MATHEMATICS OF COMPUTATION
Volume 65, Number 214
April 1996, Pages 801–822

COMPUTING ALL POWER INTEGRAL BASES IN ORDERS OF TOTALLY REAL CYCLIC SEXTIC NUMBER FIELDS

ISTVÁN GAÁL

ABSTRACT. An algorithm is given for determining all power integral bases in orders of totally real cyclic sextic number fields. The orders considered are in most cases the maximal orders of the fields. The corresponding index form equation is reduced to a relative Thue equation of degree 3 over the quadratic subfield and to some inhomogeneous Thue equations of degree 3 over the rationals. At the end of the paper, numerical examples are given.

1. INTRODUCTION

Let K be a number field of degree n with ring of integers $\mathbb{Z}_K$. To decide whether K admits a *power integer basis*, that is an integer basis of the form $\{1, \gamma, \dots, \gamma^{n-1}\}$, and to determine all such γ, is a classical problem in algebraic number theory. This problem is equivalent to solving the corresponding *index form equation*, which is a decomposable form equation of degree $n(n-1)/2$ in $n-1$ variables, with coefficients in $\mathbb{Z}$.

In [17] the author and Schulte considered index form equations in *cubic* number fields. In this case the index form equation reduces to a cubic Thue equation.

The author, Pethő and Pohst in a series of papers [10, 11, 12, 13, 14, 15] considered the same question in *quartic* number fields. Finally, it turned out [16] that also in this case it is possible to reduce the problem of resolution of index form equations to the resolution of cubic and quartic Thue equations.

The index form is reducible if there are nontrivial subfields of the number field in question. For fields of higher degree the resolution of index form equations is only feasible if the index form is reducible. For this reason, we consider now this problem in a class of sextic number fields. In case of sextic number fields the index form equation has already 5 *variables and degree* 15. The most intensively studied class of sextic fields is the class of totally real cyclic sextic fields (cf. [20, 6]). These fields admit also a couple of nice properties. This is the reason why first of all we develop a method for *totally real cyclic sextic fields*. In this case the field K has both a quadratic subfield M and a cubic subfield L, and the index form has three factors.

Received by the editor May 2, 1994 and, in revised form, March 7, 1995.
1991 *Mathematics Subject Classification.* Primary 11Y50; Secondary 11Y40, 11D57.
Key words and phrases. Cyclic sextic number fields, index form equation, power bases.
This work was begun during the author's stay in Düsseldorf as a fellow of the Alexander von Humboldt Foundation and completed under the partial support of the Hungarian National Foundation for Scientific research Grant no. 1641/91.

Remark 1. Our algorithm is in fact applicable in all sextic fields having both a quadratic and a cubic subfield. If the field is not totally real, the procedure becomes simpler.

In order to be able to describe the factors of the index form in an appropriate way, we shall restrict ourselves to orders of the form

$$\mathcal{O} = \mathbb{Z}[1, \theta, \theta^2, \omega, \omega\theta, \omega\theta^2],$$

where $\{1, \omega\}$ is a basis of M and $\theta \in \mathbb{Z}_K$. Apart from very few exceptions (about 2%), the sextic fields with a quadratic subfield admit a relative power integral basis $\{1, \theta, \theta^2\}$ over the quadratic subfield (cf. Bergé, Martinet and Olivier [2] and the tables of Olivier [23, 24]), which implies, that $\mathcal{O}$ is the main order of the field. The situation is just a little bit worse for totally real cyclic sextic fields, but also in this case we have $\mathcal{O} = \mathbb{Z}_K$ for almost all fields (cf. [23]).

Remark 2. In the few exceptional cases (which occur only for large discriminants) we can represent the integers $\gamma \in \mathbb{Z}_K$ in the form

$$\gamma = \frac{x_0 + x_1\theta + x_2\theta^2 + y_0\omega + y_1\omega\theta + y_2\omega\theta^2}{d},$$

with $x_0, x_1, x_2, y_0, y_2, y_3 \in \mathbb{Z}$ and with a denominator $d \in \mathbb{Z}$ common for all $\gamma \in \mathbb{Z}_K$. In this case we obtain the equations (11), (12), (13) with right-hand sides f_1, f_2, f_3, respectively, with $f_1, f_2, f_3 \in \mathbb{Z}$ satisfying $f_1 f_2 f_3 = \pm d^{15}\sqrt{D_K}/\sqrt{D}$, where D_K is the discriminant of the field K and D is the discriminant of order $\mathcal{O}$, (cf. (1)). One has to consider all triples f_1, f_2, f_3 with this property. Our method with slight modifications works also in this case, but the CPU time needed is much more than in most nonexceptional cases.

The main goal of our method is to show that for totally real cyclic sextic fields the problem of resolution of the index form equation can be reduced to the resolution of certain Thue equations. More exactly, we obtain a *relative Thue equation* of degree 3 over the quadratic subfield M. Moreover, for each solution of the relative Thue equation we get an equation of degree 3, in 2 dominating and 1 nondominating variables being of the same nature, like an *inhomogeneous Thue equation*.

We remark that such inhomogeneous Thue equations were first considered by Sprindzuk [27]. He showed that Baker's method is applicable to equations of this type. The author [9] pointed out that the Baker–Davenport reduction method [1] is also similarly usable as in the case of Thue equations, and hence one can determine without difficulties the solutions of such equations. Until now, these results were only of theoretical importance; this is the first case in which such inhomogeneuos equations have found a practical application.

At the end of the paper we list all power integral bases of the first five totally real cyclic sextic number fields with smallest discriminants. In all our examples we have $\mathcal{O} = \mathbb{Z}_K$.

2. Preliminaries

Let M be a real quadratic number field, with integral basis $\{1, \omega\}$. Let $f \in \mathbb{Z}_M$ be a monic, irreducible, cubic polynomial, and denote by $\theta = \theta^{(1)}, \theta^{(2)}, \theta^{(3)}$ the roots of f. Assume that $K = \mathbb{Q}(\theta)$ is a *totally real cyclic sextic number field*. Let

$$\mathcal{O} = \mathbb{Z}[1, \theta, \theta^2, \omega, \omega\theta, \omega\theta^2].$$

Denote by L the cubic subfield of K. Let $\mathbb{Z}_K, \mathbb{Z}_M, \mathbb{Z}_L$ be the rings of integers of the number fields K, M, L, respectively. Denote by $\bar{\gamma}$ the conjugate of any $\gamma \in K$ over M.

Remark 3. The field K is the composite of its quadratic subfield M and of its cubic subfield L. With any primitive element ϱ of L, $\{1, \varrho, \varrho^2, \omega, \omega\varrho, \omega\varrho^2\}$ is obviously a basis of K. If we represent any $\gamma \in K$ in this basis, it is easy to see that $(\gamma - \bar{\gamma})/(\omega - \bar{\omega}) \in L$ holds.

Let $\theta^{(4)} = \overline{\theta^{(1)}}, \theta^{(5)} = \overline{\theta^{(2)}}, \theta^{(6)} = \overline{\theta^{(3)}}$. For any $\gamma \in K$ denote by $\gamma^{(i)}$ the conjugate of γ corresponding to $\theta^{(i)}$. Note that the generating element of the Galois group of K is σ, mapping any $\gamma \in K$ with conjugates $\{\gamma = \gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}, \gamma^{(4)}, \gamma^{(5)}, \gamma^{(6)}\}$ onto $\sigma(\gamma) \in K$ with conjugates $\{\gamma^{(5)}, \gamma^{(6)}, \gamma^{(4)}, \gamma^{(2)}, \gamma^{(3)}, \gamma^{(1)}\}$. Obviously, for any $\gamma \in K$ we have $\bar{\gamma} = \sigma^3(\gamma)$, and if $\gamma \in M$, then $\bar{\gamma} = \sigma(\gamma)$.

