ACTA ARITHMETICA
LXXXIX.4 (1999)

Index form equations in quintic fields

by

István Gaál and Kálmán Győry (Debrecen)

Dedicated to Professor Alan Baker on his 60th birthday

The problem of determining power integral bases in algebraic number fields is equivalent to solving the corresponding index form equations. As is known (cf. Győry [25]), every index form equation can be reduced to an equation system consisting of unit equations in two variables over the normal closure of the original field. However, the unit rank of the normal closure is usually too large for practical use. In a recent paper Győry [27] succeeded in reducing index form equations to systems of unit equations in which the unknown units are elements of unit groups generated by much fewer generators. On the other hand, Wildanger [32] worked out an efficient enumeration algorithm that makes it feasible to solve unit equations even if the rank of the unit group is ten. Combining these developments we describe an algorithm to solve completely index form equations in quintic fields. The method is illustrated by numerical examples: we computed all power integral bases in totally real quintic fields with Galois group S_5.

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 $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. If $\{1, \omega_2, \ldots, \omega_n\}$ is any integral basis of K, then

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

1991 *Mathematics Subject Classification*: Primary 11Y50; Secondary 11D57, 11R21.

Key words and phrases: index form equations, power integral bases, computer resolution of diophantine equations.

Research of the first author supported in part by Grants 16975 and 25157 from the Hungarian National Foundation for Scientific Research.

Research of the second author supported in part by Grants 16975 and 25157 from the Hungarian National Foundation for Scientific Research and by the Hungarian Academy of Sciences.

where D_K denotes the discriminant of the field K, and $I(X_2, \ldots, X_n)$ is a form of degree $n(n-1)/2$ in $n-1$ variables with integer coefficients. This form is called the *index form* corresponding to the above integral basis. As is known, $\alpha = x_1 + \omega_2 x_2 + \ldots + \omega_n x_n \in \mathbb{Z}_K$ generates a power integral basis of K if and only if $x_1 \in \mathbb{Z}$ and $(x_2, \ldots, x_n)$ is a solution of the *index form equation*

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

Hence the problem of determining all power integral bases in K is equivalent to solving this equation.

The first effective upper bounds for the solutions of index form equations were derived by Győry [25] by means of Baker's method. As a consequence, it was shown in [25] that up to translation by elements of $\mathbb{Z}$, there are only finitely many generators of power integral bases in a number field, and effective bounds were given for the heights of these generators. Several generalizations and improvements were later established; for references see [26], [6], [4] and [28]. The best known bounds can be found in [27]. Unfortunately these general bounds are much too large for practical applications.

Using Baker's method and reduction algorithms Gaál and Schulte [23] determined all power integral bases in cubic number fields of small discriminant. The quartic fields were considered by Gaál, Pethő and Pohst in a series of papers (cf. e.g. [15]–[19]). Efficient algorithms were given for special quartic fields, and a general approach is described in [18] and [19] for arbitrary quartic fields. Independently, by algebraic means Koppenhöfer [30] developed a similar method for quartic fields. A special family of cyclic quintic fields was studied by Gaál and Pohst [21]. The problem of power integral bases in sextic fields with quadratic subfields was investigated by Gaál [8], [9] and Gaál and Pohst [20]. Higher degree number fields that are composits of two subfields were considered in Gaál [12], and an application of these ideas to fields of degree 9 being composits of cubic fields can be found in Gaál [14]. For a survey on this topic see [10], [11], [13]. Note that utilizing the subfield structure of the fields under consideration and the corresponding factorization of the index form, in the above mentioned papers *the index form equation was always reduced to simpler types of diophantine equations of lower degree and in a fewer number of variables*. In these investigations several types of Thue equations play an important role (cf. [11]).

Using the general approach of Győry [25], *the index form equation* (1) *can be reduced to an equation system consisting of unit equations in two variables*, where the unknown units belong to the normal closure of the field K. Further, applying Baker's method, a bound can be obtained for the absolute values of the exponents of the fundamental units in the representations of the unknown units. For concrete equations the next step is

to reduce this bound by using the LLL algorithm. The reduction algorithm being very efficient, a crucial problem in the resolution of these unit equations is to test the extremely large number of possible "small" exponents with absolute values under the reduced bound. Even if the reduced bound is moderate (< 100), the direct enumeration is almost hopeless whenever the number of exponents is greater than 4. Using this approach Klebel [29] solved relative index form equations in normal extensions of low degree over imaginary quadratic fields. Further, Smart [31] and recently Wildanger [32] gave ideas how to diminish the number of unit equations to be solved by using the action of the Galois group on these equations. By means of this method Smart [31] solved index form equations in sextic fields having an imaginary quadratic subfield.

Wildanger [32] has recently worked out a very efficient method for the *enumeration of the "small" values of the exponents* in a unit equation. This is based on the ellipsoid method of Fincke and Pohst [5]. This enabled him to solve index form equations in normal fields of degree 8, 10, 12, 16, 18 and 22 whose unit ranks do not exceed 10.

Recently Győry [27] has refined his general approach [25] by reducing the index form equation (1) to a system of unit equations in which the *unknown units are elements of unit groups having much fewer generators*. Therefore the number of "small" exponents to be tested can be considerably diminished.

The combination of the above mentioned new approach of Győry [27] with a variant of Wildanger's enumeration method described by Gaál and Pohst [22] makes it feasible to solve index form equations in *quintic fields*. The possible Galois groups of quintic fields are C_5 (the cyclic group), D_5 (the dihedral group of order 10), M_{20} (the metacyclic group of degree 5), A_5 and S_5 (cf. [2]). By a theorem of Gras [24] the index form equation (1) has no solution for quintic K having cyclic Galois group, except for the case when K is the maximal real subfield of the 11th cyclotomic field. The orders of the groups C_5 and D_5 do not exceed 10, hence in these cases the Wildanger's algorithm can be applied to solve the index form equation.

