Journal de Théorie des Nombres
de Bordeaux **18** (2006), 537–557

Bases of canonical number systems in quartic algebraic number fields

par Horst BRUNOTTE, Andrea HUSZTI et Attila PETHŐ

Dedicated to Professor Michael Pohst on the occasion of his 60th birthday

Résumé. Les systèmes canoniques de numération peuvent être considérés comme des généralisations naturelles de la numération classique des entiers. Dans la présente note, une modification d'un algorithme de B. Kovács et A. Pethő est établie et appliquée au calcul des systèmes canoniques de numération dans certains anneaux d'entiers de corps de nombres algébriques. L'algorithme permet de déterminer tous les systèmes canoniques de numération de quelques corps de nombres de degré quatre.

Abstract. Canonical number systems can be viewed as natural generalizations of radix representations of ordinary integers to algebraic integers. A slightly modified version of an algorithm of B. Kovács and A. Pethő is presented here for the determination of canonical number systems in orders of algebraic number fields. Using this algorithm canonical number systems of some quartic fields are computed.

1. Introduction

The investigation of the question wether an algebraic number field is monogenic is a classical problem in algebraic number theory (cf. [9]). According to B. Kovács [19] the existence of a power integral basis in an algebraic number field is equivalent to the existence of a canonical number system for its maximal order. Moreover, using a deep result of K. Győry [13] on generators of orders of algebraic number fields B. Kovács [19] proved that up to translation by integers there exist only finitely many canonical number systems in the maximal order of an algebraic number field.

Let R be an order of an algebraic number field and $\alpha \in R$.

[1]Research was supported in part by grant T67580 of the Hungarian National Foundation for Scientific Research

Manuscrit reçu le 10 janvier 2006.

Mots clefs. canonical number system, radix representation, power integral basis.

Definition. (cf. [3], Definition 4.1, [5]) The algebraic integer α is called a basis of a canonical number system (or CNS basis) for R if every nonzero element of R can be represented in the form

$$n_0 + n_1\alpha + \cdots + n_l\alpha^l$$

with $n_i \in \{0, \ldots, |Norm_{\mathbb{Q}(\alpha)|\mathbb{Q}}(\alpha)| - 1\}, n_l \neq 0$.

Canonical number systems can be viewed as natural generalizations of radix representations of ordinary integers (V. Grünwald [12]) to algebraic integers. Originating from observations of D. E. Knuth [17] (see also [18], Ch. 4) the theory of canonical number systems was developed by I. Kátai and J. Szabó [16], B. Kovács [19], I. Kátai and B. Kovács ([14], [15]), W. J. Gilbert [10] and others. There are connections to the theories of finite automata (see e.g. K. Scheicher [30], J. M. Thuswaldner [32]) and fractal tilings (see e.g. S. Akiyama and J. M. Thuswaldner [5]). Recently S. Akiyama et al. [2] put canonical number systems (CNS) into a more general framework thereby opening links to other areas, e.g. to a long-standing problem on Salem numbers.

B. Kovács and A. Pethő [20] established an algorithm for finding all CNS bases of monogenic algebraic number fields (see also [27] for a comprehensive description of this algorithm and its background). In this note we present a slightly modified version of this algorithm for the determination of CNS bases of orders of algebraic number fields. The method is exploited here for some families of number fields of low degrees; our main applications are cyclotomic and simple fields of degree four. CNS bases in quadratic number fields were described by several authors (see [14],[15],[10],[11],[32],[4] and others); further, CNS bases are explicitely known for some cubic and quartic fields ([20], [3], [27]). The list of CNS bases of simplest cubic fields given in [3] is extended in the present note too.

The authors wish to express many thanks to Professors S. Akiyama and J. M. Thuswaldner for their constant support.

2. CNS bases of algebraic number fields

In the sequel we denote by $\mathbb{Q}$ the field of rational numbers, by $\mathbb{Z}$ the set of integers and by $\mathbb{N}$ the set of nonnegative integers. For an algebraic integer γ we let $\mu_\gamma \in \mathbb{Z}[X]$ be its minimal polynomial and $\mathcal{C}_\gamma$ the set of all CNS bases for $\mathbb{Z}[\gamma]$. We denote by $\mathcal{C}$ the set of CNS polynomials; for the general definition of CNS polynomials we refer the reader to A. Pethő [25], however, for our purposes it suffices to keep in mind that α is a CNS basis for $\mathbb{Z}[\alpha]$ if and only if μ_α is a CNS polynomial. It can algorithmically be decided whether a given integral polynomial is a CNS polynomial or not (see [1]).

B. Kovács [19] introduced the following set of polynomials

$$\mathcal{K} = \{p_d X^d + p_{d-1}X^{d-1} + \cdots + p_0 \in \mathbb{Z}[X] \mid \\ d \geq 1, 1 = p_d \leq p_{d-1} \leq \ldots \leq p_1 \leq p_0 \geq 2\}$$

which plays a decisive role in the theory of CNS polynomials (see [1], Theorem 2.3).

Lemma 2.1. (B. Kovács – A. Pethő) *For every nonzero algebraic integer α the following constants can be computed effectively:*

$$k_\alpha = \min\{k \in \mathbb{Z} \mid \mu_\alpha(X+n) \in \mathcal{K} \text{ for all } n \in \mathbb{Z} \text{ with } n \geq k\},$$

$$c_\alpha = \min\{k \in \mathbb{Z} \mid \mu_\alpha(X+k) \in \mathcal{C}\}.$$

Proof. See [20], Section 5. □

Note that $c_\alpha \leq k_\alpha$ by ([19], Lemma 2) and that if β is a conjugate of α then $k_\beta = k_\alpha$ and $c_\beta = c_\alpha$.

Corollary 2.1. *If α is a CNS basis for an order R then $c_\alpha \leq 0, \alpha - c_\alpha$ is a CNS basis for R, but $\alpha - c_\alpha + 1$ is not a CNS basis for R.*

Proof. This is clear by the definitions. □

To a polynomial $P(X) = p_d X^d + p_{d-1}X^{d-1} + \cdots + p_0 \in \mathbb{Z}[X], p_d = 1$ we associate the mapping $\tau_P = \tau : \mathbb{Z}^d \to \mathbb{Z}^d$ defined by

$$\tau_P(\underline{A}) = \left(-\left\lfloor \frac{p_1 A_1 + \cdots + p_d A_d}{p_0} \right\rfloor, A_1, \ldots, A_{d-1} \right),$$

where $\underline{A} = (A_1, \ldots, A_d) \in \mathbb{Z}^d$. This turned out very useful to prove $P(X) \in \mathcal{C}$. Indeed Brunotte [7] proved the following theorem, that gives an efficient algorithm for testing if a polynomial is CNS or not.

Theorem 2.1. *Assume that $E \subseteq \mathbb{Z}^d$ has the following properties:*

(i) $(1, 0, \ldots, 0) \in E$,
(ii) $-E \subseteq E$,
(iii) $\tau(E) \subseteq E$,
(iv) *for every $e \in E$ there exist some $l > 0$ with $\tau^l(e) = 0$.*

Then $P(X) \in \mathcal{C}$.

The following notion seems to be convenient for the intentions of the present note.

Definition. The algebraic integer α is called a fundamental CNS basis for R if it satisfies the following properties:

(1) $\alpha - n$ is a CNS basis for R for all $n \in \mathbb{N}$.
(2) $\alpha + 1$ is a not CNS basis for R.

Theorem 2.2. *Let γ be an algebraic integer. Then there exist finite effectively computable disjoint subsets $\mathcal{F}_0(\gamma), \mathcal{F}_1(\gamma) \subset \mathcal{C}_\gamma$ with the properties:*

(i) *For every $\alpha \in \mathcal{C}_\gamma$ there exists some $n \in \mathbb{N}$ with $\alpha + n \in \mathcal{F}_0(\gamma) \cup \mathcal{F}_1(\gamma)$.*
(ii) *$\mathcal{F}_1(\gamma)$ consists of fundamental CNS bases for $\mathbb{Z}[\gamma]$.*

Proof. By ([20], Theorem 5) there exist finitely many effectively computable

$$\alpha_1, \dots, \alpha_t \in \mathbb{Z}[\gamma], \quad n_1, \dots, n_t \in \mathbb{Z}, \quad N_1, \dots, N_t \subset \mathbb{Z}, \quad N_1, \dots, N_t \text{ finite}$$

such that for every $\alpha \in \mathbb{Z}[\gamma]$ we have

$$\begin{aligned} &(2.1) \quad \alpha \in \mathcal{C}_\gamma \iff \\ &\qquad \alpha = \alpha_i - h \text{ for some } i \in \{1, \dots, t\}, \quad h \in \mathbb{Z} \text{ and } h \geq n_i \text{ or } h \in N_i. \end{aligned}$$

Therefore the set

$$F := \{\alpha_i - n_i \,|\, i = 1, \dots, t\} \cup \bigcup_{i=1}^{t} \{\alpha_i - h \,|\, h \in N_i\}$$

is a finite effectively computable subset of $\mathcal{C}_\gamma$.

