

Power integral bases in sextic fields with a cubic subfield

István Járasi
University of Debrecen,
Institute of Mathematics and Informatics
H-4010 Debrecen Pf.12
e-mail: ijarasi@dragon.klte.hu

June 8, 2005

Abstract

In the present paper we give an algorithm to compute generators of power integral bases having "small" coordinates in an integral basis in sextic fields containing a cubic subfield.

As an application of the method, we give a sufficient condition for infinite parametric families of number fields of this type to have power integral basis. To illustrate the statement we construct parametric families of fields and describe generators of power integral bases in them.

AMS Classification Codes (2000): 11Y50; 11D57

1 Introduction

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

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

It is obvious that $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is an integral basis, if and only if $I(\alpha) = \pm 1$. Such an integral basis is called power integral basis. If there exists such $\alpha \in \mathbb{Z}_K$, then \mathbb{Z}_K is called monogene.

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

$$D(l(x)) = (I(x_2, \dots, x_n))^2 \cdot D_K$$

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

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

the equation

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

holds. So the problem of determining power integral basis is equivalent to determine the elements of index 1 or to solve the index form equation

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

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

$$I(\alpha) = \frac{\prod_{1 \leq i < j \leq n} |\alpha_i - \alpha_j|}{\sqrt{|D_K|}} \quad (1)$$

where α_i ($1 \leq i \leq n$) denote the conjugates of α .

For an arbitrary $z \in \mathbb{Z}$ the indices of $\pm\alpha + z$ are the same. These numbers are called equivalent. In 1976 K.Györy [9] proved effectively that an index form equation has only finitely many solutions, that is up to equivalence there are only finitely many elements of \mathbb{Z}_K of index 1. For a survey on power integral bases see [4].

In this paper we consider sextic fields. There are no general algorithms for solving index form equations in sextic fields. The only case when we can determine the generators of power integral bases is the case of sextic fields with a quadratic subfield, cf. I.Gaál [2], [1] and I.Gaál and M.Pohst [7]. In these cases the index form equation implies a relative Thue equation over the quadratic subfield which makes the resolution easier.

Our purpose is to consider sextic fields having a cubic subfield. This important case is not yet covered by former methods. In this case the index form equation is much more complicated than in the previously considered

sextic fields and it does not seem to be feasible by the known methods to describe a fast algorithm for the complete resolution of the index form equation.

Hence our purpose is to determine the "small" solutions of the index form equation, that is to compute generators of power integral bases having "small" coordinates in an integral basis. In this sense "small" means a bound of about 10^5 which means that the solutions we find cover all solutions with high probability. Especially, the generators of power integral bases used in applications have "small" coordinates.

2 Sextic fields with a cubic subfield

Let K be a sextic field having a cubic subfield M . Let us denote by \mathbb{Z}_K and \mathbb{Z}_M the rings of integers of K and M , respectively. We will consider in detail the more interesting case when M is totally real. The case of complex cubic subfields is much easier to consider using the same algorithm since in that case the unit rank of M is only 1.

Assume $M = \mathbb{Q}(\varrho)$ and $K = M(\vartheta)$ with algebraic integers ϱ, ϑ . For simplicity let us choose ϱ and ϑ so that $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ is an integral basis in K , so that an arbitrary $\alpha \in \mathbb{Z}_K$ can be written as

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

where $x_0, x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}$. Note that if ϱ and ϑ with this property do not exist (this happens very seldom), then in the representation (2) we have to use a common denominator g . In such cases the same algorithm can be used, the only difference is that instead of ± 1 some constants depending on g appear on the right hand sides of our equations.

