Annales Univ. Sci. Budapest., Sect. Comp. 18 (1999) 167-174

ON THE PERIODIC EXPANSION OF ALGEBRAIC NUMBERS

A. Pethő (Debrecen, Hungary)

To the memory of B. Kovács and I. Környei

1. Introduction

Let $\mathbb{K}$ be an algebraic number field of degree n with ring of integers $\mathbb{Z}_{\mathbb{K}}$. Let $\mathbb{K}^{(i)}$, $i = 1, \ldots, n$ denote the conjugates of $\mathbb{K}$ in the field of the complex numbers $\mathbb{C}$. Similarly $\alpha^{(i)}$ will denote the i-th conjugate of $\alpha \in \mathbb{K}$ $(i = 1, \ldots, n)$. For $\alpha \in \mathbb{Z}_{\mathbb{K}}$ and $\mathcal{N} \subseteq \mathbb{Z}$ the pair $\{\alpha, \mathcal{N}\}$ is called a number system $\mathcal{NS}$, if there exist uniquely for every $0 \neq \beta \in \mathbb{Z}[\alpha]$ a nonnegative integer $L(\beta)$ and $b_0, \ldots, b_{L(\beta)} \in \mathcal{N}$ such that $b_{L(\beta)} \neq 0$ and

$$\beta = \sum_{i=0}^{L(\beta)} b_i \alpha^i. \tag{1}$$

After partial results Kovács and Pethő [8] gave a complete characterization of number systems in algebraic number fields. In [9] they gave asymptotic estimate for $L(\beta)$, which you find here as Lemma 1.

Having a number system it is natural to ask which elements of $\mathbb{R}(\alpha)$ have an infinite power series expansion of α with "digits" from $\mathcal{N}$. Remark that the field $\mathbb{R}(\alpha)$ is $\mathbb{R}$, the field of the real numbers and $\mathbb{C}$, according as α is real or non-real. Another natural question is whether the well-known rationality criterion of the ordinary q-ary representation of real numbers may be generalized for the new situation.

Research supported by the Hungarian National Foundation for Scientific Research, Grant No. 16791.

To be more precise, let $\{\alpha, \mathcal{N}\}$ be a $\mathcal{NS}$ such that $\mathbb{K} = \mathbb{Q}(\alpha)$. We shall denote by $\mathcal{S}(\alpha)$ the set of those complex numbers γ for which either $\gamma = 0$ or

$$\gamma = \sum_{i=L(\gamma)}^{\infty} a_{-i}\alpha^{-i} \tag{2}$$

with some $a_i \in \mathcal{N}$, $i = L(\gamma), L(\gamma) - 1, \ldots$ and $a_{-L(\gamma)} \neq 0$. We shall call (2) the $\alpha\mathcal{N}$-expansion of γ. This concept was introduced by Kátai and Szabó [3]. They proved that if α is a Gaussian integer and $\{\alpha, \mathcal{N}\}$ is a $\mathcal{NS}$ in $\mathbb{Z}[i]$ then any complex number has an $\alpha\mathcal{N}$-expansion. Later Kovács [5] characterized those $\{\alpha, \mathcal{N}\}$ number systems for which any $\gamma \in \mathbb{R}(\alpha)$ have $\alpha\mathcal{N}$-expansions. Using this result and properties of interval filling sequences Kovács and Maksa [7] proved far reaching generalization of the theorem of Kátai and Szabó. They proved for example that if α is real $\mathcal{N} = \{0, 1, \ldots, |Norm(\alpha)| - 1\}$ then any real γ have $\alpha\mathcal{N}$-expansions. $Norm(\alpha)$ denotes the norm of α.

