JP Journal of Algebra, Number Theory and Applications

http://www.pphmj.com
http://dx.doi.org/10.17654/NT047010087
Volume 47, Number 1, 2020, Pages 87-98 **ISSN: 0972-5555**

MONOGENITY IN TOTALLY COMPLEX SEXTIC FIELDS, REVISITED

István Gaál

Mathematical Institute
University of Debrecen
H-4002 Debrecen Pf. 400, Hungary
e-mail: gaal.istvan@unideb.hu

Abstract

In addition to rather complicated general methods it is interesting and valuable to develop fast efficient methods for calculating generators of power integral bases in special types of number fields. We consider sextic fields containing real cubic and complex quadratic fields. We develop a very simple and very efficient method to calculate generators of power integral bases in this type of fields. Our method can be applied to infinite families of number fields, as well. We substantially improve the former methods. Our algorithm is illustrated with detailed examples, involving infinite parametric families.

1. Introduction

In the following we shall denote by $\mathbb{Z}_K$ and D_K the ring of integers and the discriminant, respectively, of any number field K.

There is an extensive literature of monogenity of number fields and

Received: April 8, 2020; Accepted: May 20, 2020
2010 Mathematics Subject Classification: Primary 11R04, 11R21; Secondary 11Y50; 11D59.
Keywords and phrases: monogenity, power integral basis, Thue equations, sextic fields, calculating the solutions.

power integral bases, see [11], [7]. A number field K of degree n is *monogenic* if $\mathbb{Z}_K$ is a simple ring extension of $\mathbb{Z}$, that is there exists $\alpha \in \mathbb{Z}_K$ with $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. In this case $(1, \alpha, \ldots, \alpha^{n-1})$ is an integral basis of K, called *power integral basis.* (We also call α the *generator* of this power integral basis.) The algebraic integer α generates a power integral basis if and only if its *index*

$$I(\alpha) = \sqrt{\left| \frac{D(\alpha)}{D_K} \right|}$$

is equal to 1, where $D(\alpha)$ is the discriminant of α.

The calculation of generators of power integral bases can be reduced to certain diophantine equations, called *index form equations*, cf. [7].

There exist general algorithms for solving index form equations in cubic, quartic, quintic, sextic fields, however the general algorithms for quintic and sextic fields are already quite tedious, see [2]. Therefore it is worthy to develop efficient methods for the resolution of special types of higher degree number fields.

In this paper we study totally complex sextic fields that are composites of a totally real cubic and an imaginary quadratic fields. These fields were investigated in [6] where we reduced the relative Thue equation involved to absolute Thue inequalities. That method was further developed in [9]. However some ideas of [8] lead to a considerable improvement of that algorithm, what we are going to detail here. We also note that a parametric family of this type of number fields, consisting of composites of the simplest cubic fields and imaginary quadratic fields was studied in [10], but applying results on the connected simplest family of relative Thue equations, which counts as a more complicated approach.

2. Composites of Real Cubic and Imaginary Quadratic Fields

Let $\vartheta = \vartheta^{(1)}, \vartheta^{(2)}, \vartheta^{(3)}$ be the roots of the totally real polynomial $f(x)$

$= x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ and let $L = \mathbb{Q}(\vartheta)$. Let $0 < d \in \mathbb{Z}$ be a square-free integer, set $M = \mathbb{Q}(i\sqrt{d})$. Our purpose is to calculate all generators of power integral bases in $K = L \cdot M = \mathbb{Q}(\vartheta, i\sqrt{d})$. Set

$$\omega = i\sqrt{d} \text{ if } -d \equiv 2, 3 \pmod 4 \text{ and } \omega = \frac{1 + i\sqrt{d}}{2} \text{ if } -d \equiv 1 \pmod 4.$$

Denote by γ' the conjugate of any $\gamma \in M$.

To make our presentation as simple as possible, we formulate our statements for the order

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

The cubic field L very often happens to have integral basis $(1, \vartheta, \vartheta^2)$, and if D_L is relatively prime to D_M, then indeed $\mathcal{O} = \mathbb{Z}_K$. However, otherwise our statements are applicable with minor modifications, see Remark 2.

Let us represent any $\alpha \in \mathcal{O}$ in the form

$$\alpha = x_0 + x_1\vartheta + x_2\vartheta^2 + y_0\omega + y_1\omega\vartheta + y_2\omega\vartheta^2 = X_0 + X_1\vartheta + X_2\vartheta^2, \quad (1)$$

where $x_j, y_j \in \mathbb{Z}$, $X_j = x_j + \omega y_j \in \mathbb{Z}_M$ $(j = 0, 1, 2)$.