Let

$$X = x_0 + x_1\varrho + x_2\varrho^2, \quad Y = y_0 + y_1\varrho + y_2\varrho^2,$$

then X and Y are integers in M and

$$\alpha = X + \vartheta Y. \quad (3)$$

3 The structure of the index

We denote by ϱ_i the conjugates of ϱ for $i = 1, 2, 3$ and by $\vartheta_i, \bar{\vartheta}_i$ the conjugates of ϑ over $M_i = \mathbb{Q}(\varrho_i)$ for $i = 1, 2, 3$. In general for any $\gamma \in M$ we denote by γ_i the conjugates of γ corresponding to ϱ_i . For any $\gamma \in K$ we denote by $\gamma_i, \bar{\gamma}_i$ the conjugates of γ corresponding to $\vartheta_i, \bar{\vartheta}_i$, respectively.

Using the integral basis $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ for the discriminant of the field K we get

$$\sqrt{|D_K|} = (\varrho_1 - \varrho_2)^2(\varrho_2 - \varrho_3)^2(\varrho_3 - \varrho_1)^2(\vartheta_1 - \bar{\vartheta}_1)(\vartheta_2 - \bar{\vartheta}_2)(\vartheta_3 - \bar{\vartheta}_3).$$

Let

$$\beta_k = \frac{(\alpha_i - \alpha_j)(\bar{\alpha}_i - \bar{\alpha}_j)(\bar{\alpha}_i - \alpha_j)(\alpha_i - \bar{\alpha}_j)}{(\varrho_i - \varrho_j)^2}, \quad (4)$$

where $k = 1, 2, 3$ belong to $(i, j) = (2, 3), (3, 1), (1, 2)$, respectively.

Then the following theorem holds:

Theorem 1 *If $\alpha \in \mathbb{Z}_K$ generates a power integral basis in K , then β_k is an algebraic integer in $M_k = \mathbb{Q}(\varrho_k)$ for $k = 1, 2, 3$.*

PROOF. First we show, that β_k is an algebraic integer. Let $M_i = \mathbb{Q}(\varrho_i)$. Since $\vartheta_i, \bar{\vartheta}_i$ are the roots of a quadratic polynomial having algebraic coefficients in \mathbb{Z}_{M_i} we have

$$\vartheta_i = \frac{\nu_i + \sqrt{\mu_i}}{2}, \quad \bar{\vartheta}_i = \frac{\nu_i - \sqrt{\mu_i}}{2},$$

and similarly

$$\vartheta_j = \frac{\nu_j + \sqrt{\mu_j}}{2}, \quad \bar{\vartheta}_j = \frac{\nu_j - \sqrt{\mu_j}}{2},$$

where $\nu, \mu \in \mathbb{Z}_M$ are algebraic integers, $\nu_i, \nu_j, \mu_i, \mu_j$ denote their conjugates. Since the relative norms are algebraic integers we have

$$\vartheta_i \cdot \bar{\vartheta}_i = \frac{\nu_i^2 - \mu_i}{4} \in \mathbb{Z}_{M_i}, \quad \vartheta_j \cdot \bar{\vartheta}_j = \frac{\nu_j^2 - \mu_j}{4} \in \mathbb{Z}_{M_j}.$$

Using (3) this implies

$$(\alpha_i - \alpha_j)(\alpha_i - \bar{\alpha}_j) =$$

$$\left(X_i - X_j + \frac{\nu_i + \sqrt{\mu_i}}{2} Y_i - \frac{\nu_j + \sqrt{\mu_j}}{2} Y_j \right) \cdot \left(X_i - X_j + \frac{\nu_i + \sqrt{\mu_i}}{2} Y_i - \frac{\nu_j - \sqrt{\mu_j}}{2} Y_j \right).$$

It is obvious that the difference of the i -th and the j -th conjugates of integers in \mathbb{Z}_M is divisible by $(\varrho_i - \varrho_j)$ because of their representation in the basis $\{1, \varrho, \varrho^2\}$. So in both of the two factors $X_i - X_j$ is divisible by $(\varrho_i - \varrho_j)$. It is similar to show that the same holds for the remaining factor, that is