In the present paper we consider the most difficult cases, that is, *quintic fields with Galois groups M_{20}, A_5 or S_5*. Also, to make the presentation simpler we restrict ourselves to the most interesting case of *totally real fields*. In Sections 2–6 we describe our algorithm for the resolution of index form equations. As an illustration of our method we calculate in Section 7 all solutions of index form equations in two totally real quintic fields with Galois group S_5.

2. Reduction to unit equations. We now apply the general method of Győry [27] to reduce index form equations in quintic fields to appropri-

ate systems of unit equations. A suitable representation (4) of the integer elements that makes the formulas simpler was formerly used e.g. by Gaál, Pethő and Pohst [18].

Let K be a totally real quintic field with Galois group M_{20}, A_5 or S_5, with ring of integers $\mathbb{Z}_K$ and discriminant D_K. Let ξ be an integral generator of K with conjugates $\xi^{(1)} = \xi, \xi^{(2)}, \ldots, \xi^{(5)}$ over $\mathbb{Q}$. We write $K^{(i)}$ for $\mathbb{Q}(\xi^{(i)})$.

For any primitive integral element ϑ of K we denote by

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

the index of ϑ. Then

$$D_{K/\mathbb{Q}}(\vartheta) = I(\vartheta)^2 D_K. \tag{2}$$

For $d = I(\xi)$ we have $d \cdot \mathbb{Z}_K \subseteq \mathbb{Z}[\xi]$. Let $\{1, \omega_2, \omega_3, \omega_4, \omega_5\}$ be an integral basis of K, where

$$\omega_i = \frac{a_{i0} + a_{i1}\xi + \ldots + a_{i4}\xi^4}{d} \quad \text{for } i = 2, \ldots, 5$$

with rational integers a_{ij}. Denote by $I(X_2, \ldots, X_5)$ the corresponding index form. For each solution $(x_2, \ldots, x_5) \in \mathbb{Z}^4$ of the index form equation

$$I(x_2, \ldots, x_5) = \pm 1 \tag{3}$$

consider $\vartheta = x_2\omega_2 + \ldots + x_5\omega_5$. We can write ϑ as

$$\vartheta = \frac{y_0 + y_1\xi + \ldots + y_4\xi^4}{d} \tag{4}$$

with $y_0, y_1, \ldots, y_4 \in \mathbb{Z}$. In our algorithm we are going to determine $y_1, \ldots, y_4$. The corresponding $x_2, \ldots, x_5$ can be easily determined by using the above representations of $\omega_2, \ldots, \omega_5$.

Consider the linear forms

$$l_{ij}(\underline{Y}) = (\xi^{(i)} - \xi^{(j)})Y_1 + \ldots + ((\xi^{(i)})^4 - (\xi^{(j)})^4)Y_4$$

for distinct i, j with $1 \le i, j \le 5$. It follows from (2) and (4) that ϑ represented in the form (4) generates a power integral basis in K if and only if $\underline{y} = (y_1, \ldots, y_4)$ satisfies the equation

$$\prod_{\substack{1 \le i,j \le 5 \\ i \ne j}} l_{ij}(\underline{y}) = d^{18} D_{K/\mathbb{Q}}(\xi) \quad \text{in } \underline{y} \in \mathbb{Z}^4. \tag{5}$$

Consider the subfield $L_{i,j} = \mathbb{Q}(\xi^{(i)} + \xi^{(j)}, \xi^{(i)}\xi^{(j)})$ of $K^{(i)}K^{(j)}$. The groups M_{20}, A_5 and S_5 are doubly transitive. Hence the field $K^{(i)}K^{(j)}$ is of degree $5 \cdot 4 = 20$ over $\mathbb{Q}$. The elements of $L_{i,j}$ remain fixed under the action $(i, j) \to (j, i)$ of the Galois group, thus $L_{i,j}$ is a proper subfield of $K^{(i)}K^{(j)}$. Since $\mathbb{Q}(\xi^{(i)}, \xi^{(j)})$ is a quadratic extension of $L_{i,j}$, in our case $L_{i,j}$ is of degree 10 over $\mathbb{Q}$. (Note that in our examples in Section 7 we had $L_{i,j} = \mathbb{Q}(\xi^{(i)} + \xi^{(j)}) = \mathbb{Q}(\xi^{(i)}\xi^{(j)})$.)

Denote by $\lambda^{(i,j)}$ the conjugate of any $\lambda = \lambda^{(1,2)} \in L_{1,2}$ corresponding to $\xi^{(i)} + \xi^{(j)}, \xi^{(i)}\xi^{(j)}$ $(1 \le i < j \le 5)$ and for simplicity let $\lambda^{(j,i)} = \lambda^{(i,j)}$. It follows from (4) that

$$\delta = \frac{d(\vartheta^{(1)} - \vartheta^{(2)})}{\xi^{(1)} - \xi^{(2)}}$$

is an integer in the field $L_{1,2}$. In view of (4), equation (5) can be written in the form

$$\prod_{1 \le i < j \le 5} \delta^{(i,j)} = \pm d^9.$$

This is just a norm equation in $L_{1,2}$ over $\mathbb{Q}$. Hence there exist an integer γ of norm $\pm d^9$ and a unit η in $L_{1,2}$ such that

$$\delta^{(i,j)} = \gamma^{(i,j)} \eta^{(i,j)} \tag{6}$$

for any i, j with $1 \le i < j \le 5$. Note that the following computations must be performed for a complete set of non-associate elements of norm $\pm d^9$.

For any distinct i, j, k we have

$$l_{ij}(\underline{Y}) + l_{jk}(\underline{Y}) + l_{ki}(\underline{Y}) = 0. \tag{7}$$

Putting

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

we deduce from (4), (6) and (7) that

$$\alpha^{(ijk)} \frac{\eta^{(i,j)}}{\eta^{(i,k)}} + \alpha^{(kji)} \frac{\eta^{(k,j)}}{\eta^{(k,i)}} = 1. \tag{8}$$

Unit equations of this type were considered in [25], [31] and [32] as equations in the normal closure of K or in $K^{(i)}K^{(j)}K^{(k)}$, and the corresponding unknown units $\eta^{(i,j)}/\eta^{(i,k)}$, $\eta^{(k,j)}/\eta^{(k,i)}$ were represented in a system of fundamental units of that field. In the present situation, if e.g. the Galois group of K is S_5, then the number of fundamental units is $5 \cdot 4 \cdot 3 - 1 = 59$. As we shall see below, the new approach of [27] requires much fewer generators.