The conjugates of α are obtained the following way:

$$\begin{aligned}\alpha^{(j,1)} &= x_0 + x_1\vartheta^{(j)} + x_2(\vartheta^{(j)})^2 + y_0\omega + y_1\omega\vartheta^{(j)} + y_2\omega(\vartheta^{(j)})^2 \\ &= X_0 + X_1\vartheta^{(j)} + X_2(\vartheta^{(j)})^2, \\ \alpha^{(j,2)} &= x_0 + x_1\vartheta^{(j)} + x_2(\vartheta^{(j)})^2 + y_0\omega' + y_1\omega'\vartheta^{(j)} + y_2\omega'(\vartheta^{(j)})^2 \\ &= X_0' + X_1'\vartheta^{(j)} + X_2'(\vartheta^{(j)})^2,\end{aligned}$$

for $j = 1, 2, 3$.

Keeping the coefficients as variables, consider the symmetric polynomial

$$F(x_1, x_2, y_0, y_1, y_2)$$

$$= (\alpha^{(1,1)} - \alpha^{(2,2)})(\alpha^{(1,1)} - \alpha^{(2,3)})(\alpha^{(1,2)} - \alpha^{(2,1)})$$

$$(\alpha^{(1,2)} - \alpha^{(2,3)})(\alpha^{(1,3)} - \alpha^{(2,1)})(\alpha^{(1,3)} - \alpha^{(2,2)}),$$

having all coefficients in $\mathbb{Z}$.

Theorem 1. *If* $\alpha \in \mathcal{O}$ (*in the representation* (1)) *generates a power integral basis in* $\mathcal{O}$, *then the coefficients* $x_1, x_2, y_0, y_1, y_2 \in \mathbb{Z}$ *of* α *satisfy*

$$F(x_1, x_2, y_0, y_1, y_2) = \pm 1, \tag{2}$$

and

$$N_{L/Q}(y_0 + y_1\vartheta + y_2\vartheta^2) = \pm 1. \tag{3}$$

Further, if $-d \equiv 2, 3 \pmod 4$, *then*

$$|N_{L/Q}(x_1 - (a_2 + \vartheta)x_2)| \leq 1 \tag{4}$$

and

$$|N_{L/Q}(y_1 - (a_2 + \vartheta)y_2)| \leq \frac{1}{(\sqrt{d})^3}. \tag{5}$$

If $-d \equiv 1 \pmod 4$, *then*

$$|N_{L/Q}((2x_1 + y_1) - (a_2 + \vartheta)(2x_2 + y_2))| \leq 8 \tag{6}$$

and

$$|N_{L/Q}(y_1 - (a_2 + \vartheta)y_2)| \leq \frac{8}{(\sqrt{d})^3}. \tag{7}$$

Recall, that a_2 is the coefficient of the quadratic term of the defining polynomial of ϑ.

Proof of Theorem 1.

The discriminant of the basis $(1, \vartheta, \vartheta^2, \omega, \omega\vartheta, \omega\vartheta^2)$ of $\mathcal{O}$ is

$$D_{\mathcal{O}} = D(\vartheta)^2 \cdot D_M^3. \tag{8}$$

For $j, k \in \{1, 2, 3\}$, $j \neq k$ we have

$$\begin{aligned}\alpha^{(1,j)} - \alpha^{(1,k)} &= (\vartheta^{(j)} - \vartheta^{(k)})(X_1 + (\vartheta^{(j)} + \vartheta^{(k)})X_2) \\ &= (\vartheta^{(j)} - \vartheta^{(k)})(X_1 - (a_2 + \vartheta^{(\ell)})X_2), \\ \alpha^{(2,j)} - \alpha^{(2,k)} &= (\vartheta^{(j)} - \vartheta^{(k)})(X_1' + (\vartheta^{(j)} + \vartheta^{(k)})X_2') \\ &= (\vartheta^{(j)} - \vartheta^{(k)})(X_1' - (a_2 + \vartheta^{(\ell)})X_2'),\end{aligned}$$

where $\ell = \{1, 2, 3\}\backslash\{j, k\}$. Therefore

$$\prod_{s=1}^{2} \prod_{1 \le j < k \le 3} (\alpha^{(s,j)} - \alpha^{(s,k)}) = D(\vartheta) \cdot N_{M/Q}(N_{K/M}(X_1 - (a_2 + \vartheta)X_2)). \quad (9)$$