$$\begin{aligned} & \left(\frac{\nu_i + \sqrt{\mu_i}}{2} Y_i - \frac{\nu_j + \sqrt{\mu_j}}{2} Y_j \right) \cdot \left(\frac{\nu_i + \sqrt{\mu_i}}{2} Y_i - \frac{\nu_j - \sqrt{\mu_j}}{2} Y_j \right) = \\ & - \left(\frac{\nu_i^2 - \mu_i}{4} Y_i^2 - \frac{\nu_j^2 - \mu_j}{4} Y_j^2 \right) + \frac{\nu_i + \sqrt{\mu_i}}{2} Y_i (\nu_i Y_i - \nu_j Y_j) \end{aligned}$$

is divisible by $(\varrho_i - \varrho_j)$. Similarly, $(\bar{\alpha}_i - \alpha_j)(\bar{\alpha}_i - \bar{\alpha}_j)$ is also divisible by $(\varrho_i - \varrho_j)$.

Now we turn to prove that $\beta_k \in M_k = \mathbb{Q}(\varrho_k)$. Let Γ be the Galois group of the field $\bar{M} = \mathbb{Q}(\varrho_1, \varrho_2, \varrho_3)$, and denote by Γ_0 its subgroup containing the automorphisms which leave M_k elementwise fixed. Let $\bar{K} = \mathbb{Q}(\vartheta_1, \bar{\vartheta}_1, \vartheta_2, \bar{\vartheta}_2, \vartheta_3, \bar{\vartheta}_3)$.

Let $\sigma \in \Gamma$ with $\sigma(\varrho_i) = \varrho_{j_i}$, ($i = 1, 2, 3$), where (j_1, j_2, j_3) is a permutation of $(1, 2, 3)$. Let us extend this to an automorphism $\bar{\sigma}$ of \bar{K} such that

$$\bar{\sigma}(\vartheta_i) = \vartheta_{j_i}, \bar{\sigma}(\bar{\vartheta}_i) = \bar{\vartheta}_{j_i}, (i = 1, 2, 3).$$

Let π_i be the automorphism of \bar{K} with

$$\pi_i(\vartheta_i) = \bar{\vartheta}_i, \pi_i(\bar{\vartheta}_i) = \vartheta_i,$$

and

$$\pi_i(\vartheta_j) = \vartheta_j, \pi_i(\bar{\vartheta}_j) = \bar{\vartheta}_j$$

$$\pi_i(\vartheta_k) = \vartheta_k, \pi_i(\bar{\vartheta}_k) = \bar{\vartheta}_k$$

for $i = 1, 2, 3$, $\{j, k\} = \{1, 2, 3\} \setminus \{i\}$. Then any element of the Galois group of \bar{K} can be written in the form

$$\bar{\sigma} \cdot \pi_1^{a_1} \cdot \pi_2^{a_2} \cdot \pi_3^{a_3}$$

where $\bar{\sigma}$ denotes the extension of $\sigma \in \Gamma$ with the above property, and $a_1, a_2, a_3 \in \{0, 1\}$.

It is easy to see, that the automorphisms of \overline{K} which leave M_k element-wise fixed are the form of

$$\overline{\sigma}_0 \cdot \pi_1^{a_1} \cdot \pi_2^{a_2} \cdot \pi_3^{a_3}$$

where $\overline{\sigma}_0$ denotes the extension of $\sigma_0 \in \Gamma_0$ to \overline{K} . (These elements form a subgroup in the Galois group of \overline{K}). It is easily seen that $\overline{\sigma}_0, \pi_1, \pi_2, \pi_3$ leave β_k fixed, so by the Galois theory $\beta_k \in M_k$ holds. ■

The following theorem describes the structure of the index of $\alpha \in \mathbb{Z}_K$. We note that our algorithm for finding "small" generators of power integral basis is based on Theorems 1, 2.

