Acta Sci. Math., 55 (1991), 287—299

Number systems in integral domains, especially in orders of algebraic number fields

B. KOVÁCS[1]) and A. PETHŐ[2])

1. Introduction

Let $\mathbf{R}$ be an integral domain, $\alpha\in\mathbf{R}$, $\mathcal{N}=\{n_1, n_2, \ldots, n_m\}\subset\mathbf{Z}$, where $\mathbf{Z}$ denotes the ring of integers. $\{\alpha, \mathcal{N}\}$ is called a number system in $\mathbf{R}$ if any $\gamma\in\mathbf{R}$ has a unique representation

$$(1.1)\quad \gamma = c_0+c_1\alpha+\ldots+c_h\alpha^h;\; c_j\in\mathcal{N}\;\; (i = 0, 1, \ldots, h),\; c_h \neq 0, \;\text{ if }\; h \neq 0.$$

If $\mathcal{N}=\mathcal{N}_0=\{0, 1, \ldots, m\}$ for some $m\geqq 1$, then $\{\alpha, \mathcal{N}\}$ is called canonical number system. In the sequel α will be called the base and $\mathcal{N}$ the set of digits of the number system.

If the characteristic of $\mathbf{R}$ is p, then we may identify any $n\in\mathbf{Z}$ with $n_1\in\mathbf{R}$, where $0\leqq n_1<p$ and 1 is the identity element of $\mathbf{R}$. Hence, in this case we may assume without loss of generality that $\mathcal{N}\subseteqq\{0, \ldots, p-1\}$.

This concept is a natural generalization of negative base number systems in $\mathbf{Z}$ considered by several authors. For an extensive literature we refer to KNUTH [10, 4.1]. The canonical number systems in the ring of integers of quadratic number fields were completely described by KÁTAI and SZABÓ [7], KÁTAI and KOVÁCS [5], [6].

Kovács [8] gave a necessary and sufficient condition for the existence of canonical number systems in $\mathbf{R}$. In [9] we proved that for any $q\in\mathbf{Z}$, $q<-1$ there exist infinitely many $\mathcal{N}\subset\mathbf{Z}$ such that $\{q, \mathcal{N}\}$ is a number system.

In this paper we first characterize all those integral domains which have number systems. If the characteristic of $\mathbf{R}$ is a prime, then we are able to establish all number systems in $\mathbf{R}$. This problem is more difficult if the characteristic of $\mathbf{R}$ is 0.

[1]) Research supported in part by Grant 273 and 400 from the Hungarian National Foundation for Scientific Research.

[2]) Research supported in part by Hungarian National Foundation for Scientific Research Grant 273/86.

Received May 5, 1989 and in revised form February 21, 1990.

It is considered for orders $\mathcal{O}$ of algebraic number fields. In Theorem 3 and 4 we give necessary and sufficient conditions for $\{\alpha, \mathcal{N}\}$ to be a number system in $\mathcal{O}$. Theorem 5 effectively characterizes the bases of all canonical number systems of $\mathcal{O}$. This solves a problem of GILBERT [3]. Combining results of GAÁL and SHULTE [2]. and the enumeration technique of FINCKE and POHST [1] with our Theorems we computed the representatives of all but one classes of basis of canonical number systems in rings of integers of totally real cubic fields with discriminant $\leqq 564$.

2. Results

In the sequel $\mathbf{R}$ will denote an integral domain, $\mathbf{Z}$ the ring of integers, $\mathbf{Q}$ the field of rational numbers, $\mathbf{K}$ an algebraic number field of degree n, with ring of integers $\mathbf{Z}_K$. If α is algebraic over $\mathbf{Q}$, $\mathbf{Z}[\alpha]$ denotes the smallest ring of $\mathbf{Q}(\alpha)$ containing $\mathbf{Z}$ and α. Finally $\mathbf{F}_p$ denotes the finite field with p elements, where p is a prime. With this notations we have

Theorem 1. *There exists a number system in* $\mathbf{R}$ *if and only if*

(i) $\mathbf{R}=\mathbf{Z}[\alpha]$ *for an* α, *algebraic over* $\mathbf{Q}$, *if* $\operatorname{char}\mathbf{R}=0$,

(ii) $\mathbf{R}=\mathbf{F}_p[x]$, *where* x *is transcendental over* $\mathbf{F}_p$, *if* $\operatorname{char}\mathbf{R}=p$, *$p$ is a prime.*

This theorem generalizes a result of KOVÁCS [8], where integral domains with canonical number systems were characterized.

If $\operatorname{char}\mathbf{R}=p$, then $\mathbf{R}=\mathbf{F}_p[x]$ and we can describe all number systems.

Theorem 2. $\{\alpha, \mathcal{N}\}$ *is a number system in* $\mathbf{F}_p[x]$ *if and only if* $\alpha=a_0+a_1x$, *where* $a_0, a_1\in\mathbf{F}_p, a_1\neq 0$ *and* $\mathcal{N}=\mathcal{N}_0=\{0, 1, \dots, p-1\}$.