For every $\alpha \in F$ let

$$M_\alpha = \{m \in \mathbb{Z} \,|\, m \leq k_\alpha, \alpha - k \in \mathcal{C}_\gamma \text{ for all } k = m, \dots, k_\alpha\}.$$

Observing $m \geq c_\alpha$ for all $m \in M_\alpha$ we see using Lemma 2.1 that M_α is a nonempty finite effectively computable set. Let

$$m_\alpha = \min M_\alpha$$

and

$$\mathcal{F}_0(\gamma) = \{\alpha - c_\alpha \,|\, \alpha \in F, m_\alpha > c_\alpha\}, \quad \mathcal{F}_1(\gamma) = \{\alpha - c_\alpha \,|\, \alpha \in F, m_\alpha = c_\alpha\}.$$

We show that $\mathcal{F}_1(\gamma)$ consists of fundamental CNS bases for $\mathbb{Z}[\gamma]$. Let $\varphi \in \mathcal{F}_1(\gamma)$, hence $\varphi = \alpha - c_\alpha$ with some $\alpha \in F$. By Corollary 2.1 we have $\varphi \in \mathcal{C}_\gamma, \varphi + 1 \notin \mathcal{C}_\gamma$. For $n \in \mathbb{N}$ we find

$$\varphi - n = \alpha - (m_\alpha + n) \in \mathcal{C}_\gamma,$$

because for $m_\alpha + n \leq k_\alpha$ this is clear by the definition of m_α, and for $m_\alpha + n > k_\alpha$ we have $\mu_{\varphi - n} = \mu_\alpha(X + (m_\alpha + n)) \in \mathcal{K}$ and therefore $\varphi - n \in \mathcal{C}_\gamma$ by ([19], Lemma 2).

Let $\beta \in \mathcal{C}_\gamma$. By (2.1) there are $i \in \{1, \dots, t\}$ and $h \in \mathbb{Z}$ with

$$\beta = \alpha_i - h \text{ and } h \geq n_i \text{ or } h \in N_i.$$

If $h \in N_i$ then $\beta \in F$ and $\beta - c_\beta \in \mathcal{F}_0(\gamma) \cup \mathcal{F}_1(\gamma)$ by Corollary 2.1. If $h \geq n_i$ then $\alpha = \alpha_i - n_i \in F, h - n_i - c_\alpha \in \mathbb{N}$ and

$$\beta + (h - n_i - c_\alpha) = \alpha - c_\alpha \in \mathcal{F}_0(\gamma) \cup \mathcal{F}_1(\gamma).$$

□

Remark. Note that $\varphi \in \mathcal{F}_0(\gamma)$ implies $\varphi - n \in \mathcal{F}_1(\gamma)$ for some $n \in \mathbb{N} \setminus \{0\}$. Therefore the theorem of B. KOVÁCS ([19], Lemma 2) can be rephrased in the following form: An algebraic number field is monogenic if and only if there exists a fundamental CNS basis for its maximal order.

Slightly modifying the algorithm of B. KOVÁCS and A. PETHŐ [20] we now present the algorithm for finding the above mentioned sets $\mathcal{F}_0(\gamma)$ and $\mathcal{F}_1(\gamma)$. The (finite) set T is introduced to keep track of the calculations performed; in some cases (see e.g. Theorem 3.1) the amount of computations can thereby be reduced. Recall that algebraic integers α, β are called equivalent if there is some $z \in \mathbb{Z}$ such that $\beta = z \pm \alpha$ (see e.g. [9]).

Algorithm 2.1. *(CNS basis computation)*

[Input] *A nonzero algebraic integer γ and a (finite) set $\mathcal{B}$ of representatives of the equivalence classes of generators of power integral bases of $\mathbb{Z}[\gamma]$.*

[Output] *The sets $\mathcal{F}_0(\gamma)$ and $\mathcal{F}_1(\gamma)$.*

(1.) [Initialize] *Set $\{\beta_1, \ldots, \beta_t\} = \mathcal{B} \cup (-\mathcal{B})$, $F_0 = F_1 = T = \emptyset$ and $i = 1$.*

(2.) [Compute minimal polynomial] *Compute $P = \mu_{\beta_i}$.*

(3.) [Element of $F_0 \cup F_1$ found?] *If there exist $k \in \mathbb{Z}, \delta \in \{0, 1\}$ with $(P, k, \delta) \in T$ insert $\beta_i - k$ into F_δ and go to step 11.*

(4.) [Determine upper and lower bounds] *Calculate k_{β_i} and c_{β_i}.*

(5.) [Insert element into F_1?] *If $k_{\beta_i} - c_{\beta_i} \leq 1$ insert $\beta_i - c_{\beta_i}$ into F_1, $(P, c_{\beta_i}, 1)$ into T and go to step 11, else perform step 6 for $l = c_{\beta_i} + 1, \ldots, k_{\beta_i} - 1$, put $p_{k_{\beta_i}} = 1, k = c_{\beta_i}$ and go to step 8.*

(6.) [Check CNS property] *If $P(X + l) \in \mathcal{C}$ set $p_l = 1$, otherwise set $p_l = 0$.*

(7.) [Check CNS basis condition] *If $p_k = 0$ then go to step 9.*

(8.) [Insert element into $F_0 \cup F_1$] *If $p_{k+1} = \cdots = p_{k_{\beta_i}} = 1$ insert $\beta_i - k$ into F_1, $(P, k, 1)$ into T and go to step 11, else insert $\beta_i - k$ into F_0 and $(P, k, 0)$ into T.*

(9.) [Next value of k] *Set $k \leftarrow k + 1$.*

(10.) [CNS basis check finished?] *If $k \leq k_{\beta_i} - 1$ then go to step 7.*

(11.) [Next generator] *Set* $i \leftarrow i+1$.

(12.) [Finish?] *If* $i \leq t$ *then go to step 2.*

(13.) [Terminate] *Output* $\mathcal{F}_0(\gamma) = F_0$ *and* $\mathcal{F}_1(\gamma) = F_1$ *and terminate the algorithm.*

We verify that the algorithm above delivers all CNS bases of a given order $\mathbb{Z}[\gamma]$.

Theorem 2.3. *Let* γ *be a nonzero algebraic integer and* $\mathcal{B}$ *a set of representatives of the equivalence classes of generators of power integral bases of* $\mathbb{Z}[\gamma]$. *Then Algorithm 2.1 computes the sets* $\mathcal{F}_0(\gamma), \mathcal{F}_1(\gamma)$ *with properties (i) and (ii) of Theorem 2.2.*

Proof. It is easy to see that $\mathcal{F}_0(\gamma) \cup \mathcal{F}_1(\gamma) \subset \mathcal{C}_\gamma$ and that $\mathcal{F}_1(\gamma)$ consists of fundamental CNS bases for $\mathbb{Z}[\gamma]$. Let $\alpha \in \mathcal{C}_\gamma$, hence $\alpha = n + \beta$ with some $n \in \mathbb{Z}, \beta \in \mathcal{B} \cup (-\mathcal{B})$. Clearly, $-n \geq c_\beta$. By construction there is some integer $k \in [c_\beta, k_\beta]$ with $\beta - k \in \mathcal{F}_0(\gamma) \cup \mathcal{F}_1(\gamma)$. Let $l_1, \ldots, l_s \in [c_\beta, k_\beta]$ be exactly those indices with $p_{l_\sigma} = 0 \quad (\sigma = 1, \ldots, s)$ and $c_\beta < p_1 < \ldots < p_s < k_\beta$. If $-n \geq l_s + 1$ then $\varphi = \beta - (l_s+1) \in \mathcal{F}_1(\gamma)$ and $\alpha = \varphi - (-n - (l_s+1))$. Finally, let $-n < l_s + 1$, and observe that $-n \notin \{l_1, \ldots, l_s\}$. Then $-n < l_1$ or $l_\sigma < -n < l_{\sigma+1}$ for some $\sigma \in \{1, \ldots, s-1\}$ imply $\alpha \in \mathcal{F}_0(\gamma)$. □

The following example illustrates the application of Algorithm 2.1. For polynomials outside the set $\mathcal{K}$ the CNS property was checked by the algorithm described in [7] (an improved version of this algorithm was implemented by T. BORBÉLY [6]).

Remark. Note that if $c_\beta < k_\beta$ and $\mu_\beta(X + k) \in \mathcal{C}$ for all $k \in \{c_\beta + 1, \ldots, k_\beta - 1\}$ then $-c_\beta + \beta \in \mathcal{F}_1(\gamma)$.

Lemma 2.2. *Let* $k \in \mathbb{Z}$.