Theorem 2 *If $\alpha \in \mathbb{Z}_K$ represented in the form (2) generates a power integral basis, then*

$$N_{M/\mathbb{Q}}(y_0 + y_1\varrho + y_2\varrho^2) = \pm 1, \quad (5)$$

and

$$N_{M/\mathbb{Q}}(\beta) = \pm 1. \quad (6)$$

PROOF. Recall that for the index of α we have (1). It is obvious that

$$\frac{\alpha_i - \overline{\alpha}_i}{\vartheta_i - \overline{\vartheta}_i} = y_0 + y_1\varrho_i + y_2\varrho_i^2$$

is an algebraic integer in $M_i = \mathbb{Q}(\varrho_i)$ for $i = 1, 2, 3$, these are conjugated to each other and their product is

$$N_{M/\mathbb{Q}}(y_0 + y_1\varrho + y_2\varrho^2).$$

The quotient of the remaining differences of conjugates of α and the remaining factor of $\sqrt{|D_K|}$ is

$$\beta_1\beta_2\beta_3 = N_{M/\mathbb{Q}}(\beta).$$

Since both of them are integers in \mathbb{Z} and their product is ± 1 we obtain (5) and (6). ■

4 The algorithm

Our purpose is to determine elements of index 1 of \mathbb{Z}_K for which

$$\max(|x_1|, |x_2|, |y_0|, |y_1|, |y_2|) < C. \quad (7)$$

In our examples we have $C = 10^5$. We consider only the case when M is totally real. Let $\{\eta_1, \eta_2\}$ be a set of fundamental units of M , and denote by η_{1i}, η_{2i} ($i = 1, 2, 3$) their conjugates.

Step I.

By (5) we have

$$Y_i = \pm \eta_{1i}^{b_1} \eta_{2i}^{b_2}, \quad (i = 1, 2, 3) \quad (8)$$

with $b_1, b_2 \in \mathbb{Z}$. From this we conclude

$$b_1 \log |\eta_{1i}| + b_2 \log |\eta_{2i}| = \log |Y_i|. \quad (i = 1, 2, 3) \quad (9)$$

Using the notation (with i, j as in (4))

$$C_i = \max(\log(C \cdot r_j) + \log(C \cdot r_k), \log(C \cdot r_i))$$

$$C_j = \max(\log(C \cdot r_i) + \log(C \cdot r_k), \log(C \cdot r_j))$$

by (9) we have

$$\begin{aligned} |b_1| &\leq |f_{11}| \cdot C_i + |f_{12}| \cdot C_j \\ |b_2| &\leq |f_{21}| \cdot C_i + |f_{22}| \cdot C_j \end{aligned}$$

where f_{ij} denote the entries of the matrix

$$\begin{pmatrix} \log |\eta_{1i}| & \log |\eta_{2i}| \\ \log |\eta_{1j}| & \log |\eta_{2j}| \end{pmatrix}^{-1}.$$

The above upper bounds are valid for $(i, j) = (1, 2), (2, 3), (3, 1)$. Denote by C_{b_1} and C_{b_2} the minimum of the estimates for $|b_1|$ and $|b_2|$, respectively.

The following steps must be performed for all possible values of b_1 and b_2 with

$$-C_{b_1} \leq b_1 \leq C_{b_1}, \quad -C_{b_2} \leq b_2 \leq C_{b_2}.$$

Step II.

By (6) we have

$$\beta_k = \pm \eta_{1k}^{d_1} \eta_{2k}^{d_2} \quad (k = 1, 2, 3) \quad (10)$$

with $d_1, d_2 \in \mathbb{Z}$. From this we conclude

$$d_1 \log |\eta_{1k}| + d_2 \log |\eta_{2k}| = \log |\beta_k| \quad (k = 1, 2, 3)$$

It is easy to see that

$$\begin{aligned}
\alpha_i - \alpha_j &= X_i - X_j + \vartheta_i Y_i - \vartheta_j Y_j, \\
\bar{\alpha}_i - \bar{\alpha}_j &= X_i - X_j + \bar{\vartheta}_i Y_i - \bar{\vartheta}_j Y_j, \\
\bar{\alpha}_i - \alpha_j &= X_i - X_j + \bar{\vartheta}_i Y_i - \vartheta_j Y_j, \\
\alpha_i - \bar{\alpha}_j &= X_i - X_j + \vartheta_i Y_i - \bar{\vartheta}_j Y_j.
\end{aligned} \tag{11}$$