From now on we are dealing with integral domains $\mathbf{R}$ with $\operatorname{char}\mathbf{R}=0$. If $\mathbf{R}$ has a number system, then there exists an $\alpha\in\mathbf{R}$, algebraic over $\mathbf{Q}$, such that $\mathbf{R}=\mathbf{Z}[\alpha]$. Let $\mathbf{K}=\mathbf{Q}(\alpha)$ be of degree n, and denote by $\gamma=\gamma^{(1)}, \dots, \gamma^{(n)}$ the conjugates of a $\gamma\in\mathbf{K}$. If $\{\beta, \mathcal{N}\}$ is a number system in $\mathbf{Z}[\alpha]$, then $\mathbf{Q}(\alpha)=\mathbf{Q}(\beta)$, hence the discriminant of β, $\mathbf{D}(\beta)\neq 0$. In the following two theorems we give necessary and sufficient conditions for $\{\beta, \mathcal{N}\}$ to be a number system in $\mathbf{Z}[\alpha]$, where α is an algebraic integer over $\mathbf{Q}$.

Theorem 3. *Let* α *be an algebraic integer over* $\mathbf{Q}$. *Let* $\beta\in\mathbf{Z}[\alpha]$, $\mathcal{N}\subset\mathbf{Z}$ *and put* $A=\max_{a\in\mathcal{N}}|a|$. $\{\beta, \mathcal{N}\}$ *is a number system in* $\mathbf{Z}[\alpha]$ *if and only if*

(i) $|\beta^{(j)}|>1$ *for* $j=1, 2, \dots, n$,

(ii) $\mathcal{N}$ *is a complete residue system* $\bmod |N_{\mathbf{K}/\mathbf{Q}}(\beta)|$ *containing* 0,

(iii) $\alpha\in\mathbf{Z}[\beta]$,

(iv) *all* $\gamma\in\mathbf{Z}[\alpha]$ *with*

$$|\gamma^{(j)}| \leqq \frac{A}{|\beta^{(j)}|-1}, \quad (j=1, \dots, n) \tag{2.1}$$

have a representation (1.1) *in* $\{\beta, \mathcal{N}\}$.

This theorem is well applicable in practice, because there exist only finitely many $\gamma\in\mathbf{Z}[\alpha]$ with (2.1). The disadvantage of condition (iv) is that it is not clear, if the representability of $\gamma\in\mathbf{Z}[\alpha]$ can be decided in finitely many steps. Therefore we give another characterization.

Theorem 4. *Let the notation be the same as in Theorem* 3. $\{\beta, \mathcal{N}\}$ *is a number system in* $\mathbf{Z}[\alpha]$ *if and only if* (i), (ii), (iii) *and*

$$\frac{\sum_{i=0}^{k-1} a_i\beta^i}{(\beta^k-1)} \notin \mathbf{Z}[\beta] \tag{v}$$

hold for any $a_i\in\mathcal{N}$, $(i=0, \dots, k-1)$, $a_j\neq 0$ *for at least one* $0\leqq j\leqq k-1$ *and*

$$0<k\leqq c=\left(\frac{2^{t+1}(A+1)}{D(\beta)^{1/2}}\sqrt{\sum_{j=1}^{n}\left(\frac{1}{|\beta^{(j)}|-1}\right)^2}\,(n|\beta|^n)^{(n-1)/2}\right)^n \max_{1\leqq j\leqq n}\frac{\log(A+1)}{\log(|\beta^{(j)}|)},$$

where t *denotes the number of non-real conjugates of* $\mathbf{K}$, *and*

$$|\beta| = \max_{1\leqq j\leqq n}|\beta^{(j)}|.$$

For an algebraic integer α let $\mathcal{N}_0(\alpha)=\{0, 1, \dots, |N_{\mathbf{K}/\mathbf{Q}}(\alpha)|-1\}$.

Theorem 5. *Let* $\mathcal{O}$ *be an order in the algebraic number field* $\mathbf{K}$. *There exist* $\alpha_1, \dots, \alpha_t\in\mathcal{O}$; $n_1, \dots, n_t\in\mathbf{Z}$, $N_1, \dots, N_t$ *finite subsets of* $\mathbf{Z}$, *which are all effectively computable, such that* $\{\alpha, \mathcal{N}_0(\alpha)\}$ *is a canonical number system in* $\mathcal{O}$, *if and only if* $\alpha=\alpha_i-h$ *for some integers* i, h *with* $1\leqq i\leqq t$ *and either* $h\geqq n_i$ *or* $h\in N_i$.

3. Number systems in integral domains

To prove Theorem 1 we need two Lemmas.

Lemma 1. *If* $\{\alpha, \mathcal{N}\}$ *is a number system in the integral domain* $\mathbf{R}$, *then* $0\in\mathcal{N}$.

Proof. Assume that $0\notin\mathcal{N}$. Then there exist $b_i\in\mathcal{N}$, $(i=0, \dots, k)$, such that

$$0 = b_0+b_1\alpha+\dots+b_k\alpha^k, \quad b_k\neq 0. \tag{3.1}$$

Let $0\neq\gamma\in\mathbf{R}$, then there exist $c_i\in\mathcal{N}$, $(i=0, \dots, h)$ with

$$\gamma = c_0+c_1\alpha+\dots+c_h\alpha^h, \quad c_h\neq 0. \tag{3.2}$$

From (3.1) and (3.2) it follows easily that $0\neq\gamma\alpha^{k+1}\in\mathbf{R}$ has at least two different representations. Thus Lemma 1 is proved.

Lemma 2. *Let* $\{\alpha, \mathcal{N}\}$ *be a number system in* $\mathbf{R}$ *with* $\operatorname{char}\mathbf{R}=p$. *Then* $\mathcal{N}=\mathcal{N}_0(p)=\{0, 1, \dots, p-1\}$.