(i) *For* $f_k = f(X+k)$ *with* $f = X^3 - X + 3 \in \mathbb{Z}[X]$ *we have*

$$f_k \in \mathcal{K} \iff k \geq 3$$

and

$$f_k \in \mathcal{C} \iff k = 0 \text{ or } k \geq 2.$$

(ii) *For* $f_k = f(X+k)$ *with* $f = X^3 - X - 3 \in \mathbb{Z}[X]$ *we have*

$$f_k \in \mathcal{K} \iff k \geq 4$$

and

$$f_k \in \mathcal{C} \iff k \geq 3.$$

(iii) *For* $f_k = f(X+k)$ *with* $f = X^3 - 2X^2 - 69X - 369 \in \mathbb{Z}[X]$ *we have*

$$f_k \in \mathcal{K} \iff k \geq 13 \iff f_k \in \mathcal{C}.$$

(iv) *For* $f_k = f(X+k)$ *with* $f = X^3 + 2X^2 - 69X + 369 \in \mathbb{Z}[X]$ *we have*

$$f_k \in \mathcal{K} \iff k \geq 5$$

and

$$f_k \in \mathcal{C} \iff k \geq 4.$$

Proof. (i) The first statement is clear because $f_k = X^3 + 3kX^2 + (3k^2-1)X + k^3 - k + 3$. Using this, Gilbert's theorem (see [3], Theorem 3.1) and ([3], Proposition 3.12) the second statement follows.
(ii) The first statement is clear because $f_k = X^3 + 3kX^2 + (3k^2-1)X + k^3 - k - 3$. Using this and Gilbert's theorem (see [3], Theorem 3.1) and checking $f_3 \in \mathcal{C}$ the second statement follows.
(iii) Clearly, $k < 13$ implies $f_k = X^3 + (3k-2)X^2 + (3k^2 - 4k - 69)X + k^3 - 2k^2 - 69k - 369 \notin \mathcal{K} \cup \mathcal{C}$.
(iv) Observing $f_k = X^3 + (3k+2)X^2 - (3k^2+4k-69)X + k^3 + 2k^2 - 69k + 369$ and checking $f_4 \in \mathcal{C}$ these statements can be proved analogously. □

For a monogenic algebraic number field K we write $\mathcal{F}_\delta(K)$ instead of $\mathcal{F}_\delta(\gamma)$ where γ is some generator of a power integral basis of K $(\delta \in \{0,1\})$.

Example. Let ϑ be a root of the polynomial $X^3 - X + 3 \in \mathbb{Z}[X]$. By ([9], Section 11.1) up to equivalence all generators of power integral bases of $\mathbb{Z}[\vartheta]$ are given by ϑ and $-5\vartheta + 3\vartheta^2$. By Lemma 2.2 we have $c_\vartheta = 0, k_\vartheta = 3$, and therefore by Algorithm 2.1

$$\vartheta \in \mathcal{F}_0(\mathbb{Q}(\vartheta)), -2 + \vartheta \in \mathcal{F}_1(\mathbb{Q}(\vartheta)).$$

Analogously, we have $\mu_{-\vartheta} = X^3 - X - 3, c_{-\vartheta} = 3, k_{-\vartheta} = 4$, and then

$$-3 + \vartheta \in \mathcal{F}_1(\mathbb{Q}(\vartheta)).$$

Similarly, we have $\mu_{-5\vartheta+\vartheta^2} = X^3 - 2X^2 - 69X - 369, c_{-5\vartheta+\vartheta^2} = k_{-5\vartheta+\vartheta^2} = 13$, and

$$-13 - 5\vartheta + \vartheta^2 \in \mathcal{F}_1(\mathbb{Q}(\vartheta)),$$

and finally $\mu_{5\vartheta-\vartheta^2} = X^3 + 2X^2 - 69X + 369, c_{5\vartheta-\vartheta^2} = 4, k_{5\vartheta-\vartheta^2} = 5$, and

$$-4 + 5\vartheta - \vartheta^2 \in \mathcal{F}_1(\mathbb{Q}(\vartheta)).$$

Collecting our results we find $\mathcal{F}_0(\mathbb{Q}(\vartheta)) = \{\vartheta\}$ and

$$\mathcal{F}_1(\mathbb{Q}(\vartheta)) = \{-2+\vartheta, -3-\vartheta, -13-5\vartheta+\vartheta^2, -4+5\vartheta-\vartheta^2\}.$$

In some cases the determination of CNS bases is considerably easier if γ is an algebraic integer with at least one real conjugate. We then denote by $M(\gamma)$ $(m(\gamma))$ the integer part of the maximum (minimum) of the real conjugates of γ.

Proposition 2.1. *Let γ be a nonzero algebraic integer with at least one real conjugate and $\mathcal{B}$ a set of representatives of the equivalence classes of generators of power integral bases of $\mathbb{Z}[\gamma]$.*

(i) *For $\alpha \in \mathbb{Z}[\gamma] \setminus \{0\}$ we have $c_\alpha \geq M(\alpha) + 2$ and $c_{-\alpha} \geq -m(\alpha) + 1$.*
(ii) *Let $\beta \in \mathcal{B}$. Then $\beta - M(\beta) - 2 \in \mathcal{F}_1(\gamma)$ if $\mu_{\beta - M(\beta) - 2} \in \mathcal{K}$, and $-\beta + m(\beta) - 1 \in \mathcal{F}_1(\gamma)$ if $\mu_{-\beta + m(\beta) - 1} \in \mathcal{K}$.*
(iii) *If $\mu_{\beta - M(\beta) - 2}, \mu_{-\beta + m(\beta) - 1} \in \mathcal{K}$ for all $\beta \in \mathcal{B}$ then we have $\mathcal{F}_0(\gamma) = \emptyset$ and*

$$\mathcal{F}_1(\gamma) = \big\{\beta - M(\beta) - 2, -\beta + m(\beta) - 1 \,|\, \beta \in \mathcal{B}\big\}.$$

Proof. (0) For every $\alpha \in \mathbb{Z}[\gamma]$ we have real embeddings τ_α, ρ_α of $\mathbb{Q}(\gamma)$ with

$$M(\alpha) \leq \tau_\alpha(\alpha), \quad \rho_\alpha(\alpha) < m(\alpha) + 1.$$

(i) Assume $c_\alpha = M(\alpha) + 2 - k$ for some $k \in \mathbb{N} \setminus \{0\}$. Then $\mu_\alpha(X + M(\alpha) + 2 - k) \in \mathcal{C}$, thus by ([1], Theorem 2.1)

$$\tau_\alpha(\alpha) - (M(\alpha) + 2 - k) < -1$$

which by (0) yields the contradiction

$$M(\alpha) < M(\alpha) - k + 1.$$

The other inequality is proved analogously.
(ii) It is enough to show that $(\beta - M(\beta) - 2) + 1, (-\beta + m(\beta) - 1) + 1 \notin \mathcal{C}$. In view of ([1], Theorem 2.1) this is clear because by (0)

$$\tau_\beta(\beta - M(\beta) - 1) = \tau_\beta(\beta) - M(\beta) - 1 \geq M(\beta) - M(\beta) - 1 = -1,$$

$$\rho_\beta(-\beta + m(\beta)) > -m(\beta) - 1 + m(\beta) = -1.$$

(iii) Denoting by $F = \big\{\beta - M(\beta) - 2, -\beta + m(\beta) - 1 \,|\, \beta \in \mathcal{B}\big\}$ it suffices to show that

$$\mathcal{C}_\gamma \subset \big\{\varphi - n \,|\, \varphi \in F, n \in \mathbb{N}\big\}.$$

Let $\alpha \in \mathcal{C}_\gamma, \beta \in \mathcal{B}, n \in \mathbb{Z}$ with $\alpha = n \pm \beta$. In case $\alpha = n + \beta$ we have $-M(\beta) - 2 - n \in \mathbb{N}$ by (0) and

$$\alpha + (-M(\beta) - 2 - n) = \beta - M(\beta) - 2 \in F,$$

and in case $\alpha = n - \beta$ we analogously find $m(\beta) - 1 - n \in \mathbb{N}$ and

$$\alpha + (m(\beta) - 1 - n) = -\beta + m(\beta) - 1 \in F.$$

□

3. CNS bases in quadratic and cubic number fields

We conclude our observations by computing $\mathcal{F}_0$ and $\mathcal{F}_1$ of several quadratic, cubic and quartic number fields. For the sake of completeness we start with the formulation of some well-known results in our language.

CNS bases of quadratic number fields were studied by several authors (see [14],[15],[10], [11], [32],[4] and others).