Further,

$$\alpha^{(1,j)} - \alpha^{(2,j)} = (\omega - \omega')(y_0 + y_1\vartheta^{(j)} + y_2(\vartheta^{(j)})^2),$$

hence

$$\prod_{j=1}^{3} (\alpha^{(1,j)} - \alpha^{(2,j)}) = (\omega - \omega')^3 N_{L/Q}(y_0 + y_1\vartheta + y_2\vartheta^2). \quad (10)$$

The remaining factors of $I(\alpha)$ are just those of $F(x_1, x_2, y_0, y_1, y_2)$. In view of (8) this implies that

$$\begin{aligned}I(\alpha) = \sqrt{\left|\frac{D(\alpha)}{D_{\mathcal{O}}}\right|} &= N_{M/Q}(N_{K/M}(X_1 - (a_2 + \vartheta)X_2)) \cdot N_{L/Q}(y_0 \\ &\quad + y_1\vartheta + y_2\vartheta^2) \cdot F(x_1, x_2, y_0, y_1, y_2),\end{aligned}$$

or equivalently, $I(\alpha) = 1$, if and only if (2), (3) and

$$N_{M/Q}(N_{K/M}(X_1 - (a_2 + \vartheta)X_2)) = \pm 1, \quad (11)$$

simultaneously hold.

Our present improvement concerns this last equation. (11) implies

$$|N_{K/M}(X_1 - (a_2 + \vartheta)X_2)| = \pm 1 \tag{12}$$

since the norm M/Q is just the product of the above norm and its complex conjugate. We obtain

$$\left| \prod_{j=1}^{3} ((x_1 + \omega y_1) - (a_2 + \vartheta^{(j)})(x_2 + \omega y_2)) \right| = 1.$$

Set $\beta^{(j)} = (x_1 + \omega y_1) - (a_2 + \vartheta^{(j)})(x_2 + \omega y_2)$, $j = 1, 2, 3$. Obviously $|\mathrm{Re}(\beta^{(j)})| \le |\beta^{(j)}|$ and $|\mathrm{Im}(\beta^{(j)})| \le |\beta^{(j)}|$, for $j = 1, 2, 3$, whence

$$\prod_{j=1}^{3} |\mathrm{Re}(\beta^{(j)})| \le \prod_{j=1}^{3} |\beta^{(j)}| = 1 \text{ and } \prod_{j=1}^{3} |\mathrm{Im}(\beta^{(j)})| \le |\beta^{(j)}| = 1. \tag{13}$$

If $-d \equiv 2, 3 \pmod 4$, then

$$\mathrm{Re}(\beta^{(j)}) = x_1 - (a_2 + \vartheta^{(j)})x_2, \quad \mathrm{Im}(\beta^{(j)}) = y_1 - (a_2 + \vartheta^{(j)})y_2,$$

and (13) implies (4), (5).

If $-d \equiv 1 \pmod 4$, then

$$\mathrm{Re}(\beta^{(j)}) = \frac{1}{2}((2x_1 + y_1) - (a_2 + \vartheta^{(j)})(2x_2 + y_2)),$$

$$\mathrm{Im}(\beta^{(j)}) = \frac{\sqrt{d}}{2}(y_1 - (a_2 + \vartheta^{(j)})y_2),$$

and (13) implies (6), (7).

Remark 1.

We already had equations (3) and (12) in [6], but (4), (5), (6), (7) are much stronger than the corresponding inequalities of Theorem 2.2 in [6]. These will be very useful in applications, see Sections 3, 4.

Remark 2.

If $\mathcal{O}$ is not equal to $\mathbb{Z}_K$, then any $\alpha \in \mathbb{Z}_K$ can be written in the form

$$\alpha = \frac{x_0 + x_1\vartheta + x_2\vartheta^2 + y_0\omega + y_1\omega\vartheta + y_2\omega\vartheta^2}{g}$$

with a common denominator $g \in \mathbb{Z}$. This implies

$$N_{M/Q}(N_{K/M}(X_1 - (a_2 + \vartheta)X_2)) \cdot N_{L/Q}(y_0 + y_1\vartheta + y_2\vartheta^2) \cdot F(x_1, x_2, y_0, y_1, y_2) = \pm g^{15}.$$

This factor g^{15} splits into a product of integers g_1, g_2, g_3 with $g_1g_2g_3 = g^{15}$ such that g_1, g_2, g_3 occur on the right hand sides of the above three factors, that is we get (2) with right hand side $\pm g_1$, (3) with right hand side $\pm g_2$ and (4), (5), (6), (7) with right hand sides equal to g_1 times the original right hand sides.

3. How to Apply Theorem 1?

If $d \neq 1$ in case $-d \equiv 2, 3 \pmod 4$, then (5) has only the trivial solutions $y_1 = y_2 = 0$, whence by (3) we obtain $y_0 = \pm 1$.