It is easily calculated that the discriminant D of $\mathcal{O}$ satisfies

$$\sqrt{D} = |N_{K/Q}(\theta^{(1)} - \theta^{(2)})(\omega - \bar{\omega})^3| \ . \tag{1}$$

Let $\underline{X} = (X_1, X_2, Y_0, Y_1, Y_2)$, define $L_i(\underline{X}) = X_1\theta^{(i)} + X_2(\theta^{(i)})^2 + Y_0\omega^{(i)} + Y_1\omega^{(i)}\theta^{(i)} + Y_2\omega^{(i)}(\theta^{(i)})^2$ $(1 \le i \le 6)$, and let

$$L_{ij}(\underline{X}) = L_i(\underline{X}) - L_j(\underline{X}) \ \ (1 \le i, j \le 6, i \ne j).$$

The *index form* corresponding to the basis $\{1, \theta, \theta^2, \omega, \omega\theta, \omega\theta^2\}$ of $\mathcal{O}$ is

$$I(\underline{X}) = I(X_1, X_2, Y_0, Y_1, Y_2) = \pm\frac{1}{\sqrt{D}} \prod_{1 \le i < j \le 6} L_{ij}(\underline{X}). \tag{2}$$

Our purpose is to find all solutions of the *index form equation*

$$I(\underline{x}) = I(x_1, x_2, y_0, y_1, y_2) = \pm 1 \ \text{ in } \ x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}. \tag{3}$$

This equation has only finitely many solutions (cf. [18]). An element $\gamma \in \mathcal{O}$ generates a power integral basis $\{1, \gamma, \gamma^2, \gamma^3, \gamma^4, \gamma^5\}$ if and only if the index of γ,

$$I(\gamma) = (\mathcal{O}^+ : \mathbb{Z}^+[\gamma]),$$

is equal to 1. Further, for any $x_0, x_1, x_2, y_0, y_2, y_3 \in \mathbb{Z}$ the index of

$$\gamma = x_0 + x_1\vartheta + x_2\vartheta^2 + y_0\omega + y_1\omega\vartheta + y_2\omega\vartheta^2 \tag{4}$$

satisfies

$$I(\gamma) = |I(x_1, x_2, y_0, y_1, y_2)|.$$

Hence, $\gamma \in \mathbb{Z}_K$ generates a power integral basis in K if and only if it is represented in the form (4) with an arbitrary $x_0 \in \mathbb{Z}$ and with a solution $(x_1, x_2, y_0, y_1, y_2)$ of (3).

3. The factors of the index form

In this section we split the 15 factors of the index form into 3 groups, and from these groups we build up the three factors with integer coefficients of the index form.

I. Taking the pairs $(i,j) = (1,2),(5,6),(3,1),(4,5),(2,3),(6,4)$, we can see that the forms $L_{ij}(\underline{X})$ in this group are just the six conjugates of $L_{12}(\underline{X})$. Since

$$L_{12}(\underline{X}) = (\theta^{(1)} - \theta^{(2)}) \left(X_1 + (\theta^{(1)} + \theta^{(2)})X_2 + \omega Y_1 + \omega(\theta^{(1)} + \theta^{(2)})Y_2 \right),$$

we have that the product of the six factors in this group is

$$N_{K/Q}(\theta^{(1)} - \theta^{(2)}) \cdot F_1(\underline{X}), \tag{5}$$

with

$$F_1(\underline{X}) = N_{K/Q} \left(X_1 + (\theta^{(1)} + \theta^{(2)})X_2 + \omega Y_1 + \omega(\theta^{(1)} + \theta^{(2)})Y_2 \right) \quad . \tag{6}$$

The form $F_1(\underline{X})$ is obviously primitive.

II. Take now the pairs $(i,j) = (1,5),(5,3),(3,4),(4,2),(2,6),(6,1)$. For these pairs the forms $L_{ij}(\underline{X})$ are just the six conjugates of $L_{15}(\underline{X})$. The product of these six factors is again a complete norm:

$$N_{K/Q} \left(\left(\theta^{(1)} - \theta^{(5)} \right) X_1 + \left((\theta^{(1)})^2 - (\theta^{(5)})^2 \right) X_2 + (\omega - \bar{\omega})Y_0 + \left(\omega\theta^{(1)} - \bar{\omega}\theta^{(5)} \right) Y_1 + \left(\omega(\theta^{(1)})^2 - \bar{\omega}(\theta^{(5)})^2 \right) Y_2 \right).$$

This form is not always primitive. If it is primitive, take $\alpha = 1$; otherwise, if the gcd of its coefficients in $\mathbb{Z}$ is $d > 1$, find all nonassociate integers in K of norm $\pm d$ (using the method of [8]) and let α be one of them, dividing all coefficients of $L_{15}(\underline{X})$ in $\mathbb{Z}_K$. Then the product of the six factors equals

$$N_{K/Q}(\alpha) \cdot F_2(\underline{X}), \tag{7}$$

with

$$F_2(\underline{X}) = N_{K/Q} \left(\frac{\theta^{(1)} - \theta^{(5)}}{\alpha} X_1 + \frac{(\theta^{(1)})^2 - (\theta^{(5)})^2}{\alpha} X_2 + \frac{\omega - \bar{\omega}}{\alpha} Y_0 + \frac{\omega\theta^{(1)} - \bar{\omega}\theta^{(5)}}{\alpha} Y_1 + \frac{\omega(\theta^{(1)})^2 - \bar{\omega}(\theta^{(5)})^2}{\alpha} Y_2 \right) \quad . \tag{8}$$

III. The remaining pairs are $(i,j) = (1,4),(5,2),(3,6)$. In view of our Remark 3, for all these pairs, $L_{ij}(\underline{X})/(\omega - \bar{\omega})$ has coefficients in L. Moreover, the conjugates of $L_{14}(\underline{X})/(\omega - \bar{\omega})$ over L are exactly $L_{52}(\underline{X})/(\omega - \bar{\omega})$ and $L_{36}(\underline{X})/(\omega - \bar{\omega})$. This means that the product of the three factors in this group is equal to

$$(\omega - \bar{\omega})^3 \cdot N_{L/Q} \left(\frac{\theta^{(1)} - \theta^{(4)}}{\omega - \bar{\omega}} X_1 + \frac{(\theta^{(1)})^2 - (\theta^{(4)})^2}{\omega - \bar{\omega}} X_2 + Y_0 + \frac{\omega\theta^{(1)} - \bar{\omega}\theta^{(4)}}{\omega - \bar{\omega}} Y_1 + \frac{\omega(\theta^{(1)})^2 - \bar{\omega}(\theta^{(4)})^2}{\omega - \bar{\omega}} Y_2 \right).$$

The form $L_{14}(\underline{X})/(\omega-\bar{\omega})$ does not always have integer coefficients in L. But the index form $I(\underline{X})$ has integer coefficients and therefore there must be a $\beta \in \mathbb{Z}_L$ of norm $|N_{L/Q}(\beta)| = |N_{K/Q}(\alpha)|$ (to find such an element, test again the nonassociated integers in L of norm $\pm|N_{K/Q}(\alpha)|$ obtained by the method of [8]) such that $\beta L_{14}(\underline{X})/(\omega-\bar{\omega})$ admits integer coefficients in L. Hence, the product of the three factors in this group is equal to

$$\frac{(\omega-\bar{\omega})^3}{N_{L/Q}(\beta)} \cdot F_3(\underline{X}), \tag{9}$$

with

$$\begin{aligned} F_3(\underline{X}) = N_{L/Q}\Bigg(&\frac{\beta(\theta^{(1)}-\theta^{(4)})}{\omega-\bar{\omega}}X_1 + \frac{\beta((\theta^{(1)})^2-(\theta^{(4)})^2)}{\omega-\bar{\omega}}X_2 + \beta Y_0 \\ &+ \frac{\beta(\omega\theta^{(1)}-\bar{\omega}\theta^{(4)})}{\omega-\bar{\omega}}Y_1 + \frac{\beta(\omega(\theta^{(1)})^2-\bar{\omega}(\theta^{(4)})^2)}{\omega-\bar{\omega}}Y_2\Bigg). \end{aligned} \tag{10}$$

In view of (1), (2) and $|N_{L/Q}(\beta)| = |N_{K/Q}(\alpha)|$ we conclude that the index form equation (3) is equivalent to the system of equations

$$F_1(x_1,x_2,y_1,y_2) = \pm 1, \tag{11}$$

$$F_2(x_1,x_2,y_0,y_1,y_2) = \pm 1 \quad \text{in} \quad x_1,x_2,y_0,y_1,y_2 \in \mathbb{Z}, \tag{12}$$

$$F_3(x_1,x_2,y_0,y_1,y_2) = \pm 1, \tag{13}$$

with the above $F_1, F_2, F_3 \in \mathbb{Z}[X_1, X_2, Y_0, Y_1, Y_2]$.

4. A relative Thue equation over the quadratic subfield

We consider now the first equation (11) of the above system. In view of (6) it can be rewritten as

$$N_{K/Q}((x_1+\omega y_1)+(\theta^{(1)}+\theta^{(2)})(x_2+\omega y_2)) = \pm 1 \quad \text{in} \quad x_1,x_2,y_0,y_1,y_2 \in \mathbb{Z}.$$

The element $\varrho = \theta^{(1)}+\theta^{(2)} \in K$ is of degree 6, $x = x_1+\omega y_1$ and $y = x_2+\omega y_2$ are in $\mathbb{Z}_M$. Then the equation is equivalent to

$$N_{K/Q}(x+\varrho y) = \pm 1 \quad \text{in} \quad x,y \in \mathbb{Z}_M. \tag{14}$$

Denote by μ the fundamental unit of M with $\mu > 1$. Then (14) implies

$$N_{K/M}(x+\varrho y) = \pm\mu^s$$

with some $s \in \mathbb{Z}$. Taking $s = 3q+r$, with $q, r \in \mathbb{Z}, 0 \le r < 3$ and $x' = x\mu^{-q}, y' = y\mu^{-q}$, we get

$$N_{K/M}(x'+\varrho y') = \pm\mu^r \quad \text{in} \quad x',y' \in \mathbb{Z}_M. \tag{15}$$

For a fixed r this equation is a *relative Thue equation* over M. It is well known that such an equation has only finitely many solutions. This means that equation (14) can be reduced to three ($r = 0, 1, 2$ in (15)) relative Thue equations.