Theorem 3.1. (I. Kátai – B. Kovács, W. J. Gilbert) *Let $D \neq 0, 1$ be a square-free rational integer and $\vartheta = \sqrt{D}$. Then $\mathcal{F}_0(\mathbb{Q}(\vartheta)) = \emptyset$ and*

$$\mathcal{F}_1(\mathbb{Q}(\vartheta)) = \begin{cases} \left\{-\left\lfloor \frac{1+\sqrt{D}}{2} \right\rfloor + \frac{-3+\vartheta}{2}, \left\lfloor \frac{1-\sqrt{D}}{2} \right\rfloor - \frac{3+\vartheta}{2}\right\} & , \text{ if } D > 0, D \equiv 1 \\ & \pmod 4, \\ \left\{-2 - \left\lfloor \sqrt{D} \right\rfloor + \vartheta, -2 - \left\lfloor \sqrt{D} \right\rfloor - \vartheta\right\} & , \text{ if } D > 0, D \not\equiv 1 \\ & \pmod 4, \\ \left\{\frac{-3+\vartheta}{2}, -\frac{3+\vartheta}{2}\right\} & , \text{ if } D = -3, \\ \left\{\frac{1+\vartheta}{2}, \frac{1-\vartheta}{2}\right\} & , \text{ if } D < 0, D \neq -3, \\ & D \equiv 1 \pmod 4, \\ \left\{-1+\vartheta, -1-\vartheta\right\} & , \text{ if } D = -1, \\ \left\{\vartheta, -\vartheta\right\} & , \text{ if } D < 0, D \neq -1, \\ & D \not\equiv 1 \pmod 4. \end{cases}$$

Proof. A representative of the generators of power integral bases of $\mathbb{Q}(\vartheta)$ is given by $\beta = \frac{1+\vartheta}{2}$ if $D \equiv 1 \pmod 4$ ($\beta = \vartheta$ if $D \not\equiv 1 \pmod 4$). If $D > 0$ we have $m(\beta) = \left\lfloor \frac{1-\sqrt{D}}{2} \right\rfloor, M(\beta) = \left\lfloor \frac{1+\sqrt{D}}{2} \right\rfloor$ for $D \equiv 1 \pmod 4$ ($m(\beta) = \left\lfloor -\sqrt{D} \right\rfloor, M(\beta) = \left\lfloor \sqrt{D} \right\rfloor$ for $D \not\equiv 1 \pmod 4$) and our assertions follow from Proposition 2.1 and ([10], Theorem 1). For $D < 0$ Algorithm 2.1 and ([10], Theorem 1) yield the assertions. □

Using a theorem of S. Körmendi [21] S. Akiyama et al. ([3], Theorem 4.5) described all CNS in a family of pure cubic number fields.

Theorem 3.2. (S. Kőrmendi – S. Akiyama *et al.*) *Let $m \in \mathbb{N} \setminus \{0\}$ be not divisible by 3 and $m^3 + 1$ squarefree. For $\vartheta = \sqrt[3]{m^3+1}$ we have $\mathcal{F}_0(\mathbb{Q}(\vartheta)) = \emptyset$ and*

$$\mathcal{F}_1(\mathbb{Q}(\vartheta)) = \{-\vartheta, -m-2+\vartheta, -2m^2-2+m\vartheta+\vartheta^2, -m^2-2-m\vartheta-\vartheta^2\}.$$

Further, S. Akiyama et al. ([3], Theorem 4.4) determined all CNS in a family of simplest cubic number fields (for details see D. Shanks [31]). We state and slightly extend their result in our context.

Theorem 3.3. (S. Akiyama *et al.*) *Let $t \in \mathbb{Z}, t \geq -1$ and ϑ denote a root of the polynomial*

$$X^3 - tX^2 - (t+3)X - 1.$$

Then we have $\mathcal{F}_0(\mathbb{Q}(\vartheta)) = \emptyset$ and

$$\mathcal{F}_1(\mathbb{Q}(\vartheta)) = \{-3-\vartheta, -t-5-t\vartheta+\vartheta^2, -1+(t+1)\vartheta-\vartheta^2\} \cup \mathcal{G} \cup \mathcal{G}_{-1} \cup \mathcal{G}_0 \cup \mathcal{G}_2$$

where

$$\mathcal{G} = \begin{cases} \{-t-3+\vartheta, -1+t\vartheta-\vartheta^2, -t-5-(t+1)\vartheta+\vartheta^2\}, & \text{if } t \geq 0, \\ \emptyset \text{ otherwise}, \end{cases}$$

$$\mathcal{G}_{-1} = \begin{cases} \{-3+\vartheta, -2-\vartheta-\vartheta^2, -5+\vartheta^2, -19+9\vartheta+4\vartheta^2, -5-9\vartheta-4\vartheta^2 \\ \quad -22+5\vartheta+9\vartheta^2, -2-5\vartheta-9\vartheta^2, -25-4\vartheta+5\vartheta^2, 1+4\vartheta-5\vartheta^2, \\ \quad -7-\vartheta+\vartheta^2, -1+\vartheta-\vartheta^2, -6+2\vartheta+\vartheta^2, -2-2\vartheta-\vartheta^2, \\ \quad -6+\vartheta+2\vartheta^2, -2-\vartheta-\vartheta^2\}, & \text{if } t = -1, \\ \emptyset \text{ otherwise}, \end{cases}$$

$$\mathcal{G}_0 = \begin{cases} \{-9+2\vartheta+\vartheta^2, -2-2\vartheta-\vartheta^2, -11-3\vartheta+2\vartheta^2, -1+3\vartheta-2\vartheta^2, \\ \quad -10-\vartheta+3\vartheta^2, -1+\vartheta-3\vartheta^2\}, & \text{if } t = 0, \\ \emptyset \text{ otherwise}, \end{cases}$$

$$\mathcal{G}_2 = \begin{cases} \{-37+3\vartheta+2\vartheta^2, -2-3\vartheta-2\vartheta^2, -42-20\vartheta+9\vartheta^2, \\ \quad 3+20\vartheta-9\vartheta^2, -43-23\vartheta+7\vartheta^2, -4+23\vartheta-7\vartheta^2\}, & \text{if } t = 2, \\ \emptyset \text{ otherwise}. \end{cases}$$

Proof. We proceed similarly as in Example 2, but leave the verifications of computational details to the reader. By [9] up to equivalence all generators of power integral bases of $\mathbb{Z}[\vartheta]$ are the following:

- for arbitrary t: $\vartheta, -t\vartheta+\vartheta^2, (t+1)\vartheta-\vartheta^2$;
- for $t=-1$ additionally: $9\vartheta+4\vartheta^2, 5\vartheta+9\vartheta^2, -4\vartheta+5\vartheta^2, -\vartheta+\vartheta^2, 2\vartheta+\vartheta^2, \vartheta+2\vartheta^2$;
- for $t=0$ additionally: $2\vartheta+\vartheta^2, -3\vartheta+2\vartheta^2, -\vartheta+3\vartheta^2$;
- for $t=2$ additionally: $3\vartheta+2\vartheta^2, -20\vartheta+9\vartheta^2, -23\vartheta+7\vartheta^2$.

The proof is now accomplished by Proposition 2.1 and Table 1 below where we use the following notation: β is a generator of a power integral basis of $\mathbb{Q}(\vartheta)$. The minimal polynomial $\mu_\beta = X^3+a_1X^2+a_2X+a_3$ of β is given by (a_1, a_2, a_3). Lower bounds for the constants c_β, k_β are given by Proposition 2.1. For their determination ([3], Theorem 3.1) and ([8], Theorem 5.1) are used. Observe that in all cases considered here Remark 2 applies if $c_\beta \leq k_\beta - 2$ or $c_{-\beta} \leq k_{-\beta} - 2$. □

β	t	μ_β	$m(\beta)$	$M(\beta)$	c_β	k_β	$c_{-\beta}$	$k_{-\beta}$
ϑ	≥ 5	$(-t, -t-3, -1)$	-2	$t+1$	$t+3$	$t+3$	3	3
ϑ	$0 \dots 4$	$(-t, -t-3, -1)$	-2	$t+1$	$t+3$	$t+3$	3	4
ϑ	-1	$(1, -2, -1)$	-2	1	3	4	3	4
$-t\vartheta+\vartheta^2$	≥ 5	$(-2t-6, t^2+7t+9, -t^2-3t-1)$	0	$t+3$	$t+5$	$t+5$	1	1
$-t\vartheta+\vartheta^2$	$2, 3, 4$	$(-2t-6, t^2+7t+9, -t^2-3t-1)$	0	$t+3$	$t+5$	$t+6$	1	1
$-\vartheta+\vartheta^2$	1	$(-8, 17, -5)$	0	4	6	7	1	2
ϑ^2	0	$(-6, 9, -1)$	0	3	5	6	1	2
$\vartheta+\vartheta^2$	-1	$(-4, 3, 1)$	-1	2	4	5	2	3
$(t+1)\vartheta-\vartheta^2$	≥ 3	$(t+6, 3t+9, 2t+3)$	$-t-4$	-1	1	2	$t+5$	$t+5$
$(t+1)\vartheta-\vartheta^2$	$0, 1, 2$	$(t+6, 3t+9, 2t+3)$	$-t-4$	-1	1	2	$t+5$	$t+6$
$-\vartheta^2$	-1	$(5, 6, 1)$	-4	-1	1	3	5	6
$3\vartheta+2\vartheta^2$	2	$(-34, -39, -11)$	-1	35	37	37	2	3
$-20\vartheta+9\vartheta^2$	2	$(-86, 2041, -8029)$	4	40	42	43	-3	-3
$-23\vartheta+7\vartheta^2$	2	$(-52, 477, -1217)$	5	41	43	43	-4	-3
$9\vartheta+4\vartheta^2$	-1	$(-11, -102, -181)$	-4	17	19	19	5	6
$5\vartheta+9\vartheta^2$	-1	$(-40, 391, 181)$	-1	20	22	23	2	2
$-4\vartheta+5\vartheta^2$	-1	$(-29, 138, -181)$	2	23	25	25	-1	0
$-\vartheta+\vartheta^2$	-1	$(-6, 5, -1)$	0	5	7	7	1	2
$2\vartheta+\vartheta^2$	0	$(-6, -9, -3)$	-1	7	9	9	2	3
$2\vartheta+\vartheta^2$	-1	$(-3, -4, -1)$	-1	4	6	6	2	3
$-3\vartheta+2\vartheta^2$	0	$(-12, 27, -17)$	1	9	11	11	0	1
$-\vartheta+3\vartheta^2$	0	$(-18, 87, -53)$	0	8	10	11	1	1
$\vartheta+2\vartheta^2$	-1	$(-9, 20, 1)$	-1	4	6	7	2	2

TABLE 1

4. CNS bases in quartic cyclotomic fields

In this section we treat the cyclotomic fields of degree 4.