This problem was completely solved, even in more general setting, by Kátai and Környei [2]. By their result any $\gamma \in \mathbb{R}(\alpha)$ has an $\alpha\mathcal{N}$-expansion. Using this theorem Kovács and Környei [6] proved that the $\alpha\mathcal{N}$-expansion of a $\gamma \in \mathbb{R}(\alpha)$ is periodic if and only if $\gamma \in \mathbb{Q}(\alpha)$. Unfortunately, the method of Kovács and Környei is not algorithmic, one can hardly compute the periodic expansion of a given $\gamma \in \mathbb{Q}(\alpha)$.

The aim of this paper is to prove that at least one periodic $\alpha\mathcal{N}$-expansion of any $\gamma \in \mathbb{Q}(\alpha)$ can be found by using the arithmetic of $\mathbb{Z}_{\mathbb{K}}$. Our method is independent from the abovementioned theorem of Kátai and Környei, it is essentially the same as the method which computes the periodic q-ary expansion of rational numbers. We are stating now our result.

Theorem 1. *Let $\{\alpha, \mathcal{N}\}$ be a $\mathcal{NS}$ such that $K = \mathbb{Q}(\alpha)$. Then there exists an algorithm which computes a periodic $\alpha\mathcal{N}$-expansion for any $\gamma \in \mathbb{K}$.*

It is obvious from the theorem of Kátai and Környei that any $\gamma \in \mathbb{R}(\alpha)$ may have many different $\alpha\mathcal{N}$-expansions. On the other hand it is not clear how many periodic $\alpha\mathcal{N}$-expansions of the elements of $\mathbb{K}$ may have. We shall point out in Section 3 that even the periodic $\alpha\mathcal{N}$-expansion of the elements of $\mathbb{K}$ is not unique. In all of the examples I studied, the different expansions were closely related, more precisely they were different only in finitely many digits. It remains an open question whether there exist essentially different periodic expansions.

2. Proof of Theorem 1

An important tool in the proof of Theorem 1 is the following theorem of Kovács and Pethő [9].

Lemma 1. *Let $\{\alpha, \mathcal{N}\}$ be a $\mathcal{NS}$, α being of degree n and $0 \neq \gamma \in \mathbb{Z}[\alpha]$. Then there exist constants $c_1(\alpha, \mathcal{N})$, $c_2(\alpha, \mathcal{N})$ such that*

$$\max_{1 \leq i \leq n} \frac{\log |\gamma^{(i)}|}{\log |\alpha^{(i)}|} + c_1(\alpha, \mathcal{N}) \leq L(\gamma) \leq \max_{1 \leq i \leq n} \frac{\log |\gamma^{(i)}|}{\log |\alpha^{(i)}|} + c_2(\alpha, \mathcal{N}).$$

Remark that the constants c_1 and c_2 do not depend on γ.

In the proof of Theorem 1 we follow essentially the proof of the analogous statement for the q-ary representation of real numbers as given in Bundschuh [1]. Let $0 \neq \gamma \in \mathbb{K} = \mathbb{Q}(\alpha)$. Write $\gamma = \frac{\beta}{\delta}$ with $\beta, \delta \in \mathbb{Z}[\alpha]$.

Assume first that $(\delta) + (\alpha) = (1)$, where and in the sequel (δ) denotes the principal ideal generated by δ in $\mathbb{Z}_{\mathbb{K}}$. There exists an integer $d > 0$ such that $\alpha^d \equiv 1 \pmod{\delta}$ holds in $\mathbb{Z}[\alpha]$. Let fix d and put $\alpha^d - 1 = \delta\kappa_1$. Then for $m \geq 1$ integer δ divides obviously $\alpha^{dm} - 1$. Put $\alpha^{dm} - 1 = \delta\kappa_m$. Then we have $\mathcal{K}_m \in \mathbb{Z}[\alpha]$ and

$$\gamma = \frac{\beta\kappa_1}{\alpha^d - 1} = \frac{\beta\kappa_m}{\alpha^{dm} - 1} = \frac{\beta\kappa_1(\alpha^{d(m-1)} + \ldots + 1)}{\alpha^{dm} - 1} = \frac{\varepsilon_m}{\alpha^{dm} - 1}. \tag{3}$$