Proof. We may assume by $\operatorname{char}\mathbf{R}=p$, that $0\leqq a<p$ holds for all $a\in\mathcal{N}$. Obviously $0\in\mathcal{N}$ by Lemma 1. Assume now that there exists an $0<a<p$ with $a\notin\mathcal{N}$. Then there exist $c_i\in\mathcal{N}$, $i=0, \dots, k$, $c_k\neq 0$ with

$$a = c_0+c_1\alpha+\dots+c_k\alpha^k. \tag{3.3}$$

This implies that α is algebraic over $\mathbf{F}_p$. Hence $\mathbf{R}\subset\mathbf{F}_p[\alpha]$ is finite. But the number of different representations (1.1) in $\{\alpha, \mathcal{N}\}$ is infinite. Hence there exists $\gamma\in\mathbf{R}$ with infinitely many different representations. This contradiction proves Lemma 2.

Proof of Theorem 1. First let $\operatorname{char}\mathbf{R}=0$. Assume that there exists a number system $\{\alpha, \mathcal{N}\}$ in $\mathbf{R}$. Let $N=\max\limits_{a\in\mathcal{N}}|a|+1$. Then $N\geqq 1$, because $\mathbf{R}\neq\{0\}$. Since $N\in\mathbf{R}$, there exist $k\geqq 0$, $c_i\in\mathcal{N}$, $i=0, \dots, k$ with $N=c_0+c_1\alpha+\dots+c_k\alpha^k$. We have $k>0$ because $(N-c_0)\neq 0$. Therefore α is algebraic over $\mathbf{Q}$. All $\gamma\in\mathbf{R}$ have representations (1.1), whence $\mathbf{R}=\mathbf{Z}[\alpha]$.

On the other hand, by [8, Theorem 1] there exists a canonical number system in $\mathbf{Z}[\alpha]$, which proves the first assertion of Theorem 1.

Let now $\operatorname{char}\mathbf{R}=p$, where p is a prime, and let $\{\alpha, \mathcal{N}\}$ be a number system in $\mathbf{R}$. Then by Lemma 2, $\mathcal{N}=\mathcal{N}_0$, i.e. $\{\alpha, \mathcal{N}\}$ is a canonical number system in $\mathbf{R}$. This implies by [8, Theorem 2] that $\mathbf{R}=\mathbf{F}_p[x]$. On the other hand there exists a number system in this ring.

Proof of Theorem 2. Let $\{\alpha, \mathcal{N}\}$ be a number system in $\mathbf{F}_p[x]$. Then by Lemma 2, $\mathcal{N}=\{0, 1, \dots, p-1\}$. Let $\alpha=P(x)\in\mathbf{F}_p[x]$, then the degree of P in x is at least 1. On the other hand there exist $k\geqq 1$, $a_i\in\mathcal{N}$, $0\leqq i\leqq k$, $a_k\neq 0$ with $x=a_0+$ $+a_1(P(x))+\dots+a_k(P(x))^k$. This implies that $P(x)|(x-a_0)$, hence $\deg P(x)\leqq 1$. Combining the inequalities for $\deg P(x)$ we conclude $\alpha=a_0+a_1x$ with $a_1\neq 0$. Thus the condition is necessary.

Let now $\alpha=a_0+a_1x$, $a_1\neq 0$. From $x=a_1^{-1}(\alpha-a_0)$ it follows that all elements of $\mathbf{F}_p[x]$ is representable in $\{\alpha, \mathcal{N}\}$. Theorem 2 is proved.

4. Number systems in $\mathbf{Z}[\alpha]$

The main purpose of this section is to prove Theorems 3, and 4. We shall use the notation introduced in Section 2.

Lemma 3. *Let α be algebraic over $\mathbf{Q}$, of degree n. If $\{\beta, \mathcal{N}\}$ is a number system in $\mathbf{Z}[\alpha]$, then $|\beta^{(j)}| \geqq 1$ for all $j=1, \ldots, n$.*

Proof. Assume that there exists a j, $1 \leqq j \leqq n$ with $|\beta^{(j)}|<1$. Suppose that $\gamma \in \mathbf{Z}[\alpha]$ has the representation $\gamma = a_0 + a_1\beta + \ldots + a_h\beta^h$ in $\{\beta, \mathcal{N}\}$. Then

$$|\gamma^{(j)}| < A \frac{1}{1-|\beta^{(j)}|},$$

where $A = \max_{a \in \mathcal{N}} |a|$. But this is impossible because $\mathbf{Z}[\alpha^{(j)}]$ has elements with absolute value larger than $\dfrac{A}{1-|\beta^{(j)}|}$. Lemma 3 is proved.

From now on α will denote an algebraic integer of degree n over $\mathbf{Q}$. Let $\mathbf{K}=\mathbf{Q}(\alpha)$ and denote $\mathbf{Z}_{\mathbf{K}}$ its ring of integers.