We show that by analyzing equation (14) in a proper way we can find all $x = x_1+\omega y_1, y = x_2+\omega y_2 \in \mathbb{Z}_M$, such that all solutions of (14) are of the form $\pm\mu^s x, \pm\mu^s y$ with some $s \in \mathbb{Z}$. The cases $r = 0, 1, 2$ can be dealt with simultaneously; only one solving procedure is needed.

We remark that recently de Weger [31] also solved a relative Thue equation over a quadratic field by somewhat different methods.

4.1. Fundamental units. Denote by τ a unit in the cubic subfield L such that $\{\tau, \tau^{(3)}\}$ forms a fundamental system of units in L. (Such a τ always exists, cf. [20].) The system $\{\mu, \tau, \tau^{(3)}\}$ can always be extended to a fundamental system of units in K ([20]).

Equation (14) can always be reduced to a unit equation in two variables over K (see [7]). In our case, since we deal with relative conjugates over M, the factor corresponding to μ cancels, and the units in this unit equation have 4 factors with unknown exponents. There is a well–known constructive method to analyze such unit equations (cf. [11]).

However (see [20]), in about 95% of the totally real cyclic sextic fields there exists a unit ξ such that $\{\mu, \tau, \tau^{(3)}, \xi, \xi^{(5)}\}$ is a fundamental system of units in K. (Exceptions occur only for very large discriminants.) Such a system of fundamental units makes the formulas very much simpler (cf. also Remark 4 in §4.4), and ideas of this type may be fruitful in some other applications, too. For this reason, we assume in the following that $\{\mu, \tau, \tau^{(3)}, \xi, \xi^{(5)}\}$ is a system of fundamental units in K, and we develop our method in detail under this condition.

Lemma 1. *Let μ, τ, ξ be as above. If $\{\mu, \tau, \tau^{(3)}, \xi, \xi^{(5)}\}$ is a fundamental system of units in K, then the same holds for $\{\mu, \tau, \tau^{(3)}, \xi, \xi^{(3)}\}$.*

Proof. We have

$$N_{K/M}(\xi) = \xi\xi^{(2)}\xi^{(3)} = \pm\mu^t \tag{16}$$

with a $t \in \mathbb{Z}$. On the other hand,

$$N_{K/L}(\xi) = \xi\xi^{(4)} = \pm\tau^a(\tau^{(3)})^b$$

with suitable $a, b, \in \mathbb{Z}$. This implies

$$\xi^{(2)}\xi^{(5)} = \pm(\tau^{(2)})^a\tau^b = \pm\left(\frac{\pm 1}{\tau(\tau^{(3)})}\right)^a \tau^b = \pm\tau^{b-a}(\tau^{(3)})^{-a},$$

whence

$$\xi^{(5)} = \pm(\xi^{(2)})^{-1}\tau^{b-a}(\tau^{(3)})^{-a} \quad .$$

Combining this expression with (16), we obtain

$$\xi^{(5)} = \pm\xi\xi^{(3)}\tau^{b-a}(\tau^{(3)})^{-a}\mu^{-t},$$

which implies the assertion. □

4.2. Application of Baker's method. Let $x, y \in \mathbb{Z}_M$ be an arbitrary but fixed solution of (14). Let $\beta = x + \varrho y$. Obviously,

$$\beta = \pm\mu^l\tau^a(\tau^{(3)})^b\xi^c(\xi^{(3)})^d, \tag{17}$$

with $l, a, b, c, d \in \mathbb{Z}$.

We use the identity

$$\left(\varrho^{(1)} - \varrho^{(2)}\right)\beta^{(3)} + \left(\varrho^{(2)} - \varrho^{(3)}\right)\beta^{(1)} + \left(\varrho^{(3)} - \varrho^{(1)}\right)\beta^{(2)} = 0$$

to get

$$\frac{\left(\varrho^{(1)}-\varrho^{(3)}\right)\beta^{(2)}}{\left(\varrho^{(3)}-\varrho^{(2)}\right)\beta^{(1)}}+1=\frac{\left(\varrho^{(1)}-\varrho^{(2)}\right)\beta^{(3)}}{\left(\varrho^{(3)}-\varrho^{(2)}\right)\beta^{(1)}}. \tag{18}$$

From

$$\tau\tau^{(2)}\tau^{(3)}=\pm 1 \quad \text{and} \quad \xi\xi^{(2)}\xi^{(3)}=\pm\mu^t$$

(cf. the proof of Lemma 1) and (17) we conclude

$$\left|\frac{\beta^{(2)}}{\beta^{(1)}}\right|=\left|\tau^{b-2a}(\tau^{(3)})^{-b-a}\xi^{d-2c}(\xi^{(3)})^{-d-c}\mu^{tc}\right| \tag{19}$$

$$=\left|\varepsilon_1^a\varepsilon_2^b\varepsilon_3^c\varepsilon_4^d\right|, \tag{20}$$

with

$$\varepsilon_1=\frac{1}{\tau^2\tau^{(3)}},\ \ \varepsilon_2=\frac{\tau}{\tau^{(3)}},\ \ \varepsilon_3=\frac{\mu^t}{\xi^2\xi^{(3)}},\ \ \varepsilon_4=\frac{\xi}{\xi^{(3)}}.$$

It follows from (19) that $\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4$ are multiplicatively independent. Similarly, we obtain

$$\left|\frac{\beta^{(3)}}{\beta^{(1)}}\right|=\left|\tau^{-a-b}(\tau^{(3)})^{a-2b}\xi^{-c-d}(\xi^{(3)})^{c-2d}\mu^{kd}\right|$$

$$=|\eta_1^a\eta_2^b\eta_3^c\eta_4^d|, \tag{21}$$

with multiplicatively independent

$$\eta_1=\frac{\tau^{(3)}}{\tau},\ \ \eta_2=\frac{1}{\tau(\tau^{(3)})^2},\ \ \eta_3=\frac{\xi^{(3)}}{\xi},\ \ \eta_4=\frac{\mu^t}{\xi(\xi^{(3)})^2}.$$

Set $\gamma=\beta^{(3)}/\beta$. Denote by $\gamma^{(I)}$ the conjugate of γ with

$$|\log(\gamma^{(I)})|=\max_{1\le i\le 6}|\log(\gamma^{(i)})|. \tag{22}$$

We have

$$\log|\gamma^{(k)}|=a\log|\eta_1^{(k)}|+b\log|\eta_2^{(k)}|+c\log|\eta_3^{(k)}|+d\log|\eta_4^{(k)}| \quad (1\le k\le 6).$$

Consider this system as a system of linear equations in a,b,c,d. Since the η_j are multiplicatively independent, taking any 4 of the indices $1\le k\le 6$ in the above system of equations, the matrix $\mathcal{M}$ of the system of equations is nonsingular. Choose the 4 indices such that the row norm of $\mathcal{M}^{-1}$ become as small as possible. Denote this value by c_1. Then (22) implies

$$H=\max(|a|,|b|,|c|,|d|)\le c_1|\log|\gamma^{(I)}||,$$

whence

$$|\log|\gamma^{(I)}||\ge\frac{H}{c_1}.$$

This, in view of

$$\sum_{k=1}^{6} \log|\gamma^{(k)}| = 0 \tag{23}$$

(holding because γ is a unit in K), implies in turn that there exists a conjugate $\gamma^{(i)}$ of γ with

$$\log|\gamma^{(i)}| \le \frac{-H}{5c_1}. \tag{24}$$

Take now the conjugate $(\cdot)^{(i)}$ of all terms in the equation (18). (Note that in the course of the computation one has to consider all possible values for i.) From (24) we conclude

$$\left|\left(\varepsilon_1^{(i)}\right)^a \left(\varepsilon_2^{(i)}\right)^b \left(\varepsilon_3^{(i)}\right)^c \left(\varepsilon_4^{(i)}\right)^d \varepsilon_5^{(i)} - 1\right| \le c_2 \exp\left(-\frac{H}{5c_1}\right), \tag{25}$$

with

$$\varepsilon_5 = \frac{\varrho^{(3)} - \varrho^{(1)}}{\varrho^{(3)} - \varrho^{(2)}} \quad \text{and} \quad c_2 = \left|\left(\frac{\varrho^{(1)} - \varrho^{(2)}}{\varrho^{(3)} - \varrho^{(2)}}\right)^{(i)}\right|.$$