Similarly, if $d \neq 3$ in case $-d \equiv 1 \pmod 4$, then (7) has only the trivial solutions $y_1 = y_2 = 0$, whence by (3) we obtain $y_0 = \pm 1$.

For the Gaussian integers $(d = 1)$ and Euler integers $(d = 3)$, (5), resp. (7) are Thue inequalities with some small right hand sides.

For any given y_1, y_2 equation (3) is just a cubic polynomial equation in the integer variable y_0.

In case $-d \equiv 2, 3 \pmod 4$ we can determine x_1, x_2 from the Thue equation (4).

In case $-d \equiv 1 \pmod 4$, given y_1, y_2 we can determine x_1, x_2 from the Thue equation (6), solving it with right hand sides 0, 1, …, 8.

Remark that using Magma [3] or Kash [5] it is no problem to solve cubic Thue equations with small right hand sides within a few seconds.

Having calculated x_1, x_2, y_0, y_1, y_2 we have to check if α of (1) has indeed index 1 (equations (2), (3), (11) together are equivalent with $I(\alpha) = 1$, but the inequalities (4), (5) and (6), (7), respectively, are weaker than (11)).

It is easy to explicitly calculate the polynomial $F(x_1, x_2, y_0, y_1, y_2)$. Equation (2) is very useful if we consider monogenity in infinite parametric families of number fields, see Section 4.

4. Examples

4.1. Example 1

Let $t \in \mathbb{Z}$ and consider the infinite parametric family of polynomials

$$f_t(x) = x^3 - (t^4 - t)x^2 + (t^5 - 2t^2)x + 1. \tag{14}$$

According to [1] the polynomial f_t has three real roots for $t \geq 2$. In the following let $t \geq 2$ and denote by ϑ_t a root of f_t. Let $L_t = \mathbb{Q}(\vartheta_t)$.

Set $F_t(x, y) = y^3 f_t(x/y)$. The infinite parametric family of Thue equations

$$F_t(x, y) = N_{L_t/Q}(x - \vartheta_t y) = 1 \text{ in } x, y \in \mathbb{Z} \tag{15}$$

was recently considered by Bennett and Ghadermarzi [1]. They showed that for $t \neq -1$ all solutions of the above equation are $(x, y) = (1, 0), (0, 1), (t, 1), (t^4 - 2t, 1), (1 - t^3, t^8 - 3t^5 + 3t^2)$ and for $t = -1$ it has the additional solution $(x, y) = (6, -5)$.

Let $d > 1$ be a square-free integer with $-d \equiv 2, 3 \pmod 4$ and let $\omega = i\sqrt{d}$.

Consider the order $\mathcal{O}_{t,d} = \mathbb{Z}[1, \vartheta_t, \vartheta_t^2, \omega, \omega\vartheta_t, \omega\vartheta_t^2]$ of the number field $K_{t,d} = \mathbb{Q}(\vartheta_t, i\sqrt{d})$. Remark that $(1, \vartheta_t, \vartheta_t^2)$ very often happens to be an integer basis of $\mathbb{Q}(\vartheta_t)$ (in case the discriminant of f_t is square-free, but also in other cases). Further if $(1, \vartheta_t, \vartheta_t^2)$ is an integer basis of $\mathbb{Q}(\vartheta_t)$ and the discriminant of f_t is co-prime to $4d$, then $\mathcal{O}_{t,d}$ is just the ring of integers of $K_{t,d}$.

We have

Theorem 2. *For $t \geq 2$, $d > 1$, $-d \equiv 2, 3 \pmod 4$, the order $\mathcal{O}_{t,d}$ is never monogenic.*

Proof of Theorem 2.

For $d > 1$ we have $y_1 = y_2 = 0$ from (5) and $y_0 = \pm 1$ from (3). The solutions of (4) we obtain from the result of [1] on equation (15), by a suitable transformation (if x, y is a solution of (15), then $x_1 = x + a_2 y$, $x_2 = y$ is a solution of (4), where a_2 is the coefficient of x^2 in the defining polynomial of ϑ_t, that is, $a_2 = t^4 - t$ in our case).

We substitute all possible x_1, x_2, y_0, y_1, y_2 into $F(x_1, x_2, y_0, y_1, y_2)$. We obtain cubic polynomials in d. Their coefficients are polynomials in t. All these coefficients are negative for $t \geq 2$, that is (2) cannot be satisfied.

4.2. Example 2

Let $f(x) = x^3 - x^2 - 2x + 1$. This polynomial (with discriminant 49) has real roots. Denote by ϑ a root of f. Let $L = \mathbb{Q}(\vartheta)$, with integral basis $(1, \vartheta, \vartheta^2)$.