Lemma 4. *Let $\beta \in \mathbf{Z}_{\mathbf{K}}$ be of degree n, such that $|\beta^{(j)}|>1$, $j=1, \ldots, n$; and $\mathcal{N} \subset \mathbf{Z}$ a complete residue system $\bmod |N_{\mathbf{K}/\mathbf{Q}}(\beta)|$. Put $A = \max_{a \in \mathcal{N}} |a|$. Then for any $\gamma \in \mathbf{Z}[\beta]$ and $k \in \mathbf{Z}$, $k \geqq 1$ there exist $a_0, \ldots, a_{k-1} \in \mathcal{N}$ and $\gamma' \in \mathbf{Z}[\beta]$ such that*

$$\gamma = \sum_{i=0}^{k-1} a_i\beta^i + \gamma'\beta^k \tag{4.1}$$

and

$$|\gamma'^{(j)}| < \frac{|\gamma^{(j)}|}{|\beta^{(j)}|^k} + \frac{A}{|\beta^{(j)}|-1}, \quad (j=1, \ldots, n). \tag{4.2}$$

Proof. Let $x^n + b_{n-1}x^{n-1} + \ldots + b_0$ be the defining polynomial of β. Then $|b_0| = |N_{\mathbf{K}/\mathbf{Q}}(\beta)|$. Let $\gamma \in \mathbf{Z}[\beta]$. The assertion is trivially true for $k=1$. Assume that it holds for a $k \geqq 1$, i.e.

$$\gamma = \sum_{i=0}^{k-1} a_i\beta^i + \gamma_k\beta^k, \tag{4.3}$$

where $a_i \in \mathcal{N}$, $i=0, 1, \ldots, k-1$ and $\gamma_k \in \mathbf{Z}[\beta]$. $\mathbf{Z}[\beta]$ is an order in $\mathbf{K}$, hence there exist $c_0, \ldots, c_{n-1} \in \mathbf{Z}$ with

$$\gamma_k = c_0 + c_1\beta + \ldots + c_{n-1}\beta^{n-1}.$$

Let $a \in \mathcal{N}$ with $c_0 \equiv a \pmod{|b_0|}$ and $h = (c_0 - a)/b_0$. Then

$$\gamma_k = \gamma_k - h(b_0 + b_1\beta + \ldots + b_{n-1}\beta^{n-1} + \beta^n) =$$
$$= a + (c_1 - hb_1)\beta + \ldots + (c_{n-1} - hb_{n-1})\beta^{n-1} - h\beta^n = a + \beta\gamma_{k+1}.$$

Inserting this into (4.3), we get (4.1) for $k+1$, which proves (4.1) for any $\gamma\in\mathbf{Z}[\beta]$ and $k\geqq 0$.

Taking conjugates in (4.1) we obtain

$$\gamma^{(j)} = \sum_{i=0}^{k-1} a_i(\beta^{(j)})^i+\gamma'^{(j)}(\beta^{(j)})^k$$

for any $j=1, \dots, n$. This implies

$$|\gamma'^{(j)}| \leqq \frac{|\gamma^{(j)}|}{|\beta^{(j)}|^k}+\frac{1}{|\beta^{(j)}|^k}\sum_{i=0}^{k-1}|a_i||\beta^{(j)}|^i,$$

from which (4.2) follows immediately. Lemma 4 is proved.

Proof of Theorem 3. First we prove the necessity of the conditions. Let $\{\beta, \mathcal{N}\}$ be a number system in $\mathbf{Z}[\alpha]$. Then $\beta\in\mathbf{Z}[\alpha]$ and so $\beta\in\mathbf{Z}_{\mathbf{K}}$. By Lemma 1, $0\in\mathcal{N}$, and by [3], $\mathcal{N}$ is a complete residue system mod $|N_{\mathbf{K}/\mathbf{Q}}(\beta)|$. This proves (ii).

By Lemma 3 we have $|\beta^{(j)}|\geqq 1$, $j=1, \dots, n$. $|\beta^{(j)}|=1$, $j=1, \dots, n$ is not possible, because in this case $|N_{\mathbf{K}/\mathbf{Q}}(\beta)|=1$ and so $\mathcal{N}$ may contain only one integer. Hence there exists $1\leqq j\leqq n$ with $|\beta^{(j)}|>1$. If for an ℓ $(1\leqq\ell\leqq n)$ we have $|\beta^{(\ell)}|=1$, then $\beta^{(\ell)}$ is not real. Taking $\mathbf{L}=\mathbf{Q}(\beta^l+\bar{\beta}^l)$, then $\mathbf{L}$ is real and we have $[\mathbf{K}^{(\ell)}: \mathbf{L}]=2$, hence $\beta^{(\ell)}$ is a relative unit in $\mathbf{K}^{(\ell)}$, but then β is a unit and so there exists a h $(1\leqq h\leqq n)$ with $|\beta^{(h)}|<1$, which is impossible by Lemma 3.

(iii) and (iv) are obviously necessary for $\{\beta, \mathcal{N}\}$ to be a number system in $\mathbf{Z}[\alpha]$.

We proceed now to the proof of sufficiency. Let $\gamma\in\mathbf{Z}[\alpha]$. By (iii) $\mathbf{Z}[\alpha]\subset\mathbf{Z}[\beta]$ and so $\gamma\in\mathbf{Z}[\beta]$. There exists by (i) for any $\varepsilon>0$ an integer $k=k(\varepsilon)$ with

$$|\gamma^{(j)}| < \varepsilon|\beta^{(j)}|^k, \quad j = 1, \dots, n.$$

It is possible to find by Lemma 4 $a_i\in\mathcal{N}$, $i=0, \dots, k-1$ and $\gamma_k\in\mathbf{Z}[\beta]$ such that

$$\gamma = \sum_{i=0}^{k-1} a_i\beta^i+\gamma_k\beta^k \tag{4.4}$$

and

$$|\gamma_k^{(j)}| < \frac{|\gamma^{(j)}|}{|\beta^{(j)}|^k}+\frac{A}{|\beta^{(j)}|-1} < \varepsilon+\frac{A}{|\beta^{(j)}|-1}, \quad j = 1, \dots, n.$$

This inequality has only finitely many solutions for $\varepsilon=1$. This means, that we can choose ε such that for the corresponding k (2.1) holds. By (iv) and (4.4) we get the desired representation of γ. Theorem 3 is proved.