In view of the inequality

$$|\log t| \le 2|t-1|, \quad \text{which holds for any real} \quad t \quad \text{with} \quad |t-1| < 0.795, \tag{26}$$

(25) implies

$$\begin{aligned} \Lambda &= \left|a \log\left|\varepsilon_1^{(i)}\right| + b \log\left|\varepsilon_2^{(i)}\right| + c \log\left|\varepsilon_3^{(i)}\right| + d \log\left|\varepsilon_4^{(i)}\right| + \log\left|\varepsilon_5^{(i)}\right|\right| \\ &\le 2c_2 \exp\left(-\frac{H}{5c_1}\right), \end{aligned} \tag{27}$$

where it is assumed that

$$H > -5c_1 \log\left(\frac{0.795}{c_2}\right) = c_3. \tag{28}$$

We now wish to give a lower bound for the linear form Λ in (27) in terms of H by using Baker's method. We observe that ε_5 is multiplicatively dependent on $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$ (which are independent). We have

$$\log|\varepsilon_5| = \frac{a_0}{m}\log|\varepsilon_1| + \frac{b_0}{m}\log|\varepsilon_2| + \frac{c_0}{m}\log|\varepsilon_3| + \frac{d_0}{m}\log|\varepsilon_4|,$$

with suitable integers a_0, b_0, c_0, d_0, m. (In our examples we always had $m = 3$.) Set

$$\bar{a} = ma + a_0,\ \bar{b} = mb + b_0,\ \bar{c} = mc + c_0,\ \bar{d} = md + d_0 \tag{29}$$

and

$$H_0 = \max(|a_0|, |b_0|, |c_0|, |d_0|), \quad \bar{H} = \max(|\bar{a}|, |\bar{b}|, |\bar{c}|, |\bar{d}|).$$

Then $\bar{H} \le mH + H_0$, whence

$$H \ge \frac{\bar{H} - H_0}{m}, \tag{30}$$

and inequality (27) becomes

$$\begin{aligned} \Lambda &= \left|\bar{a}\log\left|\varepsilon_1^{(i)}\right| + \bar{b}\log\left|\varepsilon_2^{(i)}\right| + \bar{c}\log\left|\varepsilon_3^{(i)}\right| + \bar{d}\log\left|\varepsilon_4^{(i)}\right|\right| \\ &\le AB^{-\bar{H}}, \end{aligned} \tag{31}$$

with

$$A = 2mc_2 \exp\left(\frac{H_0}{5mc_1}\right) \quad \text{and} \quad B = \exp\left(\frac{1}{5mc_1}\right).$$

We used the inequality of Corollary 2 of [3] (see also [4]) to obtain a lower bound of type

$$\exp(-W(\log \bar{H} + C)) \tag{32}$$

for Λ. Combining this lower bound with (31), we obtain an upper bound $\bar{H}_B$ for $\bar{H}$. In our examples the upper bound was between 10^{44} and 10^{46}.

4.3. Reduction of the bound. The next step is to reduce the bound $\bar{H}_B$ for $\bar{H}$.

For simplicity set $\gamma_j = \left|\varepsilon_j^{(i)}\right|$ for $1 \le j \le 4$. Consider the lattice Γ spanned by the columns of the matrix

$$\Gamma = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ [C\gamma_1] & [C\gamma_2] & [C\gamma_3] & [C\gamma_4] \end{pmatrix}, \tag{33}$$

where $[\cdot]$ denotes the nearest integer and C is a constant to be determined later.

Reduce the basis (33) of the lattice Γ by the LLL-reduction algorithm (cf. [19]). Denote by $\underline{b}_1$ the first vector in the reduced basis. The assertions (i) and (ii) of the following lemma are special cases of Lemma 3.7 of [30] and of Proposition 3.1 of [28], respectively.

Lemma 2. (i) *If*

$$2^{-3/2}|\underline{b}_1| > \sqrt{34}\bar{H}_B \tag{34}$$

and $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}$ *is a solution of* (31) *with* $\bar{H} = \max(|\bar{a}|, |\bar{b}|, |\bar{c}|, |\bar{d}|) \le \bar{H}_B$, *then*

$$\bar{H} \le \frac{\log C + \log A - \log \bar{H}_B}{\log B}. \tag{35}$$

(ii) *If* $\bar{H}_1$ *is a positive constant,*

$$|\underline{b}_1| > \sqrt{152}\bar{H}_1 \tag{36}$$

and $\bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}$ *is a solution of* (31) *with* $\bar{H} = \max(|\bar{a}|, |\bar{b}|, |\bar{c}|, |\bar{d}|) \le \bar{H}_1$, *then*

$$\bar{H} \le \frac{\log C + \log A - \log\left(\sqrt{0.125|\underline{b_1}|^2 - 3\bar{H}_1^2} - 4\bar{H}_1\right)}{\log B}. \tag{37}$$

In the first reduction step it is advisable to use the simpler statement Lemma 2 (i). Set $C = \bar{H}_B^4$. Then C is large enough to expect that (34) is satisfied. By (35) we get a reduced bound $\bar{H}_1$ for $\bar{H}$, which was in our examples between 5000 and 9500.

In the second and further reduction steps, usually Lemma 2 (ii) is applied, in order to get more exact estimates. We set $\bar{H}_1$ to be the bound obtained in the preceding reduction step. If we take $C = \bar{H}_1^4$, inequality (36) usually holds, but in order to get a better reduced bound, we try to diminish the value of C as much as possible. After the first reduction step, the bound $\bar{H}_1$ is not so extremely large like in the first step, hence the LLL–reduction of the lattice Γ requires only a negligible computing time, and therefore it is worth making some trials to obtain a better bound. For this purpose, we find the smallest h such that with $C = 10^h$, (36) is satisfied.

In our examples we reduced the bound $\bar{H}_B$ in 4 steps and finally obtained a bound between 400–1100. A typical sequence of the bounds is, e.g., $10^{45}, 5214, 662, 530, 524$. Note that in our examples we had $0.69 \le A \le 160, 5.4 \le B \le 11.4$.

We have to use Baker's method and perform the reduction for all possible values $1 \le i \le 6$. Denote by $\bar{H}_R$ the maximum of the reduced bounds obtained for $1 \le i \le 6$.

We end this subsection with calculating the bound for H implied by the reduced bound for $\bar{H}$ (cf. (29)):

$$H = \max(|a|, |b|, |c|, |d|) \le H_R = \frac{\bar{H}_R + H_0}{m}.$$

This bound usually also satisfies $H_R > c_3$ (cf. (28)). In our examples, H_R was between 171 and 359.

4.4. Testing over the remaining set. Consider again equation (18). In view of our notation it can be rewritten as

$$\pm\varepsilon_1^a\varepsilon_2^b\varepsilon_3^c\varepsilon_4^d\varepsilon_5 + 1 = \pm\eta_1^a\eta_2^b\eta_3^c\eta_4^d\eta_5, \tag{38}$$

with

$$\eta_5 = \frac{\varrho^{(1)} - \varrho^{(2)}}{\varrho^{(3)} - \varrho^{(2)}}.$$

Remark 4. The main advantage of our choice of fundamental units (cf. §4.1) is that at this step we have an equation (38) with the same exponents on both sides.

The bound H_R is too large to test directly all possible values of a, b, c, d with absolute values below H_R. For this reason, we apply a *sieve method*. We remark that a similar test is used in [29]. The idea is that we embed $\mathcal{O}$ into $\mathbb{Z}_p$ for a prime p. To perform the embedding, one merely has to embed θ and ω, which induces the embedding for any element in $\mathcal{O}$. First we represent ω in the form

$$\omega = \frac{\sum_{i=0}^{5} g_i\theta^i}{g_d}$$

with integers $g_i \ \ (0 \le i \le 5), \ \ g_d$. Then, if the prime does not divide g_d, we can easily calculate the image of ω from the image of ϑ.

We determine primes $p_1, p_2, \dots$ such that

- The minimal polynomial of θ over $\mathbb{Q}$ splits into linear factors $\bmod p_i$,
- p_i does not divide the discriminant D of $\mathcal{O}$, and
- p_i does not divide g_d.

Then we can compute integers e_{ji}, f_{ji} with the property

$$\varepsilon_j \equiv e_{ji} \pmod{\wp_i} \quad (1 \le j \le 5),$$

$$\eta_j \equiv f_{ji} \pmod{\wp_i} \quad (1 \le j \le 5),$$

with a prime ideal $\wp_i$ lying above p_i. Then equation (38) becomes

$$\pm e_{1i}^a e_{2i}^b e_{3i}^c e_{4i}^d e_{5i} + 1 \equiv \pm f_{1i}^a f_{2i}^b f_{3i}^c f_{4i}^d f_{5i} \pmod{p_i}. \tag{39}$$

We test all possible exponents $(a, b, c, d) \mod (p_1 - 1)$. If a tuple (a_0, b_0, c_0, d_0) is a solution of (39) $\bmod p_1$, then we generate all possible a, b, c, d such that

$$a \equiv a_0, \ \ b \equiv b_0, \ \ c \equiv c_0, \ \ d \equiv d_0 \pmod{(p_1 - 1)},$$

and

$$\max(|a|, |b|, |c|, |d|) < H_R.$$

For all these possible tuples (a, b, c, d) we test (39) modulo p_2 and the surviving tuples modulo p_3 etc. After about the fourth test the set of possible solutions does not reduce any more and the tuples in this set are usually solutions of (38) as well.