By (8) the values of b_1 and b_2 determine Y_i and Y_j . Using (4),(10),(11) and the estimate

$$|X_i - X_j| = |x_1(\varrho_i - \varrho_j) + x_2(\varrho_i^2 - \varrho_j^2)| \leq C \cdot (|\varrho_i - \varrho_j| + |\varrho_i^2 - \varrho_j^2|)$$

one can derive upper bounds for $|d_1|$ and $|d_2|$ for $(i, j) = (1, 2), (2, 3), (3, 1)$ similarly as in Step I. Denote by C_{d_1} and C_{d_2} the minimum of these bounds for $|d_1|$ and $|d_2|$, respectively.

The following steps must be performed for all possible values of d_1 and d_2 with

$$-C_{d_1} \leq d_1 \leq C_{d_1}, \quad -C_{d_2} \leq d_2 \leq C_{d_2}.$$

Step III.

Using the above type of indices i, j, k let

$$\begin{aligned}
A_k &= X_i - X_j + \frac{(\vartheta_i + \bar{\vartheta}_i)Y_i - (\vartheta_j + \bar{\vartheta}_j)Y_j}{2}, \\
B_k &= Y_i(\vartheta_i - \bar{\vartheta}_i), \\
C_k &= Y_j(\vartheta_j - \bar{\vartheta}_j).
\end{aligned} \tag{12}$$

Using this notation by (11) we have

$$\begin{aligned}
\alpha_i - \alpha_j &= A_k - \frac{B_k + C_k}{2}, \\
\bar{\alpha}_i - \bar{\alpha}_j &= A_k - \frac{B_k - C_k}{2}, \\
\bar{\alpha}_i - \alpha_j &= A_k + \frac{B_k - C_k}{2}, \\
\alpha_i - \bar{\alpha}_j &= A_k + \frac{B_k + C_k}{2},
\end{aligned}$$

so (10) is equivalent to

$$\begin{aligned} & \left(A_k + \frac{B_k + C_k}{2}\right) \left(A_k - \frac{B_k + C_k}{2}\right) \left(A_k + \frac{B_k - C_k}{2}\right) \left(A_k - \frac{B_k - C_k}{2}\right) \\ &= \pm \eta_{1k}^{d_1} \eta_{2k}^{d_2} (\varrho_i - \varrho_j)^2, \end{aligned}$$

that is

$$\left(A_k^2 - \left(\frac{B_k + C_k}{2}\right)^2\right) \left(A_k^2 - \left(\frac{B_k - C_k}{2}\right)^2\right) = \pm \eta_{1k}^{d_1} \eta_{2k}^{d_2} (\varrho_i - \varrho_j)^2.$$

From this it is easy to see, that the above quartic equation in A_k can be reduced to quadratic equations in A_k . Note that this reduces radically the computational time, because it is much easier to solve a quadratic equation using only a square root than to solve a quartic equation using iteration methods.

Having solved the above equations in A_k , we can calculate $X_i - X_j$ by equation (12). For $k = 1, 2$ we calculate $X_2 - X_3, X_3 - X_1$ and then we can determine x_1 and x_2 from the system of equations

$$\begin{aligned} X_2 - X_3 &= x_1(\varrho_2 - \varrho_3) + x_2(\varrho_2^2 - \varrho_3^2), \\ X_3 - X_1 &= x_1(\varrho_3 - \varrho_1) + x_2(\varrho_3^2 - \varrho_1^2). \end{aligned}$$

If x_1 and x_2 are integers then we found a possible solution of our index form equation.

The values of the y_i -s for $i = 1, 2, 3$ can be determined similarly by solving the system of linear equations (cf. (8))

$$y_0 + y_1 \varrho_i + y_2 \varrho_i^2 = \pm \eta_{1i}^{b_1} \eta_{2i}^{b_2} \quad (i = 1, 2, 3).$$

Obviously, this system of equations has integer solutions in y_0, y_1, y_2 , because by Theorem 2 the Y_i is a unit of M_i and by our assumption $\{1, \varrho_i, \varrho_i^2\}$ is an integral basis in M_i ($i = 1, 2, 3$).