As $0 \neq \varepsilon_m \in \mathbb{Z}[\alpha]$, thus ε_m can be represented in $\{\alpha, \mathcal{N}\}$ and

$$L(\varepsilon_m) \leq \max_{1 \leq i \leq n} \frac{\log |\varepsilon_m^{(i)}|}{\log |\alpha^{(i)}|} + c_2 = \max_{1 \leq i \leq n} \frac{\log |(\beta\kappa_1)^{(i)}| + \log \left| \frac{\alpha^{(i)dm} - 1}{\alpha^{(i)} - 1} \right|}{\log |\alpha^{(i)}|} + c_2 <$$

$$< \max_{1 \leq i \leq n} \frac{\log |(\beta\kappa_1)^{(i)}| - \log |\alpha^{(i)} - 1|}{\log |\alpha^{(i)}|} + c_2 + dm.$$

Notice that the first two summands are independent from m, hence

$$|L(\varepsilon_m) - dm| \leq c_3$$

with c_3 independent from m, and we can write

$$\varepsilon_m = \sum_{i=0}^{dm-1} a_{mi}\alpha^i + \sum_{i=dm}^{L(\varepsilon_m)} a_{mi}\alpha^i = \omega_m + \alpha^{dm}\tau_m$$

with $a_{mi} \in \mathcal{N}$, $i = 0, \ldots, L(\varepsilon_m)$. As the length of τ_m is bounded by a constant, which does not depend on m and the "digits" a_{mi}, $i = dm, \ldots, L(\varepsilon_m)$ belong to a finite set, there are only finitely many possibilities for τ_m, $m = 1, 2, \ldots$ Thus there exist $0 < \ell < k$ integers such that $\tau_{2^\ell} = \tau_{2^k} = \tau$. Let fix ℓ and k for the sequel. We have

$$\begin{aligned}\varepsilon_{2^k} &= \beta\kappa_1 \frac{\alpha^{d\cdot 2^k} - 1}{\alpha^d - 1} = \beta\kappa_1 \frac{\alpha^{d\cdot 2^\ell} - 1}{\alpha^d - 1} \cdot \frac{\alpha^{d\cdot 2^k} - 1}{\alpha^{d\cdot 2^\ell} - 1} = \\ &= \varepsilon_{2^\ell}(1 + \alpha^{d\cdot 2^\ell} + \ldots + \alpha^{d(2^k - 2^\ell)}) = \\ &= \omega_{2^\ell} + (\omega_{2^\ell} + \tau)\alpha^{d\cdot 2^\ell}(1 + \alpha^{d\cdot 2^\ell} + \ldots + \alpha^{d(2^k - 2^{\ell+1})} + \alpha^{d\cdot 2^k}\tau.\end{aligned}$$

On the other hand

$$\varepsilon_{2^k} = \omega_{2^k} + \alpha^{d\cdot 2^k}\tau.$$

Both ω_{2^ℓ} and τ are assumed already represented in $\{\alpha, \mathcal{N}\}$. If we write $\omega_{2^\ell} + \tau$ in $\{\alpha, \mathcal{N}\}$ then it may happen that the length of $\omega_{2^\ell} + \tau$ is longer than $d \cdot 2^\ell - 1$. Let

$$\eta_k = (\omega_{2^\ell} + \tau) \sum_{i=0}^{2^{k-\ell}-2} \alpha^{d\cdot 2^{\ell_i}}.$$

We get in this notation

$$\varepsilon_{2^k} = \omega_{2^\ell} + \alpha^{d\cdot 2^\ell}\eta_k + \alpha^{d\cdot 2^k}\tau.$$

We have on the other hand

$$\varepsilon_{2^k} = \omega_{2^k} + \alpha^{d\cdot 2^k}\tau,$$

where both ω_{2^k} and τ are written in $\{\alpha, \mathcal{N}\}$. Thus $\omega_{2^k} = \omega_{2^\ell} + \alpha^{d\cdot 2^\ell}\eta_k$ and we have

$$L(\eta_k) \leq d(2^k - 2^\ell) - 1 \tag{4}$$

for the $\{\alpha, \mathcal{N}\}$ expansion of η_k.