The first sieving step requires a considerable CPU time (about 3 hours) and produces a huge amount of possible solutions. This is the reason why it is worth storing the possible tuples only after the second sieving step, which is already much faster. The third and further steps require only a negligible amount of CPU time. The primes we used in our examples were all less than 350.

For all solutions (a, b, c, d) of (38) we calculate $\tilde{\beta} = \tau^a (\tau^{(3)})^b \xi^c (\xi^{(3)})^d$ (cf. (17)). We can decide, whether there exist $x, y \in \mathbb{Z}_M$ such that

$$\tilde{\beta} = x + \varrho y.$$

If so, then all solutions of (14) corresponding to (a, b, c, d) are of the form

$$x_1 + \omega y_1 = \pm \mu^n x, \quad x_2 + \omega y_2 = \pm \mu^n y, \tag{40}$$

with $x_1, y_1, x_2, y_2 \in \mathbb{Z}$ depending already only on the unknown $n \in \mathbb{Z}$.

5. Inhomogeneous equations in two dominating variables

By (40) we express x_1, y_1, x_2, y_2 to get

$$\begin{aligned} x_1 &= \pm \frac{\mu^n x \bar{\omega} - (\bar{\mu})^n \bar{x} \omega}{\bar{\omega} - \omega}, \\ y_1 &= \pm \frac{\mu^n x - (\bar{\mu})^n \bar{x}}{\omega - \bar{\omega}}, \\ x_2 &= \pm \frac{\mu^n y \bar{\omega} - (\bar{\mu})^n \bar{y} \omega}{\bar{\omega} - \omega}, \\ y_2 &= \pm \frac{\mu^n y - (\bar{\mu})^n \bar{y}}{\omega - \bar{\omega}}. \end{aligned} \tag{41}$$

In the following we have to determine n (which fixes also the values of x_1, y_1, x_2, y_2 up to sign) and y_0 of (3). For this purpose we use equation (13).

Substituting the values of (41) into (13), we obtain an equation of the form

$$\prod_{k=1}^{3} (A_k\mu^n + B_k(\bar{\mu})^n + C_k y_0) = \pm 1, \tag{42}$$

with explicitly known algebraic coefficients $A_k, B_k, C_k \in K \quad (1 \le k \le 3)$.

We consider this equation in detail only for $n \ge 0$. The opposite case of $n < 0$ is similar by interchanging the roles of A_k and B_k.

If $n \ge 0$, then in (42) the *dominating variables* are μ^n and y_0, and the value of $(\bar{\mu})^n$ is "small" compared to the dominating variables. (We recall that we defined μ with $\mu > 1$.) The structure of this equation is very similar to that of an *inhomogeneous Thue equation* considered in [9, 27]. In many respects the situation is much simpler, because, except for small $n > 0$ (which values can be tested separately), the value of $|(\bar{\mu})^n|$ can be bounded by a quite small constant.

5.1. Baker's method. The factors of F_3 in (13) have algebraic integer coefficients and the right side of (13) is ± 1, hence

$$\nu^{(k)} = A_k\mu^n + B_k(\bar{\mu})^n + C_k y_0 = \pm(\delta_1^{(k)})^a(\delta_2^{(k)})^b \quad (1 \le k \le 3) \tag{43}$$

with $a, b \in \mathbb{Z}$, where for simplicity we take $\delta_1 = \tau, \delta_2 = \tau^{(3)}$.

We fix a small value μ_0 and determine the smallest $n_0 \quad (> 0)$ such that for $n > n_0$

$$\mu^n > \frac{1}{\mu_0}. \tag{44}$$

In our examples we took $\mu_0 = 10^{-4}$. In the course of our considerations below we shall require to increase n_0 if necessary, so that for $n > n_0$ the value of μ^n is larger than certain constants. We remark that by taking $\mu_0 = 10^{-4}$ the value of n_0 was essentially determined by (44). The values of n with $0 \le n \le n_0$ must be considered separately. Using $\mu_0 = 10^{-4}$ requires testing about 10 values n. For all fixed n, equation (42) is a cubic polynomial equation in y_0.

Denote by i the index with

$$|\nu^{(i)}| = \min_{1 \le k \le 3} |\nu^{(k)}|. \tag{45}$$

Obviously,

$$|\nu^{(i)}| \le 1. \tag{46}$$

(In the course of the computation one has to consider all possible values for i.) We have

$$|y_0| \le |\nu^{(i)}| + |A_i|\mu^n + |B_i|\mu_0 \le c_1|A_i|\mu^n \tag{47}$$

with

$$c_1 = 1.1|A_i|,$$

assuming that

$$\mu^n \geq \frac{10}{|A_i|}(1+|B_i|\mu_0). \tag{48}$$

For $k \neq i$, by (46) we obtain

$$\begin{aligned}|C_i\nu^{(k)}| &\geq |C_i\nu^{(k)} - C_k\nu^{(i)}| - |C_k\nu^{(i)}| \\ &\geq |C_iA_k - C_kA_i|\mu^n - |C_iB_k - C_kB_i|\mu_0 - |C_k| \\ &\geq 0.9|C_iA_k - C_kA_i|\mu^n\end{aligned}$$

if

$$\mu^n > \frac{|C_iB_k - C_kB_i|\mu_0 + |C_k|}{0.1|C_iA_k - C_kA_i|}. \tag{49}$$

The above inequality implies

$$|\nu^{(k)}| \geq c_2(k)\mu^n \quad (k \neq i) \tag{50}$$

with

$$c_2(k) = \frac{0.9|C_iA_k - C_kA_i|}{|C_i|} \quad (k \neq i).$$

It follows from (50) that

$$|\nu^{(k)}| > 1 \quad (k \neq i) \tag{51}$$

if we assume that

$$\mu^n > \frac{1}{c_2(k)} \quad (k \neq i). \tag{52}$$

Consider now the equations

$$\log|\nu^{(k)}| = a\log|\delta_1^{(k)}| + b\log|\delta_2^{(k)}| \quad \text{for} \quad 1 \leq k \leq 3, k \neq i,$$

as a system of linear equations in a, b. Denote by c_3 the row norm of the inverse of the matrix of this system. Then in view of (47) and (51) we conclude

$$H = \max(|a|,|b|) \leq c_3 \max_{k\neq i} \log|\nu^{(k)}| \leq c_3(\log c_4 + \log\mu^n) \tag{53}$$

with

$$c_4 = \max_{k\neq i}(|A_k| + c_1|C_k| + 0.01),$$

assuming that

$$\mu^n > 100\mu_0 \max_{k\neq i}|B_k|. \tag{54}$$

Set now $\{j,k\}=\{1,2,3\}\setminus\{i\}$. Then equation (42) can be rewritten as

$$\nu^{(i)}\nu^{(j)}\nu^{(k)}=\pm 1,$$

whence by (50) we get

$$|\nu^{(i)}|=\frac{1}{|\nu^{(j)}\nu^{(k)}|}\le\frac{1}{c_2(j)c_2(k)}\mu^{-2n}. \tag{55}$$

In this inhomogeneous case, Siegel's identity becomes

$$(C_iA_j-C_jA_i)\nu^{(k)}+(C_jA_k-C_kA_j)\nu^{(i)}+(C_kA_i-C_iA_k)\nu^{(j)}=(\bar{\mu})^n\chi,$$

where

$$\chi=B_k(C_iA_j-C_jA_i)+B_i(C_jA_k-C_kA_j)+B_j(C_kA_i-C_iA_k).$$

Let $c_5=|\chi|$. By (55), (50) and (53) this identity implies

(56)

$$\begin{aligned}\left|\frac{(C_iA_j-C_jA_i)\nu^{(k)}}{(C_iA_k-C_kA_i)\nu^{(j)}}-1\right|&\le\left|\frac{C_kA_j-C_jA_k}{C_iA_k-C_kA_i}\right|\left|\frac{\nu^{(i)}}{\nu^{(j)}}\right|+\frac{c_5|\bar{\mu}|^n}{|(C_iA_k-C_kA_i)\nu^{(j)}|}\\&\le c_6\mu^{-3n}+c_7\mu^{-2n}\le(c_6\mu_0+c_7)\exp\left(-2\log\mu^n\right)\\&\le\exp\left(c_8-\frac{2H}{c_3}\right),\end{aligned}$$

with

$$c_6=\left|\frac{C_kA_j-C_jA_k}{C_iA_k-C_kA_i}\right|\frac{1}{c_2(j)^2c_2(k)},$$

$$c_7=\frac{c_5}{|C_iA_k-C_kA_i|c_2(j)}\quad\text{and}\quad c_8=\log(c_6\mu_0+c_7)+2\log c_4.$$