Let $d \geq 1$ be a square-free integer, set $\omega = i\sqrt{d}$ if $-d \equiv 2, 3 \pmod 4$ and $\omega = (1 + i\sqrt{d})/2$ if $-d \equiv 1 \pmod 4$.

Consider the order $\mathcal{O}_d = \mathbb{Z}[1, \vartheta, \vartheta^2, \omega, \omega\vartheta, \omega\vartheta^2]$ of the field $K_d = \mathbb{Q}(\vartheta, i\sqrt{d})$. If $4d$ (respectively d) is co-prime to 49, then $\mathcal{O}_d$ is the ring of integers of $K_d = \mathbb{Q}(\vartheta, i\sqrt{d})$. We have

Theorem 3. *The order $\mathcal{O}_d$ is only monogenic for $d = 1$, in which case all generators of power integral bases are of the form*

$$\alpha = x_0 + x_1\vartheta + x_2\vartheta^2 + iy_0 + iy_1\vartheta + iy_2\vartheta^2,$$

where $x_0 \in \mathbb{Z}$,

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

Proof of Theorem 3.

I.A. Assume $-d \equiv 2, 3 \pmod 4$ and $d > 1$. Then we have $y_1 = y_2 = 0$ from (5) and $y_0 = \pm 1$ from (3). To calculate x_1, x_2 we solve equation (4), that is,

$$|N_{L/Q}(x_1 - (-1 + \vartheta)x_2)| \leq 1$$

by Magma. Substituting all possible x_1, x_2, y_0, y_1, y_2 into $F(x_1, x_2, y_0, y_1, y_2)$, we obtain cubic polynomials in d with all negative coefficients, that is (2) cannot be satisfied.

I.B. Let $d = -1$. We calculate all solutions y_1, y_2 of (5). For all these explicit values we determine y_0 from (3). We determine the possible values of x_1, x_2 from (4). Calculating the indices of α of (1) for all possible x_1, x_2, y_0, y_1, y_2 we obtain the generators of power integral bases.

II.A. Assume $-d \equiv 1 \pmod 4$ and $d > 3$. Then we have $y_1 = y_2 = 0$ from (7) and $y_0 = \pm 1$ from (3). To calculate x_1, x_2 we solve equation (6). We substitute all possible x_1, x_2, y_0, y_1, y_2 into $F_3(x_1, x_2, y_0, y_1, y_2)$ and obtain that (2) cannot be satisfied.

II.B. Let $d = 3$. Using Magma we calculate the possible solutions of (7). For all these y_1, y_2 we calculate y_0 from (3). Further, for all y_1, y_2 we calculate the solutions x_1, x_2 of (6). Testing the indices of α of (1) for all these x_1, x_2, y_0, y_1, y_2, we do not get any elements of index 1.

5. Computational Aspects

All calculations connected with the above examples were performed in Maple [4], except for solving the Thue equations, which was done in Kash [5] and Magma [3]. Our procedures were executed on an average laptop running under Windows. The CPU time took all together some seconds.

References

[1] M. A. Bennett and A. Ghadermarzi, Extremal families of cubic Thue equations, J. Théor. Nombres Bordx. 27 (2015), 389-403.

[2] Y. Bilu, I. Gaál and K. György, Index form equations in sextic fields: a hard computation, Acta Arith. 115 (2004), 85-96.

[3] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system, I. The user language, J. Symbolic Comput. 24 (1997), 235-265.

[4] B. W. Char, K. O. Geddes, G. H. Gonnet, M. B. Monagan and S. M. Watt (eds.), MAPLE, Reference Manual, Watcom Publications, Waterloo, Canada, 1988.

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

[6] I. Gaál, Computing elements of given index in totally complex cyclic sextic fields, J. Symbolic Comput. 20(1) (1995), 61-69.

[7] I. Gaál, Diophantine Equations and Power Integral Bases: Theory and Algorithms, 2 ed. ed., Birkhäuser, Boston, 2019.

[8] I. Gaál, Calculating "small" solutions of inhomogeneous relative Thue inequalities, submitted.

[9] I. Gaál, B. Jadrijević and L. Remete, Totally real Thue inequalities over imaginary quadratic fields, Glas. Mat. Ser. III 53(2) (2018), 229-238.

[10] I. Gaál and L. Remete, Power integral bases in a family of sextic fields with quadratic subfields, Tatra Mt. Math. Publ. 64 (2015), 59-66.

[11] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, 3rd ed., Springer, 2004.