Proof of Theorem 4. In the proof of Theorem 3 we have seen that (i), (ii) and (iii) are necessary conditions for $\{\beta, \mathcal{N}\}$ to be a number system in $\mathbf{Z}[\alpha]$. Assume now that there exist a $0<k$ and $a_i\in\mathcal{N}$, $i=0, \ldots, k-1$ such that

$$0 \neq -\gamma = \frac{\sum_{i=0}^{k-1} a_i\beta^i}{(\beta^k-1)} \in \mathbf{Z}[\beta],$$

then

$$\gamma = \sum_{i=0}^{k-1} a_i\beta^i + \gamma\beta^k. \tag{4.5}$$

But $\gamma\in\mathbf{Z}[\beta]$ implies the representability of γ in the form

$$\gamma = c_0 + c_1\beta + \ldots + c_h\beta^h, \quad c_i\in\mathcal{N}, \ 1 \leqq i \leqq h. \tag{4.6}$$

Inserting (4.6) into the right-hand side of (4.5) we get a second finite representation of γ in $\{\beta, \mathcal{N}\}$ which is not allowed. Hence assumption (v) is necessary.

To prove the sufficiency of (v), it is enough to show that any $\gamma\in\mathbf{Z}[\alpha]$ with

$$|\gamma^{(j)}| \leqq \frac{A+1}{|\beta^{(j)}|-1}, \quad j = 1, \ldots, n \tag{4.7}$$

have a representation (1.1) in $\{\beta, \mathcal{N}\}$.

Let $\mathbf{K}^{(1)}, \ldots, \mathbf{K}^{(s)}$ be the real, $\mathbf{K}^{(s+1)}, \ldots, \mathbf{K}^{(s+2t)}$ the non-real conjugates of $\mathbf{K}$; $s+2t=n$. Then (4.7) implies

$$\begin{gathered} |\gamma^{(j)}| \leqq \frac{A+1}{|\beta^{(j)}|-1}, \quad j = 1, \ldots, s, \\ |\mathrm{Re}\,\gamma^{(s+j)}|, \ |\mathrm{Im}\,\gamma^{(s+j)}| \leqq \frac{A+1}{|\beta^{(j)}|-1} \quad j = 1, \ldots, t. \end{gathered} \tag{4.8}$$

Write $\gamma=c_0+c_1\beta+\ldots+c_{n-1}\beta^{n-1}$ with $c_i\in\mathbf{Z}$, $i=0, \ldots, n-1$. The number of solutions of (4.8) in $c_0, \ldots, c_{n-1}$, and so, the number of $\gamma\in\mathbf{Z}[\alpha]$ satisfying (4.7) is bounded above by

$$\left(\frac{2^{t+1}(A+1)}{D(\beta)^{1/2}}\sqrt{\sum_{j=1}^{n}\left(\frac{1}{|\beta^{(j)}|-1}\right)^2}\,(n|\beta|^n)^{(n-1)/2}\right)^n.$$

Let $\gamma\in\mathbf{Z}[\alpha]$ satisfying (4.7). Choose k so that

$$\frac{|\gamma^{(j)}|}{|\beta^{(j)}|^k} \leqq \frac{A+1}{|\beta^{(j)}|^k(|\beta^{(j)}|-1)} \leqq \frac{1}{|\beta^{(j)}|-1}$$

holds for any $j=1, \ldots, n$, i.e. let

$$k = \max_{1\leqq j\leqq n} \frac{\log(A+1)}{\log|\beta^{(j)}|}.$$

Then by Lemma 4, there exist $a_0, \ldots, a_{k-1} \in \mathcal{N}$ and $\gamma_1 \in \mathbf{Z}[\alpha]$ such that

$$\gamma = \sum_{i=0}^{k-1} a_i\beta^i + \gamma_1\beta^k.$$

and γ_1 satisfies (4.7). Repeating the application of Lemma 4 to γ_1 instead of γ we get a sequence $\gamma, \gamma_1, \gamma_2, \ldots$ of elements of $\mathbf{Z}[\alpha]$ with (4.7). This procedure either terminates with $\gamma_i = 0$ or will be periodic. If it is periodic, then we may assume that it is purely periodic, i.e.

$$\gamma = a_0 + a_1\beta + \ldots + a_{h-1}\beta^{h-1} + \gamma\beta^h \tag{4.9}$$

holds with $a_i \in \mathcal{N}$ and $h \leqq c$. At least one of $a_i \neq 0$, because otherwise β would be a root of unity. (4.9) implies that

$$-\gamma = (a_0 + a_1\beta + \ldots + a_{h-1}\beta^{h-1})/(\beta^h - 1) \in \mathbf{Z}[\alpha],$$

which contradicts the assumption. Theorem 4 is proved.

5. Canonical number systems in orders of algebraic number fields

In the sequel we set $\mathcal{N}_0(\alpha) = \{0, 1, \ldots, |a_0| - 1\}$ for an algebraic number α. Let the defining polynomial of α in $\mathbf{Z}[x]$ be $a_n x^n + \ldots + a_1 x + a_0$.