Theorem 4.1. *Let ζ be a primitive eighth root of unity. Then we have $\mathcal{F}_0(\mathbb{Q}(\zeta)) = \emptyset$ and*

$$\mathcal{F}_1(\mathbb{Q}(\zeta)) = \{-3 \pm \zeta^k \mid k = 1, 3, 5, 7\}.$$

Proof. By R. ROBERTSON [29] up to equivalence all generators of power integral bases of $\mathbb{Q}(\zeta)$ are given by $\zeta^k, k \in \mathbb{Z}, k$ odd. Observing $\mu_\zeta = X^4 + 1$ one immediately finds $k_\zeta = 4$. The algorithm described in [7] and ([4], Theorem 5.4) yield $c_\zeta = 3$, and a straightforward application of Algorithm 2.1 concludes the proof. □

Theorem 4.2. *Let ζ be a primitive twelfth root of unity. Then we have $\mathcal{F}_0(\mathbb{Q}(\zeta)) = \emptyset$ and*

$$\mathcal{F}_1(\mathbb{Q}(\zeta)) = \{-3+\zeta, -3-\zeta, -3+\zeta^{-1}, -3-\zeta^{-1}, -1-\zeta^2+\zeta^{-1}, -2+\zeta^2-\zeta^{-1}\}.$$

Proof. The proof works analogously as that of Theorem 4.1. □

Theorem 4.3. *Let ζ be a primitive fifth root of unity. Then we have $\mathcal{F}_0(\mathbb{Q}(\zeta)) = \emptyset$ and*

$$\mathcal{F}_1(\mathbb{Q}(\zeta)) = \{-2+\zeta, -3-\zeta, -2+\zeta+\zeta^3, -3-\zeta-\zeta^3\}.$$

Proof. By [28] up to equivalence all generators of power integral bases of $\mathbb{Z}[\zeta]$ are ζ and $\frac{1}{1+\zeta}$. One immediately checks that

$$f_k(X) = \mu_\zeta(X+k) \in \mathcal{K} \iff k \geq 4,$$

hence $k_\zeta = 4$. By ([4], Theorem 5.4) one finds $k \geq -5$ for $f_k \in \mathcal{C}$. Trivially, $f_0, f_{-1} \notin \mathcal{C}$, and an application of the algorithm described in [7] yields $f_k \notin \mathcal{C}$ for $k = -5, -4, -3, -2, 1$, but $f_2, f_3 \in \mathcal{C}$. Thus we have shown that

$$f_k \in \mathcal{C} \iff k \geq 2,$$

hence $c_\zeta = 2$ and $f_k \in \mathcal{C}$ for all $k \in \{c_\zeta, \ldots, k_\zeta\}$.

β	μ_β	c_β	k_β	$c_{-\beta}$	$k_{-\beta}$
ζ	$(1,1,1,1)$	2	4	3	5
$-\zeta-\zeta^3$	$(-2,4,-3,1)$	3	5	2	4

TABLE 2

Therefore by Algorithm 2.1 we find $-2+\zeta \in \mathcal{F}_1(\mathbb{Q}(\zeta))$. Similarly, the other cases are dealt with. The main data are listed in Table 2 below where we use the following notation: β is a generator of a power integral basis of $\mathbb{Q}(\zeta)$, the minimal polynomial $\mu_\beta = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4$ of β is given by (a_1, a_2, a_3, a_4). □

5. CNS bases in quartic number fields

For the convenience of the reader we rephrase a result of A. PETHŐ ([27], Theorem 15) in our settings.

Theorem 5.1. (A. Pethő) *Let $f \in \mathbb{N}, f \geq 3, f$ odd, $m = f^2 + 2$ and $n = f^2 - 2$. Then we have $\mathcal{F}_0(\mathbb{Q}(\sqrt{m}, \sqrt{n})) = \emptyset$ and*

$$\mathcal{F}_1(\mathbb{Q}(\sqrt{m}, \sqrt{n})) = \{ -f - 1 + \vartheta_1, -f - 1 - \vartheta_1, -1 - \frac{3f^3 + f}{2} + \vartheta_2, \\ -2 - \frac{f^3 - f}{2} - \vartheta_2\}$$

where

$$\vartheta_1 = \frac{\sqrt{m} + \sqrt{n}}{2}, \quad \vartheta_2 = f\frac{1 + \sqrt{mn}}{2} + \sqrt{n} + (f^2 - 1)\frac{\sqrt{m} + \sqrt{n}}{2}.$$

For $t \in \mathbb{Z} \setminus \{0, \pm 3\}$ let

$$P_t(X) = X^4 - tX^3 - 6X^2 + tX + 1.$$

Let $\vartheta = \vartheta_t$ be a root of $P_t(X)$, then the infinite parametric family of number fields $K_t = K = Q(\vartheta_t)$ is called *simplest quartic fields*. P. Olajos [24] proved that K_t admits a power integral bases if and only if $t = 2$ and $t = 4$, moreover he found all generators of power integral bases in these fields. Using his result we are able to compute all CNS bases in such fields.

Theorem 5.2. *We have $\mathcal{F}_0(\mathbb{Q}(\vartheta)) = \emptyset$, $\mathcal{F}_1(\mathbb{Q}(\vartheta_2)) = \mathcal{G}_2$ and $\mathcal{F}_1(\mathbb{Q}(\vartheta_4)) = \mathcal{G}_4$ where*

$$\mathcal{G}_2 = \Big\{-\frac{1}{2}\vartheta^3 + \vartheta^2 + \frac{7}{2}\vartheta - 4, \frac{1}{2}\vartheta^3 - \vartheta^2 - \frac{7}{2}\vartheta - 2, 2\vartheta^3 - \frac{9}{2}\vartheta^2 - 11\vartheta - \frac{9}{2}, \\ -2\vartheta^3 + \frac{9}{2}\vartheta^2 + 11\vartheta - \frac{19}{2}, \frac{1}{2}\vartheta^3 - 2\vartheta - \frac{13}{2}, -\frac{1}{2}\vartheta^3 + 2\vartheta - \frac{5}{2}, \frac{1}{2}\vartheta^2 + \vartheta - \frac{23}{2}, \\ -\frac{1}{2}\vartheta^2 - \vartheta - \frac{5}{2}, \vartheta^3 - \frac{3}{2}\vartheta^2 - 7\vartheta - \frac{9}{2}, -\vartheta^3 + \frac{3}{2}\vartheta^2 + 7\vartheta - \frac{11}{2}, \\ \frac{3}{2}\vartheta^3 - 2\vartheta^2 - \frac{21}{2}\vartheta - 6, -\frac{3}{2}\vartheta^3 + 2\vartheta^2 + \frac{21}{2}\vartheta - 8, \frac{1}{2}\vartheta^3 - 2\vartheta^2 + \frac{1}{2}\vartheta - 1, \\ -\frac{1}{2}\vartheta^3 + 2\vartheta^2 - \frac{1}{2}\vartheta - 11, -\vartheta^3 + \frac{5}{2}\vartheta^2 + 5\vartheta - \frac{13}{2}, \vartheta^3 - \frac{5}{2}\vartheta^2 - 5\vartheta - \frac{5}{2}, \\ \frac{1}{2}\vartheta^2 - \vartheta - \frac{9}{2}, -\frac{1}{2}\vartheta^2 + \vartheta - \frac{3}{2}, \frac{1}{2}\vartheta^2 - \frac{15}{2}, -\frac{1}{2}\vartheta^2 - \frac{3}{2}\Big\}$$

$$\mathcal{G}_4 = \Big\{-\frac{1}{4}\vartheta^3 + \frac{3}{4}\vartheta^2 + \frac{11}{4}\vartheta - \frac{13}{4}, \frac{1}{4}\vartheta^3 - \frac{3}{4}\vartheta^2 - \frac{11}{4}\vartheta - \frac{11}{4}, \frac{1}{4}\vartheta^3 - \frac{3}{4}\vartheta^2 - \frac{7}{4}\vartheta - \frac{23}{4}, \\ -\frac{1}{4}\vartheta^3 + \frac{3}{4}\vartheta^2 + \frac{7}{4}\vartheta - \frac{13}{4}, -\frac{3}{4}\vartheta^3 + \frac{13}{4}\vartheta^2 + \frac{13}{4}\vartheta - \frac{27}{4}, \frac{3}{4}\vartheta^3 - \frac{13}{4}\vartheta^2 - \frac{13}{4}\vartheta - \frac{9}{4}, \\ \frac{3}{4}\vartheta^3 - \frac{11}{4}\vartheta^2 - \frac{21}{4}\vartheta - \frac{11}{4}, -\frac{3}{4}\vartheta^3 + \frac{11}{4}\vartheta^2 + \frac{21}{4}\vartheta - \frac{25}{4}, -\frac{1}{4}\vartheta^3 + \frac{5}{4}\vartheta^2 - \frac{1}{4}\vartheta - \frac{23}{4}, \\ \frac{1}{4}\vartheta^3 - \frac{5}{4}\vartheta^2 + \frac{1}{4}\vartheta - \frac{13}{4}, -\frac{1}{4}\vartheta^3 + \frac{5}{4}\vartheta^2 + \frac{3}{4}\vartheta - \frac{19}{4}, \frac{1}{4}\vartheta^3 - \frac{5}{4}\vartheta^2 - \frac{3}{4}\vartheta - \frac{5}{4}\Big\}.$$