Note that one has to check all candidates of solutions $(x_1, x_2, y_0, y_1, y_2)$, whether α of (3) indeed has index 1.

The case of complex cubic subfields can be considered similarly. Since these fields have unit rank 1 in this case the computation is much easier.

The algorithms were implemented in Maple V and executed on a PII 350 MHz IBM PC compatible machine.

5 Numerical examples

Totally real cubic subfield M :

Example 1:

Let $g(x) = x^3 - 5x - 1$ be the defining polynomial of ϱ . Then the discriminant of the field $\mathbb{Q}(\varrho)$ is $D_M = 11 \cdot 43$, the fundamental units are $\eta_1 = \varrho, \eta_2 = 2 + \varrho$. Let the defining polynomial of ϑ over M be $f(x) = x^2 - 10x - \varrho$. Then its defining polynomial over \mathbb{Q} is $f_0(x) = x^6 - 30x^5 + 300x^4 - 1000x^3 - 5x^2 + 50x - 1$, the discriminant of the field $K = \mathbb{Q}(\vartheta)$ is $D_K = 2^6 \cdot 11^3 \cdot 43^2 \cdot 1409$. Then $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ is an integral basis in K . Using the bound $C = 10^5$ we had $C_{b_1} = 19$, $C_{b_2} = 14$, and $C_{d_1} \leq 205$, $C_{d_2} \leq 158$. The computations were performed with 100 digits of accuracy, the running time was 18 hours. The solutions are:

$$(x_1, x_2, y_0, y_1, y_2) = (0, -10, -5, 0, 1), (0, 0, -5, 0, 1), (0, 0, 1, 0, 0).$$

Example 2:

Let $g(x) = x^3 - 6x + 1$ be the defining polynomial of ϱ . Then the discriminant of the field $\mathbb{Q}(\varrho)$ is $D_M = 3^3 \cdot 31$, the fundamental units are $\eta_1 = \varrho, \eta_2 = 3 - 6\varrho + 2\varrho^2$. Let the defining polynomial of ϑ over M be $f(x) = x^2 - 6x - \varrho$. Then its defining polynomial over \mathbb{Q} is $f_0(x) = x^6 - 18x^5 + 108x^4 - 216x^3 - 6x^2 + 36x + 1$, the discriminant of the field $K = \mathbb{Q}(\vartheta)$ is $D_K = 2^7 \cdot 3^6 \cdot 31^2 \cdot 337$. Then $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ is an integral basis in K . Using the bound $C = 10^5$ we had $C_{b_1} = 16$, $C_{b_2} = 6$, and $C_{d_1} \leq 195$, $C_{d_2} \leq 142$. The computations were performed with 80 digits of accuracy, the running time was 16 hours. The solutions are:

$$(x_1, x_2, y_0, y_1, y_2) = (0, 6, 6, 0, -1), (0, 0, 6, 0, -1), (0, 0, 1, 0, 0).$$

Complex cubic subfield M :

Example 3:

Let $g(x) = x^3 + x^2 - 3x - 5$ be the defining polynomial of ϱ . Then the discriminant of the field $\mathbb{Q}(\varrho)$ is $D_M = -2^2 \cdot 67$, the fundamental unit is $\eta = -2 + \varrho$. Let the defining polynomial of ϑ over M be $f(x) = x^2 - \varrho x + 1$. Then its defining polynomial over \mathbb{Q} is $f_0(x) = x^6 + x^5 - 3x^3 + x + 1$, the discriminant of the field $K = \mathbb{Q}(\vartheta)$ is $D_K = 2^4 \cdot 3 \cdot 67^2$. Then $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ is an integral basis in K . Using the bound $C = 10^5$ we had $C_b = 10$, and $C_d \leq 78$. The computations were performed with 100 digits of accuracy, the running time was 50 minutes. The solutions are:

$$(x_1, x_2, y_0, y_1, y_2) = (-3, -1, 3, 3, 1), (-1, 0, 1, 0, 0).$$

Example 4:

Let $g(x) = x^3 - x^2 + 4x - 2$ be the defining polynomial of ϱ . Then the discriminant of the field $\mathbb{Q}(\varrho)$ is $D_M = -2^2 \cdot 53$, the fundamental unit is $\eta = -1 + 2\varrho$. Let the defining polynomial of ϑ over M be $f(x) = x^2 - \varrho x - 1$. Then its defining polynomial over \mathbb{Q} is $f_0(x) = x^6 - x^5 + x^4 - x^2 - x - 1$, the discriminant of the field $K = \mathbb{Q}(\vartheta)$ is $D_K = 2^6 \cdot 53^2$. Then $\{1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2\}$ is an integral basis in K . Using the bound $C = 10^5$ we had $C_b = 9$, and $C_d \leq 71$. The computations were performed with 100 digits of accuracy, the running time was 40 minutes. The solutions are:

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

6 Constructing infinite parametric families of monogene sextic fields with a cubic subfield

In this section we give a sufficient condition for the existence of infinite parametric families of monogene sextic fields with a cubic subfield.

Theorem 3 *Let b_0, b_1, c_0, c_1 be integers such that*

$$b_1^2 - c_0 c_1 b_1 + b_0 c_1^2 = \pm 1$$

holds.

Let ϱ be an arbitrary cubic algebraic integer, $M = \mathbb{Q}(\varrho)$, $\gamma = c_0 + c_1\varrho$, $\delta = b_0 + b_1\varrho$. Let the coefficients of the quadratic relative defining polynomial of ϑ over M be

$$\vartheta + \bar{\vartheta} = \gamma \tag{13}$$

and

$$\vartheta\bar{\vartheta} = \delta. \quad (14)$$

Then in the order $\mathcal{O} = \mathbb{Z}[1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2]$ of the field $K = \mathbb{Q}(\vartheta)$ the element ϑ generates a power integral basis.

PROOF. By Theorem 2 the element $\alpha = \vartheta$ has index 1 if the corresponding β is a unit in $\mathbb{Q}(\varrho)$. Using the notation of Theorem 3 the element β_k can be written as

$$\beta_k = \frac{(\delta_i - \delta_j)^2 + (\gamma_i - \gamma_j)(\delta_j\gamma_i - \delta_i\gamma_j)}{(\varrho_i - \varrho_j)^2}.$$

Substituting γ and δ from (13),(14) we obtain

$$\beta_k = b_1^2 - c_0c_1b_1 + b_0c_1^2 = \pm 1$$

and this completes the proof. \blacksquare

Note that making more assumptions on $\mathbb{Q}(\varrho)$ one can prove similar results using the structure of its group of units.

Remark:

It is easy to see that the equation

$$b_1^2 - c_0c_1b_1 + b_0c_1^2 = \pm 1 \quad (15)$$

has infinitely many solutions in \mathbb{Z} . For example let $c_0 = 2n$ ($n \in \mathbb{Z}$). Then one can see that $b_0 \leq n^2 + 1$ is needed, and the solutions of (15) are obtained in the following way:

if the signs of c_1 and b_1 are the same, then

$$(c_0, c_1) = (2n, \pm 1), (b_0, b_1) = (n^2 + 1, \pm n),$$

$$(c_0, c_1) = (2n, \pm 1), (b_0, b_1) = (n^2 - 1, \pm n);$$

if $c_1 \in \mathbb{Z}$ arbitrary, then

$$(c_0, c_1) = (2n, c_1), (b_0, b_1) = (n^2, nc_1 \pm 1);$$

and for an arbitrary $b_0 = n^2 - k$, $1 < k \in \mathbb{N}$ one has to consider the infinitely many solutions of the Pellian equation

$$(nc_1 - b_1)^2 - kc_1^2 = \pm 1.$$

Of course in the construction one has to check whether the relative quadratic defining polynomial of ϑ is irreducible over $\mathbb{Q}(\varrho)$