Using again inequality (26), we see that our estimate (56) implies

$$\Lambda=\left|\log\left|\frac{C_iA_j-C_jA_i}{C_iA_k-C_kA_i}\right|+a\log\left|\frac{\delta_1^{(k)}}{\delta_1^{(j)}}\right|+b\log\left|\frac{\delta_2^{(k)}}{\delta_2^{(j)}}\right|\right|\le 2\exp\left(c_8-\frac{2H}{c_3}\right), \tag{57}$$

assuming that

$$\mu^n>\sqrt{\frac{c_6\mu_0+c_7}{0.795}}. \tag{58}$$

Now we have to distinguish between two cases, according as

$$\left|\frac{C_iA_j-C_jA_i}{C_iA_k-C_kA_i}\right| \tag{59}$$

is multiplicatively independent of

$$\left|\frac{\delta_1^{(k)}}{\delta_1^{(j)}}\right|\quad\text{and}\quad\left|\frac{\delta_2^{(k)}}{\delta_2^{(j)}}\right| \tag{60}$$

or not. In our computations both cases have frequently occurred.

5.1.1. The case of independence. In case the expression (59) is multiplicatively independent of the terms in (60), we can use Baker's method (Corollary 2 of [3]) directly to the linear form Λ in (57) to obtain a lower bound of the form $\exp(-W(\log H + C))$ for Λ. Comparing this lower bound with the upper bound in (57) for Λ, we conclude with a bound H_B for H. In our examples H_B was between 10^{30} and 10^{32}.

5.1.2. The case of dependence. In this case we proceed similarly as in §4.2. There exist $a_0, b_0, m \in \mathbb{Z}$ such that

$$\log\left|\frac{C_iA_j - C_jA_i}{C_iA_k - C_kA_i}\right| = \frac{a_0}{m}\log\left|\frac{\delta_1^{(k)}}{\delta_1^{(j)}}\right| + \frac{b_0}{m}\log\left|\frac{\delta_2^{(k)}}{\delta_2^{(j)}}\right|$$

(in our examples we always had $m = 3$). Set

$$\bar{a} = ma + a_0,\ \bar{b} = mb + b_0 \tag{61}$$

and

$$H_0 = \max(|a_0|, |b_0|), \quad \bar{H} = \max(|\bar{a}|, |\bar{b}|);$$

then $\bar{H} \le mH + H_0$, whence

$$H \ge \frac{\bar{H} - H_0}{m}. \tag{62}$$

With this notation, (57) becomes

$$\Lambda = \left|\bar{a}\log\left|\frac{\delta_1^{(k)}}{\delta_1^{(j)}}\right| + \bar{b}\log\left|\frac{\delta_2^{(k)}}{\delta_2^{(j)}}\right|\right| \le c_9\exp\left(-\frac{2\bar{H}}{mc_3}\right), \tag{63}$$

with

$$c_9 = 2m\exp\left(c_8 + \frac{2H_0}{mc_3}\right).$$

We apply now Corollary 2 of [3] in the two variables case. Comparing the lower bound of type $\exp(-W(\log \bar{H} + C))$ for Λ with (63), we conclude $\bar{H} \le \bar{H}_B$. In our examples $\bar{H}_B$ was between 10^{21} and 10^{23}.

5.2. Reduction of Baker's bound. We use different methods for the reduction procedure in the cases of independece and dependence. Note, that these reduction algorithms can also be developed by using lattices and ideas similar to those used in §4.3 (cf. [30]). We follow here a more traditional way, using the continued fraction algorithm.

5.2.1. Reduction in the case of independence. Inequality (57) implies

$$|a\phi + b - \psi| \le AB^{-H}, \tag{64}$$

with

$$\phi = \frac{\log\left|\frac{\delta_1^{(k)}}{\delta_1^{(j)}}\right|}{\log\left|\frac{\delta_2^{(k)}}{\delta_2^{(j)}}\right|}, \qquad \psi = \frac{-\log\left|\frac{C_iA_j - C_jA_i}{C_iA_k - C_kA_i}\right|}{\log\left|\frac{\delta_2^{(k)}}{\delta_2^{(j)}}\right|}$$

and

$$A = \frac{2\exp c_8}{\left|\log\left|\frac{\delta_2^{(k)}}{\delta_2^{(j)}}\right|\right|}, \qquad B = \exp\left(\frac{2}{c_3}\right).$$

We apply now the Baker–Davenport Lemma [1] in a slightly modified form (cf. Lemma 2 of [9]) to inequality (64):

Lemma 3. *Let C, D be positive constants. If there exists $q \in \mathbb{Z}$ such that*

$$1 \le q \le CD, \tag{65}$$

$$\|q\phi\| < \frac{2}{CD}, \tag{66}$$

$$\|q\psi\| \ge \frac{3}{D}, \tag{67}$$

then inequality (64) *has no solutions $a, b, \in \mathbb{Z}$ with*

$$\frac{\log\left(CD^2A\right)}{\log B} \le H \le C, \tag{68}$$

where $H = \max(|a|, |b|)$ and $\|\cdot\|$ denotes the distance from the nearest integer.

We use this lemma with $C = H_B$ and $D = 100$ or 1000. Applying the continued fraction algorithm to ϕ, one can compute a q satisfying (65) and (66). The same q usually also satisfies (67), because here we are in the case of independence. In the next step, C is the bound obtained in the preceding reduction step. Applying the lemma about 4 times (until the bound does not diminish any further), we get a reduced bound for H, which was below 35 in our examples. Note that it is usually possible to reduce this bound further by testing (64) for the pairs below the reduced bound.

One has to apply Baker's method and the reduction algorithm for all possible values of i $(1 \le i \le 3)$. Let H_R be the maximum of the reduced bounds obtained for $i = 1, 2, 3$.

5.2.2. Reduction in the case of dependence. In this case, from (63) we have

$$|\bar{a}\phi + \bar{b}\psi| \le AB^{-\bar{H}}, \tag{69}$$

with

$$\phi = \log\left|\frac{\delta_1^{(k)}}{\delta_1^{(j)}}\right|, \quad \psi = \log\left|\frac{\delta_2^{(k)}}{\delta_2^{(j)}}\right|, \quad A = c_9, \quad B = \exp\left(\frac{2}{mc_3}\right).$$

Our reduction method used in this case is again based on the continued fraction algorithm.

We assume that $|\phi| < |\psi|$; the opposite case $|\phi| > |\psi|$ can be considered similarly by interchanging the roles of $\bar{a}, \phi$ with $\bar{b}, \psi$, respectively. First we consider only the coprime solutions $((\bar{a}, \bar{b}) = 1)$ of (69); we shall show that from that case one can easily obtain all solutions of (69). The case $\bar{a} = 0$ being trivial, we may also assume $\bar{a} \ne 0$.

Denote by p_i/q_i the convergents in the continued fraction expansion of $\chi = -\phi/\psi$, and by a_i the corresponding partial quotients, satisfying $p_{i+1} = a_i p_i + p_{i-1}$, $q_{i+1} = a_i q_i + q_{i-1}$ for $i \ge 0$ (cf. [21]). We use the following lemma (see [5] for its basic idea):

Lemma 4. *Assume that for $\chi = -\phi/\psi$ we have $|\chi| < 1$. Let C be a positive constant, denote by m_0 the index with $q_{m_0-1} \le C < q_{m_0}$, let*

$$A_{\max} = \max_{i \le m_0} a_i,$$

and set

$$\varepsilon = \min(|\chi|, 1 - |\chi|).$$

Then, if $\bar{a}, \bar{b} \in \mathbb{Z}$ *is a solution of* (69) *with* $\bar{a} \neq 0$, $(\bar{a}, \bar{b}) = 1$, *and* $\bar{H} = \max(|\bar{a}|, |\bar{b}|) < C$, *then* $\bar{H}$ *satisfies one of the following inequalities:*

$$B^{\bar{H}} \leq \frac{A}{|\psi|\varepsilon}, \tag{70}$$

$$B^{\bar{H}} < \frac{2A\bar{H}}{|\psi|}, \tag{71}$$

$$B^{\bar{H}} < \frac{A(A_{\max} + 2)\bar{H}}{|\psi|}. \tag{72}$$

Proof. We have

$$\left| |\chi| - \left| \frac{\bar{b}}{\bar{a}} \right| \right| \leq \left| \chi - \frac{\bar{b}}{\bar{a}} \right| \leq \frac{1}{|\psi\bar{a}|} AB^{-\bar{H}} \leq \frac{1}{|\psi|} AB^{-\bar{H}}. \tag{73}$$

If the right side of the above inequality is $< \varepsilon$, then $\bar{H} = |\bar{a}|$; in the opposite case, (70) holds. Assume that $\bar{H}$ is large enough, and therefore $\bar{H} = |\bar{a}|$. Again, either (71) holds, or we have

$$\left| \chi - \frac{\bar{b}}{\bar{a}} \right| \leq \frac{1}{|\psi\bar{a}|} AB^{-\bar{H}} \leq \frac{1}{2\bar{a}^2}.$$

By $(\bar{a}, \bar{b}) = 1$ this implies that $\bar{b}/\bar{a}$ is a convergent p_i/q_i in the continued fraction expansion of χ. It follows by $(\bar{a}, \bar{b}) = 1$ that $\bar{b} = \pm p_i$ and $\bar{a} = \pm q_i$ with $i \leq m_0 - 1$, hence (cf. [26])

$$\frac{1}{(A_{\max} + 2)q_i^2} \leq \frac{1}{(a_{i+1} + 2)q_i^2} < \left| \chi - \frac{\bar{b}}{\bar{a}} \right| \leq \frac{1}{|\psi\bar{a}|} AB^{-\bar{H}},$$

which implies (72).