Let now $t \geq 0$ an integer and consider $\varepsilon_{2^k + t(2^k - 2^\ell)}$. We have similarly as above

$$\varepsilon_{2^k + t(2^k - 2^\ell)} = \varepsilon_{2^\ell} \sum_{i=0}^{(t+1)(2^{k-\ell}-1)} \alpha^{d\cdot 2^{\ell_i}} =$$

$$= \omega_{2^\ell} + (\omega_{2^\ell} + \tau) \sum_{i=1}^{(t+1)(2^{k-\ell}-1)} \alpha^{d\cdot 2^\ell i} + \tau \cdot \alpha^{d\cdot 2^\ell[(t+1)(2^{k-\ell}-1)+1]} =$$

$$= \omega_{2^\ell} + \sum_{j=0}^{t} \alpha^{d\cdot 2^\ell(j(2^{k-\ell}-1)+1)}(\omega_{2^\ell} + \tau) \sum_{i=0}^{2^{k-\ell}-2} \alpha^{d\cdot i 2^\ell} +$$

$$+ \tau \cdot \alpha^{d\cdot 2^\ell[(t+1)(2^{k-\ell}-1)+1]} =$$

$$= \omega_{2^\ell} + \eta_k \alpha^{d\cdot 2^\ell} \sum_{j=0}^{t} \alpha^{j\cdot d(2^k-2^\ell)} + \tau\alpha^{d[(t+1)(2^k-2^\ell)+2^\ell]}.$$

This is by (4) already the $\{\alpha, \mathcal{N}\}$ expansion of $\varepsilon_{2^k+t(2^k-2^\ell)}$ if we insert the $\{\alpha, \mathcal{N}\}$ expansions of ω_{2^ℓ}, η_k and τ.

Let $A = \max\{|b|,\ b \in \mathcal{N}\}$, then we have

$$|\beta| \leq A \cdot |\alpha|^{L(\beta)} \frac{|\alpha|}{|\alpha| - 1} \tag{5}$$

for any $\beta \in \mathbb{Z}[\alpha]$. Put $B = \max\{L(\omega_{2^\ell}),\ L(\tau),\ L(\eta_k)\} = \max\{d\cdot 2^\ell,\ c_3,\ d(2^k - -2^\ell)\}$. Using (5) we get

$$\left|\varepsilon_{2^k+t(2^k-2^\ell)} - \left(\tau + \eta_k \sum_{j=1}^{\infty} \alpha^{-j\cdot d(2^k-2^\ell)}\right)\left(\alpha^{d[2^k+t(2^k-2^\ell)]} - 1\right)\right| =$$

$$= \left|\omega_{2^\ell} - \eta_k \sum_{j=t+2}^{\infty} \alpha^{-j\,d(2^k-2^\ell)} + \tau + \eta_k \sum_{j=1}^{\infty} \alpha^{-j\,d(2^k-2^\ell)}\right| \leq$$

$$\leq 4 \cdot A|\alpha|^B \left(\frac{|\alpha|}{|\alpha| - 1}\right)^2 = c_4$$

for any $t \geq 0$ with c_4, which is independent from t. Taking now into consideration (3) we have

$$\gamma = \tau + \eta_k \sum_{j=1}^{\infty} \alpha^{-j\,d(2^k-2^\ell)},$$

which is a periodic $\alpha\mathcal{N}$-expansion of γ. This proves Theorem 1 in the particular case.