Denote by $\{\varepsilon_1, \dots, \varepsilon_9\}$ a set of fundamental units in $L_{1,2}$. Then there are rational integer exponents $a_1, \dots, a_9$ such that

$$\eta^{(i,j)} = \pm(\varepsilon_1^{(i,j)})^{a_1} \dots (\varepsilon_9^{(i,j)})^{a_9}$$

for any (i, j) $(1 \le i < j \le 5)$. Introduce

$$\nu_h^{(ijk)} = \frac{\varepsilon_h^{(i,j)}}{\varepsilon_h^{(i,k)}} \quad (h = 1, \dots, 9), \qquad \mu^{(ijk)} = \prod_{h=1}^{9} (\nu_h^{(ijk)})^{a_h} \tag{9}$$

and

$$\beta^{(ijk)} = \alpha^{(ijk)} \mu^{(ijk)}. \tag{10}$$

Then the unit equation (8) can be written in the form

$$\beta^{(ijk)} + \beta^{(kji)} = 1 \tag{11}$$

or

$$\alpha^{(ijk)}(\nu_1^{(ijk)})^{a_1} \dots (\nu_9^{(ijk)})^{a_9} + \alpha^{(kji)}(\nu_1^{(kji)})^{a_1} \dots (\nu_9^{(kji)})^{a_9} = 1. \tag{12}$$

In view of our construction we have only 9 generators for both unknown units, with the same exponents $a_1, \dots, a_9$.

We note that the column vectors of the 60 by 9 matrix

$$(\log |\nu_h^{(ijk)}|)\,{}_{\substack{1\le i,j,k\le 5\\ 1\le h\le 9}} \tag{13}$$

are linearly independent, where all distinct indices i, j, k between 1 and 5 are considered. This follows by using the facts that all 9th order minors of the 10 by 9 matrix

$$(\log |\varepsilon_h^{(i,j)}|)\,{}_{\substack{1\le i<j\le 5\\ 1\le h\le 9}}$$

are different from zero and that the sum of the row vectors of this matrix is the zero vector.

In [27] it was shown in full generality that, in contrast to the arguments of [25], [31] and [32], it suffices to deal with some (in [27] well defined) unit equations of shape (8) only, which come from relations of the form (7) having the property $\sigma(\xi^{(i)}) = \xi^{(i)}$, $\sigma(\xi^{(j)}) = \xi^{(k)}$ for some element σ of the Galois group. In our case this holds for each i, j, k, since the Galois group is doubly transitive. Further, in this case it is enough to solve a single unit equation, say equation (12) for $i = 1$, $j = 2$, $k = 3$. Indeed, if (12) is already solved in $a_1, \dots, a_9$ for this choice of i, j, k, then we consider the system of linear equations

$$l_{1j}(\underline{y}) = \pm(\xi^{(1)} - \xi^{(j)})\gamma^{(1,j)}(\varepsilon_1^{(1,j)})^{a_1} \dots (\varepsilon_9^{(1,j)})^{a_9} \tag{14}$$

in $\underline{y} = (y_1, \dots, y_4)$ for $j = 2, 3, 4$ and 5. These linear equations are conjugate to each other over $\mathbb{Q}$. The linear forms $l_{1j}(\underline{Y})$, $j = 2, \dots, 5$, being linearly independent, (14) enables us to determine the unknowns $\underline{y} = (y_1, \dots, y_4)$ from the exponent vectors $(a_1, \dots, a_9)$, and hence (3) can be completely solved.

3. Application of Baker's method. Now we apply Baker's method to the unit equation (12). Taking logarithms for each distinct i, j, k we obtain

$$a_1 \log |\nu_1^{(ijk)}| + \dots + a_9 \log |\nu_9^{(ijk)}| = \log |\mu^{(ijk)}|.$$

Consider the above equations (for each distinct i, j, k) as a system of linear equations in $a_1, \dots, a_9$. As we have seen above, the column vectors of the

matrix consisting of the coefficients of $a_1, \dots, a_9$ are linearly independent. Hence we can select nine triples (i, j, k) such that the left hand sides of the corresponding linear equations are linearly independent. Let M be the 9 by 9 matrix composed of these coefficients. Denote by (i_0, j_0, k_0) the triple (i, j, k) for which $|\log|\mu^{(ijk)}||$ attains its maximum. Then, by multiplication by the inverse of M we can express the variables $a_1, \dots, a_9$ and we conclude that

$$A = \max_{1 \le h \le 9} |a_h| \le c_1 |\log|\mu^{(i_0 j_0 k_0)}||$$

where c_1 is 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 the nine equations should be selected so that c_1 becomes as small as possible. Now if $|\mu^{(i_0 j_0 k_0)}| < 1$ then $\log|\mu^{(i_0 j_0 k_0)}| \le -A/c_1$, and if $|\mu^{(i_0 j_0 k_0)}| > 1$ then the same holds for $\mu^{(i_0 k_0 j_0)} = 1/\mu^{(i_0 j_0 k_0)}$. Hence we conclude that $|\mu^{(i_0 j_0 k_0)}|$ is small for a certain triple (i_0, j_0, k_0). For simplicity we omit the subindices in the following, that is, we assume

$$\log|\mu^{(ijk)}| \le -A/c_1.$$

Set $c_2 = |\alpha^{(ijk)}|$. Then, using the inequality $|\log x| \le 2|x-1|$ holding for $|x-1| < 0.795$, we deduce from (12) that