Theorem 6. *Let α and β be algebraic integers over $\mathbf{Q}$ such that $\mathbf{Z}[\alpha] = \mathbf{Z}[\beta]$. Assume that the coefficients of the defining polynomial $x^n + \ldots + b_1 x + b_0 \in \mathbf{Z}[x]$ of β satisfy*

$$0 < b_{n-1} \leqq \ldots \leqq b_0, \quad b_0 \geqq 2. \tag{5.1}$$

Then $\{\beta, \mathcal{N}_0(\beta)\}$ is a canonical number system in $\mathbf{Z}[\alpha]$.

Proof. See the proof of Theorem 1 in [8].

Corollary. *Let α be an algebraic integer over $\mathbf{Q}$. There exists an $N_0 \in \mathbf{Z}$ such that $\{\alpha - N, \mathcal{N}_0(\alpha - N)\}$ is a canonical number system in $\mathbf{Z}[\alpha]$ for all $N \geqq N_0$.*

Proof. Let the defining polynomial of α over $\mathbf{Z}[x]$ be $P(x) = a_n x^n + \ldots + a_1 x + a_0$. We may assume that $a_n > 0$. Let $N > 0$ and $P(x+N) = b_n(N)x^n + \ldots + b_1(N)x + b_0(N)$, then $b_i(N)$'s $(i = 0, 1, \ldots, n)$ are polynomials of degree $n - i$ in N with positive leading coefficients. Hence for all sufficiently large N, the $b_i(N)$ satisfy (5.1). Therefore by Theorem 6 $\{\alpha - N, \mathcal{N}_0(\alpha - N)\}$ are canonical number systems in $\mathbf{Z}[\alpha]$.

Lemma 5. *Let α be an algebraic integer over $\mathbf{Q}$. There exists an $M_0 \in \mathbf{Z}$ such that $\{\alpha + M, \mathcal{N}_0(\alpha + M)\}$ is not a canonical number system in $\mathbf{Z}[\alpha]$ for all $M \geqq M_0$.*

Proof. Let $P(x)$ be as in the proof of the Corollary. Let $M>0$ and $P(x-M)=$ $=c_n(M)x^n+\ldots+c_1(M)x+c_0(M)$. Then $c_0(M)=P(-M)$, hence there exists an $M_0\in\mathbf{Z}$ such that $c_0(M)$ is strictly decreasing (strictly increasing if n is even) for $M>M_0$. This means that $|c_0(M)|\in\mathcal{N}_0(\alpha+M+1)$. We have further

$$\frac{|c_0(M)|}{(\alpha+M+1)-1}=\frac{|c_0(M)|}{\alpha+M}\in\mathbf{Z}[\alpha],$$

and so $\{\alpha+M+1, \mathcal{N}_0(\alpha+M+1)\}$ is not a number system in $\mathbf{Z}[\alpha]$ by Theorem 4.

Lemma 6. *Let α be an algebraic integer over $\mathbf{Q}$. If $\alpha^{(i)}\geqq-1$ holds for some real conjugate of α, then $\{\alpha, \mathcal{N}_0(\alpha)\}$ is not a canonical number system in $\mathbf{Z}[\alpha]$.*

Proof. Let $\alpha^{(i)}$ be a real conjugate of α. If $\{\alpha, \mathcal{N}_0(\alpha)\}$ is a number system, then we have $|\alpha^{(i)}|\geqq 1$ by Lemma 3. $\alpha^{(i)}=-1$ is obviously impossible. If $\alpha^{(i)}\geqq 1$ and $a_j\in\mathcal{N}_0(\alpha)$, then $a_0+a_1\alpha^{(i)}+\ldots+a_l(\alpha^{(i)})^l\geqq 0$, i.e. the negative integers are not representable in $\{\alpha^{(i)}, \mathcal{N}_0(\alpha^{(i)})\}$. Lemma 6 is proved.

Proof of Theorem 5. By the assumption $\mathcal{O}$ is an integral domain of characteristic 0, so if there exists a canonical number system $\{\alpha, \mathcal{N}_0(\alpha)\}$ in $\mathcal{O}$, then $\mathcal{O}=\mathbf{Z}[\alpha]$, i.e. $1, \alpha, \ldots, \alpha^{n-1}$ is a power basis in $\mathcal{O}$, by Theorem 1 Győry [4] proved that there exist finitely many effectively computable element $\beta_1, \beta_2, \ldots, \beta_t$ in $\mathcal{O}$ such that $1, \alpha, \ldots, \alpha^{n-1}$ is a power basis in $\mathcal{O}$, if and only if $\alpha=\beta_i+H$, for some integers H, $1\leqq i\leqq t$.

Let $1\leqq i\leqq t$ be fixed. By Lemma 5, one can find an integer M_i such that $\{\beta_i+M, \mathcal{N}_0(\beta_i+M)\}$ is not a number system in $\mathcal{O}$ for all $M>M_i$. On the other hand, by the Corollary there exists an $m_i\in\mathbf{Z}$ such that $\{\beta_i+m, \mathcal{N}_0(\beta_i+m)\}$ is a number system in $\mathcal{O}$, for all $m\leqq m_i$. Finally by Theorem 4 it is possible to decide for every $m_i<m\leqq M_i$ whether $\{\beta_i+m, \mathcal{N}_0(\beta_i+m)\}$ is a number system in $\mathcal{O}$. Taking

$$N_i=\{m|m_i<m\leqq M_i,\ \{\beta_i+m, \mathcal{N}_0(\beta_i+m)\} \text{ is number system in } \mathcal{O}\}$$

and $n_i=-m_i$, they satisfy the assertion of Theorem 5, which completes the proof.