In the second part of the proof we are dealing with the general situation, i.e. if $\gamma = \frac{\beta}{\delta}$ with $\beta, \delta \in \mathbb{Z}[\alpha]$, but $(\delta) + (\alpha) \subset (1)$ in $\mathbb{Z}_{\mathbb{K}}$. Let the prime ideal decomposition of the ideal (α, δ) in $\mathbb{Z}_{\mathbb{K}}$ be

$$(\alpha, \delta) = \mathcal{P}_1^{c_1} \dots \mathcal{P}_t^{c_t},$$

where $c_1, \dots, c_t$ are positive integers.

$$(\delta) = \mathcal{P}_1^{a_1} \dots \mathcal{P}_t^{a_t} \mathcal{Q}_\delta \quad \text{and} \quad (\alpha) = \mathcal{P}_1^{b_1} \dots \mathcal{P}_t^{b_t} \mathcal{Q}_\alpha$$

with $\mathcal{Q}_\delta + (\alpha) = (1)$. Denote by h the class number of $\mathbb{Z}_{\mathbb{K}}$. Then $\mathcal{P}_i^h = (\pi_i)$, $i = 1, \dots, t$; $\mathcal{Q}_\delta^h = (\rho_\delta)$ and $\mathcal{Q}_\alpha^h = (\rho_\alpha)$ with $\pi_1, \dots, \pi_t$, ρ_δ, $\rho_\alpha \in \mathbb{Z}_{\mathbb{K}}$, and we have

$$\delta^h = \pi_1^{a_1} \dots \pi_t^{a_t} \rho_\delta \eta_\delta \quad \text{and} \quad \alpha^h = \pi_1^{b_1} \dots \pi_t^{b_t} \rho_\alpha \eta_\alpha,$$

where η_δ and η_α are units in $\mathbb{Z}_{\mathbb{K}}$. We may assume without loss of generality, eventually changing ρ_δ and ρ_α, that $\eta_\delta = \eta_\alpha = 1$.

Let s be a positive integer such that $sb_i \geq a_i$ hold for all $i = 1, \dots, t$ and put

$$\delta_1 = \delta^h \pi_1^{sb_1 - a_1} \dots \pi_t^{sb_t - a_t} \rho_\alpha^s = \alpha^{sh} \rho_\delta.$$

Then we have

$$\gamma = \frac{\beta \cdot \delta^{h-1} \pi_1^{sb_1 - a_1} \dots \pi_t^{sb_t - a_t} \rho_\alpha^s}{\alpha^{sh} \rho_\delta} = \frac{\beta_1}{\alpha^{sh} \rho_\delta}.$$

As $(\rho_\delta) + (\alpha) = 1$, there exists a periodic $\alpha\mathcal{N}$-expansion of $\frac{\beta_1}{\rho_\delta}$. Division with α^{sh} does not change the periodicity of this expansion, only the place of the "period", hence γ admits a periodic $\alpha\mathcal{N}$-expansion. Theorem 1 is proved.

3. Examples

To illustrate how one can compute in the line of the proof of Theorem 1 a periodic $\alpha\mathcal{N}$-expansion we choose α a zero of the cubic polynomial $x^3 + 9x^2 + 24x + 17$. We proved with B.Kovács in [8] that if $\mathcal{N} = \{0, \dots, 16\}$, then $\{\alpha, \mathcal{N}\}$ is a $\mathcal{NS}$ in $\mathbb{Z}[\alpha]$. Put $\gamma = 1/2$. It is easy to check that $\alpha^7 \equiv 1 \pmod 2$ and $\alpha^j \not\equiv 1 \pmod 2$ for any $0 < j < 7$. We have

$$\alpha^7 = -7932\alpha^2 - 33326\alpha - 27387.$$

Thus

$$\frac{1}{2} = \frac{-3966\alpha^2 - 16663\alpha - 13694}{\alpha^7 - 1} =$$
$$= \frac{8 + 12\alpha + 13\alpha^2 + 4\alpha^3 + \alpha^4 + 8\alpha^5 + 4\alpha^6 + \alpha^7}{\alpha^7 - 1} =$$
$$= \left(1 + \frac{4}{\alpha} + \frac{8}{\alpha^2} + \frac{1}{\alpha^3} + \frac{4}{\alpha^4} + \frac{13}{\alpha^5} + \frac{12}{\alpha^6} + \frac{8}{\alpha^7}\right) \sum_{i=0}^{\infty} \alpha^{-7i} =$$
$$= \alpha + (4\alpha^6 + 8\alpha^5 + \alpha^4 + 4\alpha^3 + 13\alpha^2 + 12\alpha + 9) \sum_{i=1}^{\infty} \alpha^{-7i}.$$