$$\begin{aligned} (15) \qquad & |\log|\alpha^{(kji)}| + a_1 \log|\nu_1^{(kji)}| + \ldots + a_9 \log|\nu_9^{(kji)}|| \\ & = |\log|\alpha^{(kji)}\mu^{(kij)}|| \le 2 \cdot |1 - |\alpha^{(kji)}\mu^{(kij)}|| \\ & \le 2 \cdot |1 - (\alpha^{(kji)}\mu^{(kij)})| = 2 \cdot |\alpha^{(ijk)}\mu^{(ijk)}| \le 2c_2 \exp(-A/c_1), \end{aligned}$$

provided that the right hand side is < 0.795, but in the opposite case we get a much better estimate for A. In our examples the terms in the above linear form in logarithms were linearly independent over $\mathbb{Q}$, and applying the estimates of Baker and Wüstholz [1] we obtained a lower estimate

$$|\log|\alpha^{(kji)}| + a_1 \log|\nu_1^{(kji)}| + \ldots + a_9 \log|\nu_9^{(kji)}|| > \exp(-C_0 \log A)$$

with a large constant C_0. This inequality, compared with the upper bound (15), implies an upper bound for A, that was about 10^{82}, 10^{83} in our examples. Note that if in the above linear form $\log|\alpha^{(kji)}|$ is linearly dependent over $\mathbb{Q}$ on the other terms, then we can reduce the number of variables in the form.

4. Reduction of the bounds. For a triple (k, j, i) of distinct indices $1 \le k, j, i \le 5$, consider the lattice $\mathcal{L}$ spanned by the columns of the 11 by 10 matrix

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \\ C\log|\alpha^{(kji)}| & C\log|\nu_1^{(kji)}| & \dots & C\log|\nu_9^{(kji)}| \end{pmatrix}$$

where the constant C will be specified later. Denote by b_1 the first vector of the LLL reduced basis of $\mathcal{L}$. Now Lemma 1 of Gaál and Pohst [22] yields the following:

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

$$|b_1| > \sqrt{11}\cdot 2^{9/2}A_0 \tag{16}$$

then for all solutions of the inequality

$$|\log|\alpha^{(kji)}| + a_1\log|\nu_1^{(kji)}| + \ldots + a_9\log|\nu_9^{(kji)}|| \le 2c_2\exp(-A/c_1)$$

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 have to use Lemma 1 of [22] for a lower dimensional lattice and 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 30 cases to consider.

We apply the above Lemma 1 in 4–5 steps to reduce the bounds obtained by Baker's method. In each step we take as A_0 the previous bound (initially the Baker's bound), apply Lemma 1 and get a smaller bound. To ensure (16) we have to define C large enough, usually A_0^{10} is suitable. The reduction is very efficient in the first and second step, when the new bound is about the logarithm of the previous bound, and after 4–5 steps the new bound does not yield an improvement any more. The final reduced bounds in our examples were about 130–200. It was especially hard to perform the first reduction step, where we had to take $C = 10^{900}$ and we had to use an accuracy of 1300 digits. For more details and CPU times see the last section.

5. Final enumeration. In this section we use the construction of Gaál and Pohst [22], which is in fact a variant of Wildanger's method [32]. Note that Wildanger solved unit equations where the generators of the groups are fundamental units of a field. In our case, the units are composed of $\nu_1^{(ijk)},\ldots,\nu_9^{(ijk)}$, hence the situation is much more complicated.

For a triple $I = (i,j,k)$ of distinct indices $1 \le i,j,k \le 5$ set

$$\beta^{(I)} = \beta^{(ijk)}, \qquad \alpha^{(I)} = \alpha^{(ijk)}$$

and

$$\nu_h^{(I)} = \nu_h^{(ijk)} \quad \text{for } h = 1, \dots, 9.$$

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

1. if $(i,j,k) \in I^*$ then either $(k,i,j) \in I^*$ or $(k,j,i) \in I^*$,
2. if $(i,j,k) \in I^*$ then either $(j,k,i) \in I^*$ or $(j,i,k) \in I^*$,
3. the vectors

$$\underline{e}_h = \begin{pmatrix} \log|\nu_h^{(I_1)}| \\ \vdots \\ \log|\nu_h^{(I_t)}| \end{pmatrix} \quad \text{for } h = 1, \dots, 9$$

are linearly independent.

Since the matrix (13) is of rank 9, taking sufficiently many tuples, the last condition can be satisfied. Note that taking a minimal set of tuples satisfying the above conditions reduces the amount of necessary computations considerably. Set

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

By our notation we have

$$\underline{b} = \underline{g} + a_1\underline{e}_1 + \ldots + a_9\underline{e}_9. \tag{17}$$

Denote by A_r the reduced bound obtained in the previous section. Let

$$\log S_0 = \max_{I \in I^*}(|\log|\alpha^{(I)}|| + A_r|\log|\nu_1^{(I)}|| + \ldots + A_r|\log|\nu_9^{(I)}||).$$

Then in view of our notation (9), (10), for any tuple $I = (i,j,k) \in I^*$ we have

$$1/S_0 \le |\beta^{(I)}| \le S_0. \tag{18}$$

In our examples we had $S_0 = 10^{691}$ and $S_0 = 10^{1545}$, respectively.

The next lemma (cf. Gaál and Pohst [22]) describes how we can replace S_0 by a smaller constant.

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

$$1/S \le |\beta^{(I)}| \le S \quad \textit{for all } I \in I^*.$$

Then either

$$1/s \le |\beta^{(I)}| \le s \quad \textit{for all } I \in I^* \tag{19}$$

or there is an $I = (i,j,k) \in I^*$ with

$$|\beta^{(I)} - 1| \le 1/(s-1).$$

Since our notation is somewhat different from that of [22] we repeat here the proof of this lemma.