6. Computational results

Let $\mathbf{K}$ be an algebraic number field of degree n. Let $\mathbf{K}^{(1)}, \ldots, \mathbf{K}^{(s)}$ the real and $\mathbf{K}^{(s+1)}, \ldots, \mathbf{K}^{(s+t)}, \overline{\mathbf{K}^{(s+1)}}, \ldots, \overline{\mathbf{K}^{(s+t)}}$ the non-real conjugates of $\mathbf{K}$, $n=s+2t$. Let $\mathcal{O}$ be an order in $\mathbf{K}$. For the maximal orders of $\mathbf{Q}$ and for the quadratic extensions of $\mathbf{Q}$ all canonical number systems are known of [10], [5], [6]. For higher degree fields the problem is more difficult.

Based on Theorem 5 we can give the following algorithm to determine the canonical number systems in $\mathcal{O}$:

1. Compute $\alpha_1, \ldots, \alpha_h \in \mathcal{O}$ such that $1, \alpha, \ldots, \alpha^{n-1}$ is a power basis in $\mathcal{O}$, if and only if $\alpha = \alpha_i + H$ for some $1 \leqq i \leqq h$ and $H \in \mathbf{Z}$.

2. If $s > 0$, then find the minimal n_i, $(i = 1, \ldots, h)$ such that for any $m \geqq n_i$

$$\alpha_i^{(j)} - m < -1 \quad (j = 1, \ldots, s) \quad \text{and} \quad |\alpha_i^{(s+j)} - m| > 1, \quad j = 1, \ldots, t.$$

Otherwise, compute the minimal n_i such that $P_i(-x)$ is strictly increasing for $x \geqq n_i$, where $P_i(x)$ denotes the defining polynomial of α_i over $\mathbf{Z}$.

3. Calculate M_i $(i = 1, \ldots, h)$ such that for all $m > M_i$ the coefficients of the defining polynomials of $\alpha_i - m$ satisfy (5.1).

4. Decide for every m with $n_i < m \leqq M_i$ whether $\{\alpha_i - m, \mathcal{N}_0(\alpha_i - m)\}$ is number system in $\mathcal{O}$.

The hardest problem in this algorithm is step 1. Győry [4] proved that $\alpha_1, \ldots, \alpha_h$ are effectively computable by giving explicit upper bounds for their heights. His result is based on A. Baker's theorem on linear forms in the logarithms of algebraic numbers, hence in practice it is not applicable at this time. For totally real cubic fields with discriminant $\leqq 3137$ Gaál and Schulte [2] computed such complete systems, using the Baker—Davenport reduction method.

Using their results we computed — in the sense of Theorem 5 — all but one canonical number systems in the maximal orders of totally real cubic fields with discriminant $\leqq 564$.

Steps 2 and 3 are easy to perform. For the computation of M_i we remark that it is the smallest value of $m \in \mathbf{Z}$ such that the coefficients of the defining polynomial of $\alpha_i - m$ satisfy (5.1). Of course assume that

$$1 \leqq a_1 \leqq a_2 \leqq a_3 \tag{6.1}$$

and the roots $\beta_1, \beta_2, \beta_3$ of the polynomial $P(x) = x^3 + a_1 x^2 + a_2 x + a_3$ are real with $\beta_i < -1$ $(i = 1, 2, 3)$. This implies $a_1 \geqq 4$. Since both roots of $P'(x) = 3x^2 + 2a_1 x + a_2$ are real and are less then -1 we get

$$a_2 \geqq 2a_1 - 3 \geqq a_1 + 2. \tag{6.2}$$

On the other hand $P(x+1) = x^3 + (a_1 + 3)x^2 + (a_2 + 2a_1 + 3)x + (a_3 + a_2 + a_1 + 1)$. Using (6.1) and (6.2) we get

$$a_3 + a_2 + a_1 + 1 \geqq 2a_1 + a_2 + 3,$$

hence the coefficients of x in $P(x+1)$ satisfy (5.1) too.

To perform Step 4 we have to enumerate all $\gamma \in \mathbf{Z}_K$ with (2.1) and then to check whether they are representable in the corresponding number system. For the enumeration we used the method of Fincke and Pohst [1].

In the table we listed the discriminants D of all totally real cubic fields $\mathbf{K}$ with $D \leqq 564$, which have power basis. In the column (x, y) we displayed the solutions — computed by GAÁL and SCHULTE [2] — of the index form equation of $\mathbf{K}$, corresponding to an integral basis 1, ω_1, ω_2 of $\mathbf{Z_K}$. Then in the columns $P_+(x)$, $(P_-(x))$ you find the coefficients — starting with the leading coefficient 1 — of the defining polynomial of $\beta = a + x\omega_1 + y\omega_2$, $(\beta = b - x\omega_1 - y\omega_2)$ $(a, b \in \mathbf{Z})$ such that $\{\alpha, \mathcal{N}_0(\alpha)\}$ is a number system in $\mathbf{Z_K}$ if and only if $\alpha = \beta - h$ with some integer $h \geqq 0$. We did not find sporadic cases, i.e. the finite sets N_i defined in Theorem 5 were always empty.

The computer program was developed in FORTRAN and was executed on an IBM PC—AT compatible computer. If the sequence of the coefficients of $P_+(x)$ $(P_-(x))$ is not monotonic, then the execution time depends on the number of solutions of (2.1), which was between 600 and 18 000. The computer tested about 40 solutions of (2.1)/seconds.