We use Lemma 4 in the first reduction step with $C = \bar{H}_B$. The inequalities of Lemma 4 imply that either $\bar{H}$ is small (cf. (70), (71)), or in view of (72), we can reduce the bound for $\bar{H}$. In the next step we proceed by taking the reduced bound for C and we repeat the reduction until it does not diminish the bound any further. Usually, the reduced bound is below 10 already after the first reduction, and 2–3 reduction steps are sufficient.

By the inequality

$$\left| \chi - \frac{\bar{b}}{\bar{a}} \right| \leq \frac{1}{|\psi|} AB^{-\bar{H}}$$

(cf. (73)) it is obvious that if a pair $(d\bar{a}, d\bar{b})$ with $(\bar{a}, \bar{b}) = 1$ is a solution of (69), then so also is the coprime pair $(\bar{a}, \bar{b})$. Lemma 4 makes it possible to determine the coprime solutions of (69). If, in addition, the corresponding pair $(d\bar{a}, d\bar{b})$ were also a solution of the inequality, then we would have

$$\left| \chi - \frac{\bar{b}}{\bar{a}} \right| = \left| \chi - \frac{d\bar{b}}{d\bar{a}} \right| \leq \frac{1}{|\psi|} AB^{-d\bar{H}}$$

with $\bar{H} = \max(|\bar{a}|, |\bar{b}|)$, which implies

$$d \leq \frac{1}{\bar{H}} \left(\log A - \log |\psi| - \log \left| \chi - \frac{\bar{b}}{\bar{a}} \right| \right).$$

This bound for d is usually very small (< 5). For all values of d satisfying this inequality, the pairs $(d\bar{a}, d\bar{b})$ should be tested together with $(\bar{a}, \bar{b})$. If some of them are solutions of (69), then the reduced bound should be increased if necessary to be at least as large as $\max(|d\bar{a}|, |d\bar{b}|)$. We remark that usually these calculations do not effect the reduced bound.

One has to use Baker's method and apply the reduction algorithm for all possible values of i $(1 \leq i \leq 3)$. Denote by $\bar{H}_R$ the maximum of the reduced bounds obtained for $i = 1, 2, 3$. From (61) we obtain

$$\max(|a|, |b|) \leq H_R = \frac{\bar{H}_R + H_0}{m}. \tag{74}$$

5.3. Testing small solutions. In the preceding sections we applied Baker's method and the reduction algorithm both in the case of independence (cf. §§5.1.1 and 5.2.1) and in the case of dependence (cf. §§5.1.2 and 5.2.2). Finally, we obtained a relatively small bound H_R for H.

Recall now the system of equations (43). In view of $\max(|a|, |b|) \leq H_R$, it implies

$$|A_k \mu^n + C_k y_0| < T_k \quad (1 \leq k \leq 3), \tag{75}$$

with

$$T_k = \left(\max \left(|\delta_1^{(k)}|, 1/|\delta_1^{(k)}| \right) \cdot \max \left(|\delta_2^{(k)}|, 1/|\delta_2^{(k)}| \right) \right)^{H_R} + |B_k| \mu_0 \quad (1 \leq k \leq 3).$$

This in turn implies a bound $n < N_0$ for n. Moreover, we also have to test the values of n with $n < n_0$ (cf. §5.1). This means that in the case $n > 0$ we have to test the values of n with $n < \max(N_0, n_0)$.

Usually, $N_0 \leq n_0$ and, as we remarked in §5.1, it is required to test about 10 values of n. For all fixed n, equation (42) is a cubic polynomial equation in y_0 with coefficients in $\mathbb{Z}$, and it is easy to decide if it has integer solutions in y_0.

6. Computational aspects

The computations were done partially on a HP 9000/433s workstation and partially on an IBM PC 486 AT compatible computer.

Baker's bound for the relative Thue equation (§4.2) was about $\bar{H}_B = 10^{45}$. In the first reduction step (§4.3) we used Lemma 2 (i) with $C = \bar{H}_B^4$, hence we had to use 200 (decimal)–digit numbers. The first reduction step took about three minutes on the HP workstation, the further steps were much faster.

Most CPU time was needed for testing the exponents a, b, c, d with $\max(|a|, |b|, |c|, |d|) < H_R$ (§4.4). The test of about 10^8 tuples in the first sieving step took about three hours on the PC, and reduced the number of tuples to about 10^6. The second step needed only a few minutes, and we obtained about 10^4 surviving tuples. The further steps took only a few seconds.

For all solutions of the relative Thue equation we had to solve an inhomogeneous equation in two dominating variables (§5). The complete resolution of such an

equation (calculating Baker's bound, the reduction procedure, and the test of small solutions) took about a minute on the PC. In the reduction procedure of these equations we used 100 (decimal)–digit numbers.

7. Numerical results

We computed all solutions of the index form equation (3) in the first five totally real cyclic sextic fields with smallest discriminants. The discriminants and the coefficients of the polynomial $f \in \mathbb{Z}_M$ were taken from [2]. The fundamental units of the fields K are from the tables of [20]. All other input data were computed by using the algorithms of the KANT package [22].

In all our examples, $\mathcal{O} = \mathbb{Z}_K$, and $D = D_K$ is the discriminant of K. Hence the results give all power integral bases of $\mathbb{Z}_K$.

It is clear from the tables of [25] that the fields with discriminants 300125, 371293, 453789 and 1075648 admit power integral bases. In case of the field with discriminant 820125 the generating element given in [25] has index > 1, but also in this case we found several solutions of the index form equation, that is, elements with index 1.

In our table we list the discriminant D_K of K, the quadratic field M, the element ω such that $\{1, \omega\}$ is a basis of M, and the polynomial $f \in \mathbb{Z}_M$. Finally we list the solutions $(x_1, x_2, y_0, y_1, y_2)$ of the index form equation (3) corresponding to the integer basis $\{1, \theta, \theta^2, \omega, \omega\theta, \omega\theta^2\}$ of K. If $(x_1, x_2, y_0, y_1, y_2)$ is a solution of (3), then so also is $(-x_1, -x_2, -y_0, -y_1, -y_2)$, but we list only one of them.

I. $D_K = 300125, M = \mathbb{Q}(\sqrt{5}), \omega = \frac{1+\sqrt{5}}{2}, f(t) = t^3 - (7 + 7\omega)t + (7 + 14\omega)$

x_1	x_2	y_0	y_1	y_2	x_1	x_2	y_0	y_1	y_2
–71	68	66	44	–42	–2	1	4	–2	0
–61	73	88	38	–45	–2	2	1	1	–1
–12	11	13	7	–7	–2	3	4	1	–2
–11	13	15	7	–8	–2	3	5	1	–2
–10	–5	4	6	3	1	–1	–5	0	1
–6	6	9	3	–4	1	–1	–4	0	1
–6	6	10	3	–4	1	–1	5	–2	0
–5	4	9	2	–3	1	1	–15	3	1
–5	5	5	3	–3	1	1	–5	1	0
–4	3	4	2	–2	1	2	–1	0	–1
–4	3	5	2	–2	2	–1	–5	0	1
–4	4	9	1	–3	2	–1	–4	0	1
–4	5	5	3	–3	3	–1	–13	2	2
–3	2	9	0	–2	8	5	–88	15	6
–3	2	10	0	–2	10	4	–66	17	6