P r o o f. Assume that the tuple $(i,j,k) \in I^*$ violates (19). Then either $1/S \le |\beta^{(ijk)}| \le 1/s$, which by (11) implies

$$|\beta^{(kji)} - 1| \le 1/s, \tag{20}$$

or $s \le |\beta^{(ijk)}| \le S$, whence

$$|\beta^{(jki)} - 1| = |\beta^{(ikj)}| = |1/\beta^{(ijk)}| \le 1/s.$$

Note that if the tuple (k,j,i) is not in I^*, but $(k,i,j) \in I^*$, then using $\beta^{(kij)} = 1/\beta^{(kji)}$ by (20) we have

$$|\beta^{(kij)} - 1| \le 1/(s-1),$$

and we can proceed similarly if the tuple (j,k,i) is not in I^*, but $(j,i,k) \in I^*$. ∎

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 $a_1, \dots, a_9$ for which

$$1/S \le |\beta^{(I)}| \le S \quad \text{for all } I \in I^* \quad \text{and} \quad |\beta^{(I_{t_0})} - 1| \le 1/(s-1). \tag{21}$$

We consider the enumeration of the above set H_{t_0} in detail, this being the critical step of the algorithm. Assume that $2 < s < S$ and set

$$\lambda_p = \begin{cases} \dfrac{1}{\log S} & \text{for } p \ne t_0,\ 1 \le p \le t, \\ \dfrac{1}{\log \frac{s-1}{s-2}} & \text{for } p = t_0. \end{cases}$$

Set

$$\varphi_{t_0}(\underline{b}) = \begin{pmatrix} \lambda_1 \log|\beta^{(I_1)}| \\ \vdots \\ \lambda_t \log|\beta^{(I_t)}| \end{pmatrix}, \quad \varphi_{t_0}(\underline{g}) = \begin{pmatrix} \lambda_1 \log|\alpha^{(I_1)}| \\ \vdots \\ \lambda_t \log|\alpha^{(I_t)}| \end{pmatrix}$$

and

$$\varphi_{t_0}(\underline{e}_h) = \begin{pmatrix} \lambda_1 \log|\nu_h^{(I_1)}| \\ \vdots \\ \lambda_t \log|\nu_h^{(I_t)}| \end{pmatrix} \quad \text{for } h = 1, \dots, 9.$$

Since $\underline{e}_1, \dots, \underline{e}_9$ are linearly independent, so are the images $\varphi_{t_0}(\underline{e}_1), \dots$ $\dots, \varphi_{t_0}(\underline{e}_9)$ as well, and (17) implies

$$\varphi_{t_0}(\underline{b}) = \varphi_{t_0}(\underline{g}) + a_1\varphi_{t_0}(\underline{e}_1) + \dots + a_9\varphi_{t_0}(\underline{e}_9).$$

We deduce from (21) that

$$|\log|\beta^{(I_p)}|| \le \begin{cases} \log S & \text{if } p \ne t_0, \\ \log \dfrac{s-1}{s-2} & \text{if } p = t_0. \end{cases}$$

Consequently, for the norm of the vector $\varphi_{t_0}(\underline{b})$ we have

$$\|\varphi_{t_0}(\underline{g}) + a_1\varphi_{t_0}(\underline{e}_1) + \ldots + a_9\varphi_{t_0}(\underline{e}_9)\|_2^2 = \|\varphi_{t_0}(\underline{b})\|_2^2 = \sum_{p=1}^{t} \lambda_p^2 \log^2 |\beta^{(I_p)}| \le t. \tag{22}$$

Hence we have shown that for any $(a_1, \ldots, a_9) \in H_{t_0}$ the inequality (22) holds. This inequality defines an *ellipsoid*. The lattice points contained in this ellipsoid can be enumerated by using the algorithm of Fincke and Pohst [5]. The enumeration is usually very fast, but it is essential that the "improved" version (cf. [5]) of the algorithm should be used, involving LLL reduction.

It is important to note that in our examples the vector $\underline{g}$ was linearly dependent on $\underline{e}_1, \ldots, \underline{e}_9$ over $\mathbb{R}$, that is, we had

$$\underline{g} = r_1 \cdot \underline{e}_1 + \ldots + r_9 \cdot \underline{e}_9$$

for certain real numbers $r_1, \ldots, r_9$. That is, in view of (22) we had to enumerate the solutions of the form $y_h = a_h + r_h$ $(1 \le h \le 9)$ of the ellipsoid

$$\|y_1\varphi_{t_0}(\underline{e}_1) + \ldots + y_9\varphi_{t_0}(\underline{e}_9)\|_2^2 \le t,$$

and from the values of y_h we determined the a_h. This made a bit more complicated the Cholesky decomposition involved in the Fincke–Pohst algorithm.

Applying the above procedure we choose appropriate constants $S_0 > S_1 > \ldots > S_k$. In each step we take $S = S_i, s = S_{i+1}$ and enumerate the lattice points in the corresponding ellipsoids. The initial constant is given by the reduced bound (18), the last constant S_k should be made as small as possible, so that the exponents with

$$1/S_k \le |\beta^{(I)}| \le S_k \quad \text{for all } I \in I^* \tag{23}$$

can be enumerated easily. Observe that the set (23) is also contained in an ellipsoid, namely, by (17) we have in $\mathbb{R}^t$

$$\|\underline{g} + a_1\underline{e}_1 + \ldots + a_9\underline{e}_9\|_2^2 = \|\underline{b}\|_2^2 \le t \cdot (\log S_k)^2. \tag{24}$$

In our examples we had $S_0 = 10^{691}$, resp. $S_0 = 10^{1545}$. Then we took $S_1 = 10^{50}, S_2 = 10^{20}, S_3 = 10^8, S_4 = 10^6, S_5 = 10^5, S_6 = 10^4, S_7 = 2500, S_8 = 500, S_9 = 100$. For more details and CPU times see the last section.

6. Sieving and test. As we shall see in the last section, by the enumeration of the ellipsoids the number of exponent vectors $(a_1, \dots, a_9)$ we have to consider is still very large. Hence it seems to be economical to insert a very simple modular test to eliminate almost all of these vectors.