Proof. Let γ be a generator of power integral basis in $\mathbb{Z}_K$. P. Olajos [24] showed that only the following cases can occur:

(1) $t = 2, \gamma = x \cdot \vartheta + y \cdot \frac{1+\vartheta^2}{2} + z \cdot \frac{\vartheta+\vartheta^3}{2}$ where

$$(x, y, z) = (4, 2, -1), (-13, -9, 4), (-2, 1, 0), (1, 1, 0), (-8, -3, 2), (-12, -4, 3), (0, -4, 1), (6, 5, -2), (-1, 1, 0), (0, 1, 0).$$

(2) $t = 4, \gamma = x \cdot \vartheta + y \cdot \frac{1+\vartheta^2}{2} + z \cdot \frac{1+\vartheta+\vartheta^2+\vartheta^3}{4}$ where

$$(x, y, z) = (3, 2, -1), (-2, -2, 1), (4, 8, -3), (-6, -7, 3), (0, 3, -1), (1, 3, -1).$$

From here on we proceed as in the proof of Theorem 5.3. The details of the computation are given in Table 3 below where we use the following notation: (x, y, z) denote the coordinates of γ as in the table above, the minimal polynomial $\mu_\gamma = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4$ of γ is given by (a_1, a_2, a_3, a_4).

(x, y, z)	γ	μ_γ	c_γ	k_γ	$c_{-\gamma}$	$k_{-\gamma}$
$(4, 2, -1)$	$-\frac{1}{2}\vartheta^3 + \vartheta^2 + \frac{7}{2}\vartheta + 1$	$(-8, 19, -12, 1)$	5	7	1	3
$(-13, -9, 4)$	$2\vartheta^3 - \frac{9}{2}\vartheta^2 - 11\vartheta - \frac{9}{2}$	$(36, 451, 2176, 2641)$	0	0	14	15
$(-2, 1, 0)$	$\frac{1}{2}\vartheta^3 - 2\vartheta + \frac{1}{2}$	$(-6, 1, 4, 1)$	7	8	2	4
$(1, 1, 0)$	$\frac{1}{2}\vartheta^2 + \vartheta + \frac{1}{2}$	$(-12, 19, -8, 1)$	12	12	2,	3
$(-8, -3, 2)$	$\vartheta^3 - \frac{3}{2}\vartheta^2 - 7\vartheta - \frac{3}{2}$	$(6, 1, -4, 1)$	2	4	7	8
$(-12, -4, 3)$	$\frac{3}{2}\vartheta^3 - 2\vartheta^2 - \frac{21}{2}\vartheta - 2$	$(4, -29, 44, -19)$	4	5	10	10
$(0, -4, 1)$	$\frac{1}{2}\vartheta^3 - 2\vartheta^2 + \frac{1}{2}\vartheta - 2$	$(20, 115, 260, 205)$	0	1	14	14
$(6, 5, -2)$	$-\vartheta^3 + \frac{5}{2}\vartheta^2 + 5\vartheta + \frac{5}{2}$	$(-22, 169, -508, 421)$	9	11	0	1
$(-1, 1, 0)$	$\frac{1}{2}\vartheta^2 - \vartheta + \frac{1}{2}$	$(-8, 19, -12, 1)$	5	7	1	3
$(0, 1, 0)$	$\frac{1}{2}\vartheta^2 + \frac{1}{2}$	$(-10, 25, -20, 5)$	8	9	1	3
$(3, 2, -1)$	$-\frac{1}{4}\vartheta^3 + \frac{3}{4}\vartheta^2 + \frac{11}{4}\vartheta + \frac{3}{4}$	$(-4, 2, 4, -1)$	4	6	2	4
$(-2, -2, 1)$	$\frac{1}{4}\vartheta^3 - \frac{3}{4}\vartheta^2 - \frac{7}{4}\vartheta - \frac{3}{4}$	$(0, -8, -8, -2)$	5	6	4	5
$(4, 8, -3)$	$-\frac{3}{4}\vartheta^3 + \frac{13}{4}\vartheta^2 + \frac{13}{4}\vartheta + \frac{13}{4}$	$(-24, 208, -760, 958)$	10	11	-1	0
$(-6, -7, 3)$	$\frac{3}{4}\vartheta^3 - \frac{11}{4}\vartheta^2 - \frac{21}{4}\vartheta - \frac{11}{4}$	$(16, 88, 200, 158)$	0	1	9	10
$(0, 3, -1)$	$-\frac{1}{4}\vartheta^3 + \frac{5}{4}\vartheta^2 - \frac{1}{4}\vartheta + \frac{5}{4}$	$(-8, 16, -8, -2)$	7	8	2	3
$(1, 3, -1)$	$-\frac{1}{4}\vartheta^3 + \frac{5}{4}\vartheta^2 + \frac{3}{4}\vartheta + \frac{5}{4}$	$(-12, 50, -84, 47)$	6	8	0	2

Table 3

□

Power integral bases in the polynomial order $\mathbb{Z}[\alpha]$ of K_t were described by G. Lettl and A. Pethő [22].

Theorem 5.3. *Let $t \in \mathbb{N} \setminus \{0, 3\}$ and ϑ denote a root of the polynomial*

$$X^4 - tX^3 - 6X^2 + tX + 1.$$

Then we have $\mathcal{F}_0(\mathbb{Q}(\vartheta)) = \emptyset$ *and* $\mathcal{F}_1(\mathbb{Q}(\vartheta)) = \mathcal{G} \cup \mathcal{G}_1 \cup \mathcal{G}_2 \cup \mathcal{G}_4$ *where*

$$\mathcal{G} = \begin{cases} \{-3-\vartheta, -t-2+\vartheta, -2-6\vartheta-t\vartheta^2+\vartheta^3, -t-3+6\vartheta+t\vartheta^2-\vartheta^3\}, \\ \textit{if } t \geq 5, \\ \emptyset \ \textit{otherwise}, \end{cases}$$

$$\mathcal{G}_1 = \begin{cases} \{-4+\vartheta, -4-\vartheta, -5+6\vartheta+\vartheta^2-\vartheta^3, -3-6\vartheta-\vartheta^2+\vartheta^3, \\ -23+3\vartheta^2-\vartheta^3, -1-3\vartheta^2+\vartheta^3, -14+25\vartheta+2\vartheta^2-4\vartheta^3, \\ -10-25\vartheta-2\vartheta^2+4\vartheta^3\}, \ \textit{if } t = 1, \\ \emptyset \ \textit{otherwise}, \end{cases}$$

$$\mathcal{G}_2 = \begin{cases} \{-5+\vartheta, -3-\vartheta, -5+6\vartheta+2\vartheta^2-\vartheta^3, -3-6\vartheta-2\vartheta^2+\vartheta^3\}, \\ \textit{if } t = 2, \\ \emptyset \ \textit{otherwise}, \end{cases}$$

$$\mathcal{G}_4 = \begin{cases} \{-6+\vartheta, -3-\vartheta, 1+9\vartheta-22\vartheta^2+4\vartheta^3, -78-9\vartheta+22\vartheta^2-4\vartheta^3, \\ -7+6\vartheta+4\vartheta^2-\vartheta^3, -3-6\vartheta-4\vartheta^2+\vartheta^3, -62+74\vartheta+30\vartheta^2-9\vartheta^3, \\ -15-74\vartheta-30\vartheta^2+9\vartheta^3\}, \ \textit{if } t = 4, \\ \emptyset \ \textit{otherwise}. \end{cases}$$

Before embarking on the proof of Theorem 5.3 we need some preparation. For checking the CNS property of some polynomials we exploit a technical lemma.

Lemma 5.1. *The polynomial* $X^4 + p_3X^3 + p_2X^2 + p_1X + p_0 \in \mathbb{Z}[X]$ *with the properties*

(i) $p_0 \geq 4$
(ii) $p_1 \geq p_0 + 1$
(iii) $p_3 \geq 2$
(iv) $p_1 \geq 2p_2 + 1$
(v) $2p_1 - p_2 + 2p_3 \leq 2p_0 - 1$

is a CNS polynomial.