Examples:

Example 1: Let $x^3 - (4k^2 + 4k)x^2 - (4k^2 + 4k + 1)x - (4k^2 + 4k)$, $1 \leq k$ be the defining polynomial of ϱ . It is irreducible for $k \in \mathbb{Z}$, $k \neq -1, 0$. Let the coefficients of the quadratic relative defining polynomial of ϑ over $M = \mathbb{Q}(\varrho)$ be $\vartheta + \bar{\vartheta} = -2n + \varrho$, $\vartheta\bar{\vartheta} = n^2 + 1 - n\varrho$. Then one can see that the quadratic relative defining polynomial of ϑ over M is irreducible for $n \geq 1$ so by the theorem ϑ generates a power integral basis in the order $\mathbb{Z}[1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2]$ of the field $K = \mathbb{Q}(\vartheta)$.

Example 2: Let $x^3 - nx^2 - (n+1)x - 1$ be the defining polynomial of ϱ . Let the coefficients of the quadratic relative defining polynomial of ϑ over $M = \mathbb{Q}(\varrho)$ be $\vartheta + \bar{\vartheta} = -2k + \varrho$, $\vartheta\bar{\vartheta} = k^2 + 1 - k\varrho$. So the quadratic relative defining polynomial of ϑ over M is irreducible for arbitrary $k \in \mathbb{Z}$ so by the theorem ϑ generates a power integral basis in the order $\mathbb{Z}[1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2]$ of the field $K = \mathbb{Q}(\vartheta)$.

Example 3:

Let $x^3 - (n-1)x^2 - (n+2)x - 1$ be the defining polynomial of ϱ . Let the coefficients of the quadratic relative defining polynomial of ϑ over $M = \mathbb{Q}(\varrho)$ be $\vartheta + \bar{\vartheta} = -2k + \varrho$, $\vartheta\bar{\vartheta} = k^2 + 1 - k\varrho$. So the quadratic relative defining polynomial of ϑ over M is irreducible for arbitrary $k \in \mathbb{Z}$ so by the theorem ϑ generates a power integral basis in the order $\mathbb{Z}[1, \varrho, \varrho^2, \vartheta, \vartheta\varrho, \vartheta\varrho^2]$ of the field $K = \mathbb{Q}(\vartheta)$.

References

- [1] I.Gaál, *Computing elements of given index in totally complex cyclic sextic fields*, J.Symbolic Comput., **20**(1995), 61–69.
- [2] I.Gaál, *Computing all power integral bases in orders of totally real cyclic sextic number fields*, Math. Comp., **65**(1996), 801–822.
- [3] I.Gaál, *Power integral bases in composites of number fields*, Canad. Math. Bull., **41**(1998), 158–165.

- [4] I.Gaál, *Power integer bases in algebraic number fields*, Ann. Univ. Sci. Budapest.Sect. Comput., **18** (1999), 61–87.
- [5] I.Gaál and K.Györy, *On the resolution of index form equations in quintic fields*, Acta Arith., **89**(1999), 379–396.
- [6] 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*, J.Number Theory, **57**(1996), 90–104.
- [7] I.Gaál and M.Pohst, *On the resolution of index form equations in sextic fields with an imaginary quadratic subfield*, J.Symbolic Comp., **22**(1996), 425–434.
- [8] I.Gaál and N.Schulte, *Computing all power integral bases of cubic number fields*, Math. Comp., **53** (1989), 689–696.
- [9] K.Györy, *Sur les polynomes a coefficients entiers et de discriminant donne, III*, Publ. Math.(Debrecen), **23**(1976), 141–165.
- [10] M.Mignotte and N.Tzanakis, *On a family of cubics*, J.Number Theory, **39**(1991), 41–49.
- [11] E.Thomas, *Complete solutions to a family of cubic diophantine equations*, J.Number Theory, **34**(1990), 235–250.