II. $D_K = 371293, M = \mathbb{Q}(\sqrt{13}), \omega = \frac{1+\sqrt{13}}{2}, f(t) = t^3 - \omega t^2 + (-10+5\omega)t + (2-\omega)$

x_1	x_2	y_0	y_1	y_2	x_1	x_2	y_0	y_1	y_2
–499	284	121	–383	218	–11	7	5	–9	5
–456	241	136	–350	185	–9	4	3	–7	3
–99	56	24	–76	43	–9	5	2	–7	4
–82	43	25	–63	33	–8	4	2	–6	3
–46	26	11	–35	20	–8	4	3	–6	3
–43	43	8	–33	33	–7	4	2	–6	3
–42	22	12	–32	17	–6	4	1	–5	3
–31	17	9	–24	13	–6	4	2	–5	3
–22	13	5	–17	10	–4	1	1	–2	1
–17	9	4	–13	7	–4	4	1	–3	3
–17	9	5	–13	7	–1	1	1	–2	1
–17	13	4	–13	10	–1	2	1	–3	1
–16	9	3	–12	7	0	1	5	–1	0
–16	9	4	–12	7	1	0	0	1	0
–15	8	4	–11	6	4	4	24	–3	–1
–14	8	4	–11	6	6	–2	0	–1	0
–14	8	5	–11	6	10	2	1	–4	–1

III. $D_K = 453789, M = \mathbb{Q}(\sqrt{21}), \omega = \frac{1+\sqrt{21}}{2}, f(t) = t^3 - \omega t^2 + (-1+\omega)t + (-3+\omega)$

x_1	x_2	y_0	y_1	y_2	x_1	x_2	y_0	y_1	y_2
–52	25	4	–29	14	–1	4	3	0	–1
–43	16	13	–24	9	0	–1	0	1	0
–12	7	2	–7	3	0	1	0	0	0
–11	5	4	–6	2	1	–2	–1	1	0
–9	9	1	–5	5	1	0	0	0	0
–8	–3	2	3	1	1	1	1	1	–1
–7	3	0	–4	2	1	2	3	0	–1
–5	1	1	–1	1	2	–1	–1	1	0
–5	2	2	–3	1	2	–1	0	1	–1
–5	3	2	–3	1	2	1	1	1	–1
–4	1	0	–2	1	3	–2	0	2	–1
–3	14	12	1	–5	4	3	4	1	–2
–2	2	2	–1	0	5	17	20	–2	–6
–1	2	0	–1	1					

IV. $D_K = 820125, M = \mathbb{Q}(\sqrt{5}), \omega = \frac{1+\sqrt{5}}{2}, f(t) = t^3 + (-6-6\omega)t + (6+11\omega)$

x_1	x_2	y_0	y_1	y_2	x_1	x_2	y_0	y_1	y_2
–10	8	4	6	–5	1	2	–8	2	0
–4	3	2	2	–2	2	–4	–10	0	3
–4	11	16	2	–7	2	–1	–12	2	2
–1	0	0	1	0	2	–1	–4	0	1
–1	1	3	0	–1	2	0	–9	1	1
–1	1	5	0	–1	2	0	–7	1	1
0	–2	8	–3	0	2	1	2	–2	–1
0	0	–2	1	0	3	2	–26	5	2
0	0	8	–2	–1	3	2	–22	6	2
1	0	–4	2	0	6	3	0	–4	–2
1	1	–5	1	0	8	4	–68	13	6
1	1	–3	1	0	9	4	–60	15	6

V. $D_K = 1075648, M = \mathbb{Q}(\sqrt{7}), \omega = \sqrt{7}, f(t) = t^3 - \omega t^2 + \omega$

x_1	x_2	y_0	y_1	y_2	x_1	x_2	y_0	y_1	y_2
–6	–2	1	2	1	3	–5	2	2	–1
–6	2	1	–2	1	3	5	2	–2	–1
–3	0	–1	0	1	5	–8	4	2	–3
1	0	0	0	0	5	8	4	–2	–3
2	–4	1	1	–1	11	–10	7	4	–4
2	0	2	0	–1	11	10	7	–4	–4
2	4	1	–1	–1					

References

1. A. Baker and H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford **20** (1969), 129–137. MR **40:**1333
2. A.M. Bergé, J. Martinet and M. Olivier, *The computation of sextic fields with a quadratic subfield*, Math. Comp. **54** (1990), 869–884. MR **90k:**11169
3. J. Blass, A.M.W. Glass, D.K. Manski, D.B. Meronk and R.P. Steiner, *Constants for lower bounds for linear forms in the logarithms of algebraic numbers II: The homogeneous rational case*, Acta Arith. **55** (1990), 15–22. MR **91h:**11064
4. J. Blass, A.M.W. Glass, D.K. Manski, D.B. Meronk and R.P. Steiner, *Corrigendum to the paper: Constants for lower bounds for linear forms in the logarithms of algebraic numbers II: The homogeneous rational case*, Acta Arith. **65** (1993), p. 383. MR **95d:**11093
5. W.J. Ellison, *Recipes for solving diophantine problems by Baker's method*, Sém. Theorie des Nombres (1970–1971), exp. no. 11. MR **52:**10591
6. V. Ennola, S. Mäki and R. Turunen, *On real cyclic sextic fields*, Math. Comp. **45** (1985), 591–611. MR **86m:**11084
7. J.H. Evertse, K. Győry, C.L. Stewart and R. Tijdeman, *S–unit equations and their applications*, New Advances in Transcendence Theory, ed. by A.Baker, Cambridge University Press, 1988, pp. 110–174. MR **89j:**11028
8. U. Fincke and M. Pohst, *A procedure for determining algebraic integers of given norm*, EUROCAL 83, Lecture Notes in Computer Science, No. 162, Springer Verlag, New York, 1983, pp. 194–202. MR **86k:**11078
9. I. Gaál, *On the resolution of inhomogeneous norm form equations in two dominating variables*, Math. Comp. **51** (1988), 359–373. MR **89m:**11030

10. 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. MR **92g:**11031
11. I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in biquadratic number fields, II*, J. Number Theory **38** (1991), 35–51. MR **92g:**11031
12. I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in biquadratic number fields, III. The bicyclic biquadratic case*, J. Number Theory **53** (1995), 100–114.
13. I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in dihedral number fields*, J. Experimental Math. **3** (1994), 245–254.
14. I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations*, Proc. of the 1991 International Symposium on Symbolic and Algebraic Computation, ed. by Stephen M. Watt, ACM Press, 1991, pp. 185-186.
15. I. Gaál, A. Pethő and M. Pohst, *On the resolution of index form equations in quartic number fields*, J. Symbolic Comp. **16** (1993), 563–584. MR **95f:**11109
16. I. Gaál, A. Pethő and M. Pohst, *Simultaneous representation of integers by a pair of ternary quadratic forms – with an application to index form equations in quartic number fields*, to appear, J. Number Theory.
17. I. Gaál and N. Schulte, *Computing all power integral bases of cubic number fields*, Math. Comp. **53** (1989), 689–696. MR **90b:**11108
18. K. Győry, *Sur les polynomes a coefficients entiers et de discriminant donné, III*, Publ. Math.(Debrecen) **23** (1976), 141–165. MR **55:**10419c
19. A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534. MR **84a:**12002
20. S. Mäki, *The Determination of Units in Real Cyclic Sextic Fields*, Lecture Notes in Mathematics, vol. 797, Springer Verlag, Berlin–Heidelberg–New York, 1980. MR **82a:**12004
21. I. Niven and H.S. Zuckerman, *An introduction to the Theory of Numbers*, J. Wiley and Sons, New York, 1980. MR **81g:**10001
22. M. Pohst, *Computational Algebraic Number Theory*, DMV Seminar, Band 21, Birkhäuser Verlag, Basel – Boston – Berlin, 1993. MR **94j:**11132
23. M. Olivier, *Corps sextiques contenant un corps quadratique (I)*, Séminaire de Théorie des Nombres Bordeaux **1** (1989), 205–250. MR **91g:**11122
24. M. Olivier, *Corps sextiques contenant un corps quadratique (II)*, Séminaire de Théorie des Nombres Bordeaux **2** (1990), 49–102. MR **91g:**11123
25. M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, 1989. MR **92b:**11074
26. W.M. Schmidt, *Diophantine Approximations*, Springer Lecture Notes in Mathematics, No. 785, Springer Verlag, Berlin–Heidelberg–New York, 1980. MR **81j:**10038
27. V.G. Sprindzuk, *Representation of numbers by the norm forms with two dominating variables*, J. Number Theory **6** (1974), 481–486. MR **50:**7045
28. N. Tzanakis and B.M.M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory **31** (1989), 99–132. MR **90c:**11018
29. N. Tzanakis and B.M.M. de Weger, *How to explicitly solve a Thue–Mahler equation*, Compositio Math. **84** (1992), 223–288. MR **93k:**11025
30. B.M.M. de Weger, *Algorithms for Diophantine Equations*, CWI Tract 65, Amsterdam, 1989. MR **90m:**11205
31. B.M.M. de Weger, *A Thue equation with quadratic integers as variables*, Math. Comp. **64** (1995), 855–861. MR **95f:**11020

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