For the field with $D = 229$; $(x, y) = (508, 273)$ we were not able to compute all solutions of (2.1) because of the large number of solutions.

Let 1, α, α^2 be a power integral basis of a totally real cubic field. Our computation suggests that $\alpha^{(i)} < -1$ $(i = 1, 2, 3)$ is a sufficient condition for $\{\alpha, \mathcal{N}_0(\alpha)\}$ to be a number system in $\mathbf{Z_K}$.

D	(x, y)	$P_+(x)$				$P_-(x)$			
49	$(-1, -1)$ $(0, 1)$ $(1, 0)$	1	10	31	29	1	8	19	13
	$(-2, -1)$ $(1, -1)$ $(1, 2)$	1	09	20	13	1	15	68	83
	$(-5, -9)$ $(-4, 5)$ $(9, 4)$	1	46	563	769	1	26	83	71
81	$(-3, -2)$ $(1, 3)$ $(2, -1)$	1	12	27	17	1	21	126	159
	$(-1, -1)$ $(0, 1)$ $(1, 0)$	1	09	24	19	1	9	24	17
148	$(-31, 14)$	1	305	23 515	39 349	1	154	412	278
	$(-5, -3)$	1	18	50	38	1	30	242	250
	$(-1, -1)$	1	11	37	37	1	10	30	26
	$(1, 0)$	1	9	23	17	1	12	44	46
	$(1, 2)$	1	11	27	19	1	16	72	62
169	$(-2, -1)$ $(1, 0)$ $(1, 1)$	1	10	29	25	1	11	36	31

229	(−2, 1)	1	22	134	139	1	14	38	29
	(0, 1)	1	10	28	23	1	11	35	26
	(1, 0)	1	9	23	16	1	12	44	47
	(1, 4)	1	19	43	26	1	35	331	424
	(2, 1)	1	19	105	134	1	11	25	16
	(508, 273)	1	3492	3 050 996	4 329 199	(1	1749	5975	5108)?
257	(−11, −6)	1	36	121	107	1	66	1141	1695
	(−1, −1)	1	10	29	21	1	11	36	35
	(1, 0)	1	09	22	15	1	12	43	41
	(5, 2)	1	32	93	71	1	58	873	919
	(−2, −3)	1	27	202	259	1	15	34	21
	(2, 1)	1	17	86	111	1	10	23	15
316	(1, 0)	1	10	29	22	1	11	36	34
	(1, 2)	1	13	32	22	1	23	152	218
324	(1, 0)	1	10	29	23	1	11	36	33
	(−1, −1)	1	14	59	67	1	10	27	21
364	(−1, 1)								
	(0, −1)	1	13	50	49	1	11	34	31
	(1, 0)								
	(−7, −2)								
	(−2, 9)	1	40	109	77	1	77	1552	2653
	(9, −7)								
404	(1, 0)	1	10	28	22	1	11	35	27
	(1, 1)	1	11	33	29	1	13	49	43
469	(1, 0)	1	10	26	19	1	14	58	61
	(−2, −1)	1	13	51	56	1	11	35	32
473	(−2, −1)	1	13	34	25	1	20	111	107
	(0, 1)	1	11	32	27	1	13	48	37
	(1, 5)	1	28	63	37	1	53	738	935
	(7, −3)	1	39	124	103	1	72	1345	1747
	(1, 0)	1	12	43	45	1	12	43	43
564	(−3, −7)	1	77	1 541	2 239	1	40	98	62
	(−3, −1)	1	17	49	39	1	28	214	246
	(−3, 2)	1	41	455	697	1	22	56	38
	(1, 0)	1	13	51	57	1	11	35	31

References

[1] U. Fincke and M. Pohst, A procedure for determining algebraic integers of given norm, in: *Computer Algebra* (London, 1983), Lecture Notes in Computer Sci., 162, Springer (Berlin—New York, 1983), pp. 194—202.

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

[3] W. J. Gilbert, Geometry of radix representation, in: *The geometric vein*, Springer (New York—Berlin, 1981), pp. 129—139.

[4] K. GYŐRI, Sur les polynomes a coefficients entiers et de discriminant donne. III, *Publ. Math. Debrecen*, **23** (1976), 141—165.

[5] I. KÁTAI und B. KOVÁCS, Kanonische Zahlensysteme in der Theorie der quadratischen Zahlen, *Acta Sci. Math.*, **42** (1980), 99—107.

[6] I. KÁTAI and B. KOVÁCS, Canonical number systems in imaginary quadratic fields, *Acta Math. Acad. Sci. Hungar.*, **37** (1981). 159—164.

[7] I. KÁTAI and J. SZABÓ, Canonical number systems for complex integers, *Acta Sci. Math.*, **37** (1975), 255—260.

[8] B. KOVÁCS, Integral domains with canonical number systems, *Publ. Math. Debrecen*, **36** (1989), 153—156.

[9] B. KOVÁCS and A. PETHŐ, Canonical systems in the ring of integers, *Publ. Math. Debrecen*, **30** (1983), 39—45.

[10] D. E. KNUTH, *The Art of Computer Programming Vol. 2. Seminumerical Algorithms*, 2. ed., Addison Wesley Publ. Co. (Reading, Mass., 1981).

KOSSUTH LAJOS UNIVERSITY
MATHEMATICAL INSTITUTE
4010 DEBRECEN, P.O. BOX 12
HUNGARY