We calculated a prime p, relatively prime to D_K, such that the defining polynomial $f(x)$ of the generating element ξ splits completely mod p, i.e.,

$$f(x) \equiv (x - r_1)(x - r_2)(x - r_3)(x - r_4)(x - r_5) \pmod{p}$$

with rational integers $r_1, \dots, r_5$. Hence $r_1, \dots, r_5$ can be indexed so that for a certain prime ideal $\wp$ in $\mathbb{Z}_K$ lying above p and for any i $(1 \le i \le 5)$ we have

$$\xi_i \equiv r_i \pmod{\wp}.$$

Then we can calculate integers $m^{(ijk)}, n_h^{(ijk)}$ $(h = 1, \dots, 9)$ for each triple (i, j, k) of distinct indices $1 \le i, j, k \le 5$ with

$$\alpha^{(ijk)} \equiv m^{(ijk)} \pmod{\wp}$$

and

$$\nu_h^{(ijk)} \equiv n_h^{(ijk)} \pmod{\wp} \quad (1 \le h \le 9).$$

Then equation (12) implies

$$m^{(ijk)}(n_1^{(ijk)})^{a_1} \dots (n_9^{(ijk)})^{a_9} + m^{(kji)}(n_1^{(kji)})^{a_1} \dots (n_9^{(kji)})^{a_9} \equiv 1 \pmod{p},$$

a congruence which is very easy and fast to test even for large exponents. In our computations only very few exponent vectors survived this test, and usually they were solutions of (12). As we mentioned in Section 2, in our situation it is sufficient to solve equation (12) for $i = 1$, $j = 2$, $k = 3$.

7. Numerical examples. Using our algorithm we computed all power integral bases in two *totally real quintic fields with Galois group* S_5. The method was implemented in Maple and was run on a 133Mhz Pentium PC. The defining polynomials, integral bases and fundamental units were computed by the KANT package [3]. In this section we detail our computational experiences.

Example 1. Consider the totally real quintic field $K = \mathbb{Q}(\xi)$ where ξ is defined by the polynomial

$$f(x) = x^5 - 5x^3 + x^2 + 3x - 1.$$

This field has discriminant $D_K = 24217 = 61 \cdot 397$, Galois group S_5, and

$$\omega_1 = 1, \quad \omega_2 = \xi, \quad \omega_3 = \xi^2, \quad \omega_4 = \xi^3, \quad \omega_5 = \xi^4 \tag{25}$$

is an integral basis. The element $\xi^{(1)} + \xi^{(2)}$ is defined by the polynomial

$$g(x) = x^{10} - 15x^8 + x^7 + 66x^6 + x^5 - 96x^4 - 7x^3 + 37x^2 + 12x + 1.$$

The field $L_{1,2} = \mathbb{Q}(\xi^{(1)} + \xi^{(2)}, \xi^{(1)}\xi^{(2)})$ is generated by $\varrho = \xi^{(1)} + \xi^{(2)}$ only.

An integral basis of $L_{1,2}$ is

$$\{1, \varrho, \varrho^2, \varrho^3, \varrho^4, \varrho^5, \varrho^6, \varrho^7, \varrho^8,$$
$$(9 + 27\varrho + 43\varrho^2 + 20\varrho^3 + 37\varrho^4 + 5\varrho^5 + 32\varrho^6 + 3\varrho^7 + 26\varrho^8 + \varrho^9)/47\}$$

and the discriminant of $L_{1,2}$ is $D_{L_{1,2}} = 61^3 \cdot 397^3$. The coefficients of the fundamental units of $L_{1,2}$ with respect to the above integral basis are

$$\begin{array}{rrrrrrrrrr}
(21, & 107, & 192, & -5, & -120, & -40, & 84, & 20, & 30, & -60) \\
(16, & 99, & 139, & -56, & -113, & -7, & 56, & 9, & 14, & -30) \\
(10, & 4, & 65, & 197, & 85, & -110, & 56, & 34, & 50, & -90) \\
(21, & 35, & 196, & 346, & 94, & -206, & 129, & 66, & 97, & -177) \\
(0, & -53, & -31, & 200, & 145, & -90, & 14, & 24, & 35, & -60) \\
(8, & 24, & 40, & 33, & -1, & -27, & 25, & 10, & 15, & -28) \\
(15, & 13, & 118, & 248, & 78, & -143, & 84, & 45, & 66, & -120) \\
(0, & 1, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0) \\
(4, & 19, & 42, & 0, & -26, & -8, & 17, & 4, & 6, & -12)
\end{array}$$

Note that the element $\xi^{(1)}\xi^{(2)}$ has coefficients

$$(-26, -26, -197, -410, -130, 238, -140, -75, -110, 200)$$

in the above integral basis of $L_{1,2}$.

Baker's method gave the bound $A_0 = 10^{82}$ for A. This bound was reduced according to the following table:

Step	A_0	C	New bound
I	10^{82}	10^{900}	3196
II	3196	10^{55}	205
III	205	10^{43}	163
IV	163	$2 \cdot 10^{40}$	153
V	153	$2 \cdot 10^{35}$	133

In the first reduction step we had to use 1300 digits accuracy, in the following steps 100 digits were enough. As mentioned before, we had to perform the reduction in 30 possible cases for the indices (k, j, i). The CPU time for the first step was about 10 hours. The following steps took only some minutes. The final reduced bound 133 gave $S_0 = 10^{691}$ (cf. (18)) to start the final enumeration.

For the final enumeration we used the set of 15 ellipsoids defined by

$$I^* = \{(1,2,3), (2,1,3), (3,1,2), (1,2,4), (2,1,4), (4,1,2), (1,2,5),$$
$$(2,1,5), (5,1,2), (1,3,4), (3,1,4), (4,1,3), (3,4,5), (4,5,3), (5,3,4)\}.$$

Parallel to the enumeration we used sieving modulo $p = 3329$, which was suitable since

$$f(x) \equiv (x + 1752)(x + 1067)(x + 1695)(x + 379)(x + 1765) \pmod{3329}.$$

In the following table we summarize the final enumeration using the ellipsoid method. In the table we display S, s, the approximate number of exponent vectors $(a_1, \dots, a_9)$ enumerated in the 15 ellipsoids, and the number of the exponent vectors that survived the modular test. The last line represents the enumeration of the single ellipsoid (24).

