. We performed a second sieving using the prime 12421 which allowed only 23308 vectors out of the above 1943950 possible vectors. It turned out that there are only 199 distinct vectors out of these 23308 vectors (the same vectors can of course be contained in several ellipsoids). The third sieve was performed with the prime 78277, there remained 45 possible vectors which survived also a fourth sieve with the prime 68813. All these 45 surviving vectors yielded a solution of (3). These solutions are listed in the following table. Note that if $(y_1, \dots, y_6)$ is a solution then so also is $(-y_1, \dots, -y_6)$ but we list only one of them. (Recall that in the representation (2) we have $d = 1$.)

$(y_2, y_3, y_4, y_5, y_6) =$

$(1,0,0,0,0),\ (-1,1,0,0,0),\ (-2,-2,1,0,0),\ (2,7,-2,-3,1),$

$(4,9,-3,-3,1),\ (-4,12,0,-4,1),\ (5,-1,-3,1,0),\ (-5,-5,4,2,-1),$

$(5,6,-2,-3,1),\ (-5,9,1,-4,1),\ (5,9,-3,-3,1),\ (-6,2,3,-1,0),$

$(6,-5,-2,1,0),\ (6,8,-3,-3,1),\ (7,1,-4,1,0),\ (-7,6,2,-1,0),$

$(-7,-6,5,2,-1),\ (8,10,-4,-3,1),\ (9,10,-4,-3,1),\ (10,0,-4,1,0),$

$(10,8,-6,-2,1),\ (-10,-17,6,6,-2),\ (11,3,-8,2,0),\ (-11,-7,6,2,-1),$

$(-11,-13,7,5,-2),\ (-11,18,2,-5,1),\ (12,7,-6,-2,1),$

$(-13,-6,6,2,-1),\ (13,15,-8,-5,2),\ (-14,-14,8,5,-2),$

$(16,16,-9,-5,2),\ (17,16,-9,-5,2),\ (18,11,-10,-4,2),$

$(20,22,-11,-8,3),\ (21,-10,-8,6,-1),\ (22,24,-12,-8,3),$

$(23,14,-12,-4,2),\ (-26,-20,14,7,-3),\ (43,45,-21,-14,5),$

$(-46,-45,26,15,-6),\ (108,106,-63,-36,15),\ (-119,-118,68,40,-16),$

$(153,-26,-126,75,-12),\ (173,167,-105,-58,25),$

$(-590,-585,336,198,-79).$

Acknowledgements. The authors are thankful to the referee for his helpful remarks and to John Cremona for improving the language of the paper.

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, M. Schörnig 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 length in a lattice, including a complexity analysis*, Math. Comput. 44 (1985), 463–471.
[4] I. Gaál, *Diophantine Equations and Power Integral Bases*, Birkhäuser Boston, 2002.
[5] —, *Power integral bases in cubic relative extensions*, Experiment. Math. 10 (2001), 133–139.
[6] I. Gaál and K. Győry, *Index form equations in quintic fields*, Acta Arith. 89 (1999), 379–396.
[7] 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.
[8] K. Győry, *Sur les polynômes à coefficients entiers et de discriminant donné, III*, Publ. Math. Debrecen 23 (1976), 141–165.
[9] —, *Bounds for the solutions of decomposable form equations*, ibid. 52 (1998), 1–31.
[10] —, *Discriminant form and index form equations*, in: Algebraic Number Theory and Diophantine Analysis, de Gruyter, 2000, 191–214.
[11] K. Wildanger, *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern*, J. Number Theory 82 (2000), 188–224.

A2X, Université Bordeaux 1
351 cours de la Libération
F-33405 Talence Cedex, France
E-mail: bilu@math.u-bordeaux.fr

Mathematical Institute
University of Debrecen
H-4010 Debrecen Pf. 12, Hungary
E-mail: igaal@math.klte.hu
gyory@math.klte.hu

Received on 7.10.2003
and in revised form on 23.4.2004 (4644)