Proof. Let

$$E = \{(e_1, \ldots, e_4) \in \mathbb{Z}^4 \,|\, |e_i| \leq 2 \quad (i = 1, \ldots, 4), \quad (e_2, e_1) \neq (0, \pm 2),$$

$$e_i e_{i+1} \leq 0 \quad (i = 1, 2, 3), \quad |e_i| = 2 \implies e_{i-1} \neq 0 \quad (i = 2, 3, 4)\}$$

and $\tau_P(\underline{A})$ be the mapping defined in Section 2. Clearly, property (i) of Theorem 2.1 is satisfied. We show(ii) and (iii) of the same Theorem in

several steps thereby using the notation of ([26], Lemma 1): $a \overset{(S)}{\longrightarrow}$ indicates that $\tau_P(\underline{A})$ falls into step(s) S considered before.

(1) $e_4 \geq 0, \tau_P(0,0,0,e_4) = 0$
(2) $e_4 \leq 0, (0,0,1,e_4) \overset{(1)}{\longrightarrow}$
(3) $(0,1,-1,e_4) \overset{(2)}{\longrightarrow}$
(4) $e_3 \in \{0,1\}, (1,-1,e_3,e_4) \overset{(3)}{\longrightarrow}$
(5) $(-1,1,-1,e_4) \overset{(4)}{\longrightarrow}$
(6) $(1,-1,2,e_4) \overset{(3,5)}{\longrightarrow}$
(7) $(-1,1,0,e_4) \overset{(4)}{\longrightarrow}$
(8) $e_3 \in \{0,1\}, (1,0,e_3,e_4) \overset{(7)}{\longrightarrow}$
(9) $(0,0,e_3,e_4) \overset{(1,8)}{\longrightarrow}$
(10) $(0,1,0,e_4) \overset{(9)}{\longrightarrow}$
(11) $(1,0,-1,e_4) \overset{(7,10)}{\longrightarrow}$
(12) $(0,-1,2,e_4) \overset{(11)}{\longrightarrow}$
(13) $(-1,2,-1,e_4) \overset{(6,12)}{\longrightarrow}$
(14) $(2,-1,1,e_4) \overset{(13)}{\longrightarrow}$
(15) $(-1,1,e_3,e_4) \overset{(4,5,7,14)}{\longrightarrow}$
(16) $e_4 \leq -1, (-1,2,e_3,e_4) \overset{(6,12)}{\longrightarrow}$
(17) $(2,-1,0,e_4) \overset{(16)}{\longrightarrow}$
(18) $(-1,0,1,e_4) \overset{(4,17)}{\longrightarrow}$
(19) $(0,1,e_3,e_4) \overset{(9)}{\longrightarrow}$
(20) $(0,-1,e_3,e_4) \overset{(11)}{\longrightarrow}$
(21) $(0,e_2,e_3,e_4) \overset{(9,19,20)}{\longrightarrow}$
(22) $e_1 \geq 1, (e_1,e_2,e_3,e_4) \overset{(13,15,21)}{\longrightarrow}$
(23) $(1,-1,2,e_4) \overset{(21)}{\longrightarrow}$
(24) $(-1,e_2,e_3,e_4) \overset{(4,6,17)}{\longrightarrow}$
(25) $(e_1,e_2,e_3,e_4) \overset{(21,22,24)}{\longrightarrow}$

This concludes the proof. □

We are now in a position to verify Theorem 5.3.

Proof of Theorem 5.3. By [9] up to equivalence all generators of power integral bases of $\mathbb{Z}[\vartheta]$ are the following:

- for $t \in \mathbb{N} \setminus \{0,3\}$: $\vartheta, 6\vartheta + t\vartheta^2 - \vartheta^3$,

- for $t = 1$ additionally: $3\vartheta^2 - \vartheta^3, 25\vartheta + 2\vartheta^2 - 4\vartheta^3$,
- for $t = 4$ additionally: $9\vartheta - 22\vartheta^2 + 4\vartheta^3, -74\vartheta - 30\vartheta^2 + 9\vartheta^3$.

We proceed analogously as in the proof of Theorem 3.3 by using Proposition 2.1 and Table 4 below with the following notation: β is a generator of a power integral basis of $\mathbb{Q}(\vartheta)$. The minimal polynomial $\mu_\beta = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4$ of β is listed in the form (a_1, a_2, a_3, a_4). Lower bounds for the constants c_β, k_β are given by Proposition 2.1. For their determination ([3], Theorem 3.1) and Corollary 5.1 are used in a straightforward way. Similarly as in the proof of Theorem 3.3 Remark 2 is used. □

β	t	μ_β	$m(\beta)$	$M(\beta)$	c_β	k_β	$c_{-\beta}$	$k_{-\beta}$
ϑ	$\neq 1, 2$	$(-t, -6, t, 1)$	-2	t	$t+2$	$t+2$	3	4
ϑ	1	$(-1, -6, 1, 1)$	-3	2	4	6	4	5
ϑ	2	$(-2, -6, 2, 1)$	-2	3	5	6	3	5
$6\vartheta + t\vartheta^2 - \vartheta^3$	$\neq 1$, 2, 4	$(-3t, 3t^2 - 6, -t^3 + 11t, -5t^2 + 1)$	-1	$t+1$	$t+3$	$t+4$	2	2
$6\vartheta + \vartheta^2 - \vartheta^3$	1	$(-1, -6, 1, 1)$	-3	2	4	6	4	5
$6\vartheta + 2\vartheta^2 - \vartheta^3$	2	$(-6, -6, 14, -19)$	-2	3	5	7	3	4
$6\vartheta + 4\vartheta^2 - \vartheta^3$	4	$(-12, 42, -20, -79)$	-2	5	7	8	3	3
$3\vartheta^2 - \vartheta^3$	1	$(-23, 39, -22, 4)$	0	21	23	23	1	3
$25\vartheta + 2\vartheta^2 - 4\vartheta^3$	1	$(13, -96, -1993, -7241)$	-9	12	14	14	10	12
$9\vartheta - 22\vartheta^2 + 4\vartheta^3$	4	$(84, 618, 1580, 1361)$	-77	-3	-1	1	78	78
$-74\vartheta - 30\vartheta^2 + 9\vartheta^3$	4	$(20, -1878, 29932, -144239)$	-61	13	15	17	62	62

TABLE 4

Finally we consider another family of orders in a parametrized family of quartic number fields, where all power integral bases are known. Let $t \in \mathbb{Z}$, $t \geq 0$, and $P(X) = X^4 - tX^3 - X^2 + tX + 1$. Denote by α one of the zeros of $P(X)$. In the following we deal with the order $\mathcal{O} = Z[\alpha]$ of $Q(\alpha)$.

M. Mignotte, A. Pethő and R. Roth [23] gave the following result:

Theorem 5.4. (M. MIGNOTTE, A. PETHŐ, R. ROTH) *Let $t \geq 4$. Then every element $\gamma \in \mathcal{O}$ such that $Z[\gamma] = \mathcal{O}$ is equivalent to some element $\gamma = x\alpha + y\alpha^2 + z\alpha^3$ with*

$$(x, y, z) \in \{(1, 0, 0), (1, t, -1), (t, t-1, -1), (t, -t-1, 1), (1, 0, -1), (1, -t(t^2+1), t^2)\}$$

except when $t = 4$*, in which case additionally* $(x, y, z) \in \{(209, 140, -49), (209, -312, 64)\}$. [1]

Theorem 5.5. *Let* $t \geq 4$*. We have* $\mathcal{F}_0(\mathbb{Q}(\alpha)) = \emptyset$ *and* $\mathcal{F}_1(\mathbb{Q}(\alpha)) = \mathcal{G}_4 \cup \mathcal{G}_t$ *where*

$$\mathcal{G}_4 = \left\{209\alpha + 140\alpha^2 - 49\alpha^3 + 350, 209\alpha - 312\alpha^2 + 64\alpha^3 - 71\right\}$$
$$\mathcal{G}_t = \left\{\alpha + t + 1, \alpha + t\alpha^2 - \alpha^3 + t + 2, t\alpha + (t-1)\alpha^2 - \alpha^3 + 8,\right.$$
$$\left. t\alpha - (t+1)\alpha^2 + \alpha^3 + 2, \alpha - \alpha^3 + 2, \alpha - t(t^2+1)\alpha^2 + t^2\alpha^3 - t + 1\right\}.$$

Proof. We follow the same line as in the proof of Theorem 5.3. First we compute the data necessary to apply Algorithm 2.1. For the zeroes of the polynomial $P(X)$ we use the following estimates:

$$\alpha_1 = t - 1/t^3 - 1/t^5 - 4/t^7 - 9/t^9, \quad \alpha_2 = -1/t - 1/t^5 - 1/t^7 - 5/t^9,$$
$$\alpha_3 = 1 + 1/2t + 1/8t^2 + 1/2t^3, \qquad \alpha_4 = -1 + 1/2t - 1/8t^2.$$

In a straightforward way we obtain $M(\gamma)$ for any possible value of γ. Knowing $M(\gamma)$ it is easy to establish k_γ. Because of the special form of $P(X)$ we do not need $k_{-\gamma}$. Indeed denote by σ the automorphism of $\mathbb{Q}(\alpha)$, which maps α to $-\frac{1}{\alpha}$. Then an easy computation shows that

$$\sigma(-\alpha) = \alpha + t\alpha^2 - \alpha^3 - t$$
$$\sigma(-(t\alpha + (t-1)\alpha^2 - \alpha^3)) = t\alpha - (t-1)\alpha^2 + \alpha^3 + 1$$
$$\sigma(-(\alpha - \alpha^3)) = \alpha - t(t^2+1)\alpha^2 + t^2\alpha^3 + t^3$$

and if $t = 4$ then

$$\sigma(-(209\alpha + 140\alpha^2 - 49\alpha^3)) = 209\alpha - 312\alpha^2 + 64\alpha^3 + 116.$$

The details of the computation are given in Table 5 below where we use the following notation: (x, y, z) denote the coordinates of $\gamma = x\alpha + y\alpha^2 + z\alpha^3$ as in Theorem 5.4, the minimal polynomial $\mu_\gamma = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4$ of γ is given by (a_1, a_2, a_3, a_4).