Step	S	s	Enumerated	Survived
I	10^{691}	10^{50}	0	0
II	10^{50}	10^{20}	0	0
III	10^{20}	10^{10}	$15 \cdot 5000$	94
IV	10^{10}	10^{8}	$15 \cdot 1900$	39
V	10^{8}	10^{6}	$15 \cdot 30000$	532
VI	10^{6}	10^{5}	$15 \cdot 30000$	563
VII	10^{5}	10^{4}	$15 \cdot 72000$	1413
VIII	10000	2500	$15 \cdot 50000$	946
IX	2500	500	$15 \cdot 66000$	1300
X	500	100	$15 \cdot 53000$	1032
XI	100	0	1792512	2135

Steps I–II were very fast, then III–IV took about one hour, V–X about two hours each. The last step XI was again very time consuming, taking about 8 hours of CPU time. We believe that using a finer splitting of the interval the CPU time can be slightly improved, but at least 8 hours of CPU time is necessary.

From the surviving exponent vectors we calculated the solutions of the index form equation corresponding to the basis (25):

$$
\begin{aligned}
&(x_2, x_3, x_4, x_5)\\
&\quad = (0,1,0,0),\ (0,2,1,-1),\ (0,4,0,-1),\ (0,5,0,-1),\\
&\qquad (1,-5,0,1),\ (1,-4,0,1),\ (1,-1,0,0),\ (1,0,0,0),\\
&\qquad (1,1,-2,-1),\ (1,4,0,-1),\ (2,-1,-1,0),\ (2,4,-1,-1),\\
&\qquad (2,9,-1,-2),\ (2,15,-1,-3),\ (2,10,-1,-2),\ (3,4,-1,-1),\\
&\qquad (3,5,-1,-1),\ (3,9,-1,-2),\ (3,10,-1,-2),\ (3,14,-1,-3),\\
&\qquad (3,18,-2,-4),\ (4,-1,-1,0),\ (4,0,-1,0),\ (4,5,-1,-1),\\
&\qquad (4,24,-2,-5),\ (4,29,-2,-6),\ (5,-4,-1,1),\ (5,8,-2,-2),\\
&\qquad (5,33,-2,-7),\ (7,5,-2,-1),\ (7,9,-2,-2),\ (7,14,-2,-3),\\
&\qquad (9,18,-3,-4),\ (11,-13,-2,3),\ (12,27,-4,-6),\ (17,28,-6,-6),\\
&\qquad (33,30,-51,-26),\ (83,170,-25,-39),\ (124,246,-40,-55).
\end{aligned}
$$

Note that if (x_2, x_3, x_4, x_5) is a solution, then so also is $(-x_2, -x_3, -x_4, -x_5)$ but we list only one of them.

EXAMPLE 2. Consider now the totally real quintic field $K = \mathbb{Q}(\xi)$ where ξ is defined by the polynomial

$$f(x) = x^5 - 6x^3 + x^2 + 4x + 1.$$

This field has discriminant $D_K = 36497$ (a prime), Galois group S_5, and

$$\omega_1 = 1, \quad \omega_2 = \xi, \quad \omega_3 = \xi^2, \quad \omega_4 = \xi^3, \quad \omega_5 = \xi^4 \tag{26}$$

is an integral basis. The element $\xi^{(1)} + \xi^{(2)}$ is defined by the polynomial

$$g(x) = x^{10} - 18x^8 + x^7 + 96x^6 - 23x^5 - 169x^4 + 44x^3 + 93x^2 - 21x - 11.$$

An integral basis of the field $L_{1,2}$ generated by $\varrho = \xi^{(1)} + \xi^{(2)}$ is

$$\begin{aligned}\{&1, \varrho, \varrho^2, \varrho^3, \varrho^4, \varrho^5, \varrho^6, \varrho^7, \varrho^8,\\ &(44074 + 62732\varrho + 54220\varrho^2 + 50326\varrho^3 + 32569\varrho^4 + 35601\varrho^5\\ &+ 31671\varrho^6 + 29542\varrho^7 + 8471\varrho^8 + \varrho^9)/79083\}\end{aligned}$$

and the discriminant of $L_{1,2}$ is $D_{L_{1,2}} = 36497^3$. The coefficients of the fundamental units of $L_{1,2}$ with respect to the above integral basis are

$$\begin{array}{rrrrrrrrrr}
(456, & 651, & 564, & 527, & 340, & 367, & 328, & 307, & 88, & -821)\\
(3077, & 4375, & 3797, & 3534, & 2273, & 2480, & 2214, & 2066, & 592, & -5527)\\
(7000, & 9968, & 8645, & 8026, & 5166, & 5648, & 5040, & 4701, & 1347, & -12577)\\
(4354, & 6185, & 5339, & 4980, & 3222, & 3504, & 3124, & 2917, & 836, & -7804)\\
(457, & 651, & 564, & 527, & 340, & 367, & 328, & 307, & 88, & -821)\\
(3559, & 5061, & 4378, & 4077, & 2629, & 2867, & 2558, & 2387, & 684, & -6386)\\
(4171, & 5937, & 5144, & 4773, & 3075, & 3366, & 3002, & 2799, & 802, & -7489)\\
(4642, & 6606, & 5716, & 5308, & 3423, & 3743, & 3338, & 3113, & 892, & -8329)\\
(151, & 212, & 182, & 176, & 115, & 120, & 107, & 101, & 29, & -270)
\end{array}$$

Note that the element $\xi^{(1)}\xi^{(2)}$ has coefficients

$$(-4354, -6185, -5339, -4980, -3222, -3504, -3124, -2917, -836, 7804)$$

in the above integral basis of $L_{1,2}$.

Baker's method gave the bound $A_0 = 10^{83}$ for A. This bound was reduced according to the following table:

Step	A_0	C	New bound
I	10^{83}	10^{900}	4078
II	4078	10^{55}	263
III	263	10^{44}	214
IV	214	10^{42}	204

The reduction took about the same CPU time as in Example 1. The final reduced bound 204 gave $S_0 = 10^{1545}$ (cf. (18)) to start the final enumeration.

For the final enumeration we used the set of the same 15 ellipsoids as in Example 1.