Finally we shall show that the periodic $\alpha\mathcal{N}$-expansion is generally not unique. Let $p(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$ such that $1 = a_0 \leq a_1 \leq \leq \ldots \leq a_n$, $a_n \geq 2$, α a zero of $p(x)$ and $\mathcal{N} = \{0, \ldots, a_n - 1\}$. Then $\{\alpha, \mathcal{N}\}$ is a $\mathcal{NS}$ in $\mathbb{Z}[\alpha]$ by B.Kovács [4], hence $|\alpha| > 1$.

Put

$$\gamma = a_n \sum_{i=1}^{\infty} \alpha^{-i} = a_n \frac{\alpha}{\alpha - 1}.$$

As $a_n \notin \mathcal{N}$ this is not an $\alpha\mathcal{N}$-expansion of γ, but we can easily find $\alpha\mathcal{N}$-expansions of γ. Indeed, let $0 \leq j \leq n$, then as $p(\alpha) = 0$ we have

$$\gamma = a_n \sum_{i=1}^{\infty} \alpha^{-i} - \frac{p(\alpha)}{\alpha^j} \sum_{i=0}^{\infty} \alpha^{-i(n+1)} + p(\alpha) =$$
$$= a_0\alpha^n + \ldots + a_{j-1}\alpha^{n-j+1} + (a_j - a_0)\alpha^{n-j} + (a_n - a_{n-j})\alpha^0 +$$
$$+ (a_n - a_{n-j-1})\alpha^{-1} + \ldots + (a_n - a_n)\alpha^{-j} +$$
$$+ \sum_{i=1}^{\infty} ((a_n - a_0)\alpha^n + \ldots + (a_n - a_n))\alpha^{-i(n+1)-j},$$

where $a_{-1} = 0$ if $j = 0$. It is clear that the coefficients of this power series belong to $\mathcal{N}$, hence γ has at least $n + 1$ different, periodic $\alpha\mathcal{N}$-expansions.

References

[1] **Bundschuh P.,** *Einführung in die Zahlentheorie,* Springer, 1988, 5.1.

[2] **Kátai I. and Környei I.,** On number systems in algebraic number fields, *Publ. Math. Debrecen,* **41** (1992), 289-294.

[3] **Kátai I. and Szabó J.,** Canonical number systems for complex integers, *Acta Sci. Math. Szeged,* **37** (1975), 255-260.

[4] **Kovács B.,** Integral domains with canonical number systems, *Publ. Math. Debrecen,* **36** (1989), 153-156.

[5] **Kovács B.,** Representation of complex numbers in number systems, *Acta Math. Hungar.,* **58** (1991), 113-120.

[6] **Kovács B. and Környei I.,** On the periodicity of the radix representation, *Annales Univ. Sci. Bud. Sect. Comp.,* **13** (1992), 129-133.

[7] **Kovács B. and Maksa Gy.,** Interval-filling sequences of order N and a representation of real numbers in canonical number systems, *Publ. Math. Debrecen,* **39** (1991), 305-313.

[8] **Kovács B. and Pethő A.,** Number systems in integral domains, especially in orders of algebraic number fields, *Acta Sci. Mat. Szeged,* **55** (1991), 287-299.

[9] **Kovács B. and Pethő A.,** On a representation of algebraic integers, *Studia Sci. Math. Hungar.,* **27** (1992), 169-172.

A. Pethő
Laboratory of Informatics
University of Medicine
Nagyerdei krt. 98.
H-4028 Debrecen, Hungary