By the intention of the journal we had to omit further details of the proof, because it is quite complicated and long especially in the case $\gamma = \alpha + t\alpha^2 - \alpha^3$. The interested reader may find the complete version electronically under the URL:
http://www.inf.unideb.hu/~pethoe/Publications.html. □

[1] In Theorem 4 of [23] the last vector reads $(209, -352, 64)$, but its correct value is $(209, -312, 64)$.

γ	μ_γ	$m(\gamma)$	$M(\gamma)$	c_γ	k_γ
α	$(-t,-1,t,1)$	-1	$t-1$	$t+1$	$t+3$, if $t=4$ $t+2$, if $t>4$
$\alpha+t\alpha^2-\alpha^3$	$(-3t,3t^2-1,t-t^3,1)$	0	t	$t+2$	$t+4$
$t\alpha+(t-1)\alpha^2$ $-\alpha^3$	$(2-2t,-3t+5,$ $-t+4,1)$	-1	6 $2t-1$	8 $2t+1$	8, if $t=4$ $2t+1$, if $t>4$
$t\alpha-(t+1)\alpha^2$ $+\alpha^3$	$(2t+2,3t+5,t+4,1)$	$-2t-1$	-2	2	3
$\alpha-\alpha^3$	$(t^3-t,3t^2-1,3t,1)$	$-t^3+t$	-1	2	3
α $-t(t^2+1)\alpha^2$ $+t^2\alpha^3$	$(3t^3+t,$ $3t^6+3t^4+3t^2-1,$ $t^9+3t^7+6t^5-2t^3-3t,$ $t^{10}+3t^8-t^6-3t^4+1)$	$-t^3-1$	$-t-1$	$-t+1$	$-t+1$
$209\alpha+140\alpha^2$ $-49\alpha^3$	$(-4,2,4,-1)$	-43	348	350	350
$209\alpha-312\alpha^2$ $+64\alpha^3$	$(0,-8,-8,-2)$	-465	-74	-71	-70

TABLE 5

References

[1] S. AKIYAMA, T. BORBÉLY, H. BRUNOTTE, A. PETHŐ and J. M. THUSWALDNER, *On a generalization of the radix representation – a survey*, in "High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams", Fields Institute Communcations, vol. **41** (2004), 19–27.

[2] S. AKIYAMA, T. BORBÉLY, H. BRUNOTTE, A. PETHŐ and J. M. THUSWALDNER, *Generalized radix representations and dynamical systems I*, Acta Math. Hung., **108** (2005), 207–238.

[3] S. AKIYAMA, H. BRUNOTTE and A. PETHŐ, *Cubic CNS polynomials, notes on a conjecture of W.J. Gilbert*, J. Math. Anal. and Appl., **281** (2003), 402–415.

[4] S. AKIYAMA and H. RAO, *New criteria for canonical number systems*, Acta Arith., **111** (2004), 5–25.

[5] S. AKIYAMA and J. M. THUSWALDNER, *On the topological structure of fractal tilings generated by quadratic number systems*, Comput. Math. Appl. **49** (2005), no. 9-10, 1439–1485.

[6] T. BORBÉLY, *Általánosított számrendszerek*, Master Thesis, University of Debrecen, 2003.

[7] H. BRUNOTTE, *On trinomial bases of radix representations of algebraic integers*, Acta Sci. Math. (Szeged), **67** (2001), 521–527.

[8] H. BRUNOTTE, *On cubic CNS polynomials with three real roots*, Acta Sci. Math. (Szeged), **70** (2004), 495 – 504.

[9] I. GAÁL, *Diophantine equations and power integral bases*, Birkhäuser (Berlin), (2002).

[10] W. J. GILBERT, *Radix representations of quadratic fields*, J. Math. Anal. Appl., **83** (1981), 264–274.

[11] E. H. GROSSMAN, *Number bases in quadratic fields*, Studia Sci. Math. Hungar., **20** (1985), 55–58.

[12] V. GRÜNWALD, *Intorno all'aritmetica dei sistemi numerici a base negativa con particolare riguardo al sistema numerico a base negativo-decimale per lo studio delle sue analogie coll'aritmetica ordinaria (decimale)*, Giornale di matematiche di Battaglini, **23** (1885), 203–221, 367.

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

[14] I. Kátai and B. Kovács, *Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen*, Acta Sci. Math. (Szeged), **42** (1980), 99–107.
[15] I. Kátai and B. Kovács, *Canonical number systems in imaginary quadratic fields*, Acta Math. Acad. Sci. Hungar., **37** (1981), 159–164.
[16] I. Kátai and J. Szabó, *Canonical number systems for complex integers*, Acta Sci. Math. (Szeged), **37** (1975), 255–260.
[17] D. E. Knuth, *An imaginary number system*, Comm. ACM, **3** (1960), 245 – 247.
[18] D. E. Knuth, *The Art of Computer Programming, Vol. 2 Semi-numerical Algorithms*, Addison Wesley (1998), London 3rd edition.
[19] B. Kovács, *Canonical number systems in algebraic number fields*, Acta Math. Acad. Sci. Hungar., **37** (1981), 405–407.
[20] B. Kovács and A. Pethő, *Number systems in integral domains, especially in orders of algebraic number fields,* Acta Sci. Math. (Szeged), **55** (1991), 287–299.
[21] S. Körmendi, *Canonical number systems in* $\mathbb{Q}(\sqrt[3]{2})$*,* Acta Sci. Math. (Szeged), **50** (1986), 351–357.
[22] G. Lettl and A. Pethő, *Complete solution of a family of quartic Thue equations*, Abh. Math. Sem. Univ. Hamburg **65** (1995), 365–383.
[23] M. Mignotte, A. Pethő and R. Roth, *Complete solutions of quartic Thue and index form equations,* Math. Comp. **65** (1996), 341–354.
[24] P. Olajos, *Power integral bases in the family of simplest quartic fields*, Experiment. Math. **14** (2005), 129–132.
[25] A. Pethő, *On a polynomial transformation and its application to the construction of a public key cryptosystem, Computational Number Theory*, Proc., Walter de Gruyter Publ. Comp. Eds.: A. Pethő, M. Pohst, H. G. Zimmer and H. C. Williams (1991), 31–43.
[26] A. Pethő, *Notes on CNS polynomials and integral interpolation*, More sets, graphs and numbers, 301–315, Bolyai Soc. Math. Stud., 15, Springer, Berlin, 2006.
[27] A. Pethő, *Connections between power integral bases and radix representations in algebraic number fields*, Proc. of the 2003 Nagoya Conf. "Yokoi-Chowla Conjecture and Related Problems", Furukawa Total Pr. Co. (2004), 115–125.
[28] R. Robertson, *Power bases for cyclotomic integer rings*, J. Number Theory, **69** (1998), 98–118.
[29] R. Robertson, *Power bases for 2-power cyclotomic integer rings*, J. Number Theory, **88** (2001), 196–209.
[30] K. Scheicher, *Kanonische Ziffernsysteme und Automaten,* Grazer Math. Ber., **333** (1997), 1–17.
[31] D. Shanks, *The simplest cubic fields,* Math. Comp., **28** (1974), 1137–1152.
[32] J. M. Thuswaldner, *Elementary properties of canonical number systems in quadratic fields*, in: Applications of Fibonacci Numbers, Volume 7, G. E. Bergum et al. (eds.), Kluwer Academic Publishers, Dordrecht (1998), 405–414.

Horst Brunotte
Université Gauss
Haus-Endt-Straße 88
D-40593 Düsseldorf, Germany
E-mail : brunoth@web.de

Andrea Huszti
Faculty of Informatics
University of Debrecen
P.O. Box 12, H-4010 Debrecen, Hungary
Hungarian Academy of Sciences and University of Debrecen
E-mail : husztia@inf.unideb.hu

Attila Pethő
Faculty of Informatics
University of Debrecen
P.O. Box 12, H-4010 Debrecen, Hungary
Hungarian Academy of Sciences and University of Debrecen
E-mail : pethoe@inf.unideb.hu
URL: http://www.inf.unideb.hu/~pethoe/