Parallel to the enumeration we used sieving modulo $p = 2819$, which was suitable since

$$f(x) \equiv (x+573)(x+2401)(x+926)(x+2266)(x+2291) \pmod{2819}.$$

In the following table we summarize the final enumeration using the ellipsoid method. The notation is the same as in Example 1.

Step	S	s	Enumerated	Survived
I	10^{1545}	10^{50}	0	0
II	10^{50}	10^{20}	0	0
III	10^{20}	10^{15}	0	0
IV	10^{15}	10^{10}	$15 \cdot 200$	2
V	10^{10}	10^{8}	$15 \cdot 800$	12
VI	10^{8}	10^{6}	$15 \cdot 13000$	299
VII	10^{6}	10^{5}	$15 \cdot 13500$	288
VIII	10^{5}	10^{4}	$15 \cdot 30000$	634
IX	10000	2500	$15 \cdot 20000$	445
X	2500	500	$15 \cdot 28000$	624
XI	500	100	$15 \cdot 22000$	515
XII	100	0	711746	992

Here the necessary CPU time was somewhat less than in Example 1, this can be seen by looking at the number of vectors tested.

From the surviving exponent vectors we calculated the solutions of the index form equation corresponding to the basis (26):

$$\begin{aligned}(x_2, x_3, x_4, x_5) &= (1,-6,0,1),\ (1,0,0,0),\ (2,-6,0,1),\ (2,-5,0,1),\\ &\quad (3,-11,0,2),\ (3,-5,0,1),\ (3,0,-5,2),\ (4,-5,-1,1),\\ &\quad (4,0,-3,-1),\ (4,5,-1,-1),\ (6,-6,-1,1),\ (6,15,-2,-3),\\ &\quad (7,-12,-1,2),\ (7,-11,-1,2),\ (8,-12,-1,2),\ (9,-18,-1,3),\\ &\quad (9,-17,-1,3),\ (11,-23,-1,4),\ (13,-18,-2,3),\ (15,-24,-2,4),\\ &\quad (16,-23,-2,4),\ (19,-41,-2,7),\ (31,-46,-4,8),\ (53,62,-14,-13),\\ &\quad (80,-159,-9,27),\ (115,-166,-15,29).\end{aligned}$$

Again, if (x_2, x_3, x_4, x_5) is a solution, then so also is $(-x_2, -x_3, -x_4, -x_5)$ but we list only one of them.

References

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

[2] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1993.

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

[4] J. H. Evertse and K. Győry, *Decomposable form equations*, in: New Advances in Transcendence Theory, A. Baker (ed.), Cambridge Univ. Press, 1988, 175–202.

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

[6] I. Gaál, *Inhomogeneous discriminant form equations and integral elements with given discriminant over finitely generated integral domains*, Publ. Math. Debrecen 34 (1987), 109–122.

[7] —, *Power integral bases in orders of families of quartic fields*, ibid. 42 (1993), 253–263.

[8] —, *Computing all power integral bases in orders of totally real cyclic sextic number fields*, Math. Comp. 65 (1996), 801–822.

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

[10] —, *Power integral bases in algebraic number fields*, Proc. Conf. Mátraháza, 1995, Ann. Univ. Sci. Budapest Eötvös Sect. Comp., to appear.

[11] —, *Application of Thue equations to computing power integral bases in algebraic number fields*, in: Algorithmic Number Theory (Talence, 1996), H. Cohen (ed.), Lecture Notes in Comput. Sci. 1122, Springer, 1996, 151–155.

[12] —, *Power integral bases in composits of number fields*, Canad. Math. Bull. 41 (1998), 158–165.

[13] —, *Power integral bases in algebraic number fields*, in: Number Theory, Walter de Gruyter, 1998, 243–254.

[14] —, *Solving index form equations in fields of degree nine with cubic subfields*, to appear.

[15] 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.

[16] —, —, —, *On the resolution of index form equations in biquadratic number fields, II*, ibid. 38 (1991), 35–51.

[17] —, —, —, *On the resolution of index form equations in biquadratic number fields, III. The bicyclic biquadratic case*, ibid. 53 (1995), 100–114.

[18] —, —, —, *On the resolution of index form equations in quartic number fields*, J. Symbolic Comput. 16 (1993), 563–584.

[19] —, —, —, *Simultaneous representation of integers by a pair of ternary quadratic forms—with an application to index form equations in quartic number fields*, J. Number Theory 57 (1996), 90–104.

[20] 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.

[21] —, —, *Power integral bases in a parametric family of totally real quintics*, Math. Comp. 66 (1997), 1689–1696.

[22] —, —, *On the resolution of relative Thue equations*, to appear.

[23] I. Gaál and N. Schulte, *Computing all power integral bases of cubic number fields*, Math. Comp. 53 (1989), 689–696.

[24] M. N. Gras, *Non monogénéité de l'anneau des entiers des extensions cycliques de* $\mathbb{Q}$ *de degré premier* $l \geq 5$, J. Number Theory 23 (1986), 347–353.

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

[26] —, *On norm form*, *discriminant form and index form equations*, in: Topics in Classical Number Theory, Colloq. Math. Soc. János Bolyai 34, North-Holland, 1984, 617–676.

[27] —, *Bounds for the solutions of decomposable form equations*, Publ. Math. Debrecen 52 (1998), 1–31.

[28] —, *Recent bounds for the solutions of decomposable form equations*, in: Number Theory, Walter de Gruyter, 1998, 255–270.

[29] M. Klebel, *Zur Theorie der Potenzganzheitsbases bei relativ galoisschen Zahlkörpern*, Dissertation, Univ. Augsburg, 1995.

[30] D. Koppenhöfer, *Über projektive Darstellungen von Algebren kleinen Ranges*, Dissertation, Univ. Tübingen, 1994.

[31] N. P. Smart, *Solving discriminant form equations via unit equations*, J. Symbolic Comput. 21 (1996), 367–374.

[32] 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.

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

Received on 27.11.1998
and in revised form on 14.1.1999 (3519)