Number systems over orders of algebraic number fields

Attila Pethő

Department of Computer Science, University of Debrecen, Hungary
and University of Ostrava, Faculty of Science, Czech Republic

Joint work with Jörg Thuswaldner, Leoben, Austria

23rd Czech and Slovak International Conference on Number Theory
Ostravice, August 28 - September 1, 2017

1. Introduction

Let $p \in \mathbb{Z}[x]$ and $\mathcal{D}$ be a complete residue system modulo $p(0)$. After preliminary works by Grünwald, Knuth, Penney, Kátai, Gilbert, Júlia Szabó, B. Kovács, Körmendi, Környei I called $(p, \mathcal{D})$ a *number system*, if for every $a \in \mathbb{Z}[x]$ there exist uniquely $\ell \geq 0$ and $a_0, \ldots, a_\ell \in \mathcal{D}$ such that

$$a \equiv a_0 + a_1 x + \ldots + a_\ell x^\ell \pmod{p}.$$

Example:

$$2017 \equiv 7 + 1 \cdot x + 0 \cdot x^2 + 2 \cdot x^3 \pmod{x - 10}.$$

If $\mathcal{D} = \{0, 1, \ldots, |p(0)| - 1\}$ then $(p, \mathcal{D})$ is called a *canonical number system*.

Generalizations to larger ground rings:

• Jacob and Reveilles (1995), Brunotte, Kirschenhofer and Thuswaldner (2011): $\mathbb{Z}[i]$
• Scheicher, Surer, Thuswaldner and van de Woestijne (2014): commutative rings
• Pethő and Varga (2017): Euclidean imaginary quadratic number fields.

We generalize here the number sytem concept in two directions:

• Allow orders of algebraic number fields as ground rings. (Radix representation in relative extendions.)
• The digit set is defined on a uniform way, which allow the investigation of families of polynomials. We show that the canonical digit set is extraordinary, it has very special properties.

2. Definitions and basic properties

Notations:

- $\mathbb{K}$ number field of degree k,
- $\alpha^{(1)}, \dots, \alpha^{(k)}$ the conjugates of $\alpha \in \mathbb{K}$,
- $\mathcal{O}$ an order in $\mathbb{K}$, *i.e.*, a ring which is a full $\mathbb{Z}$-module in $\mathbb{K}$.
- $1 = \omega_1, \omega_2, \dots, \omega_k$ a $\mathbb{Z}$-basis of $\mathcal{O}$,
- $H(a) = \max\{|a_l^{(j)}|,\ l = 0, \dots, n,\ j = 1, \dots, k\}$ the *height* of a, provided $a(x) = \sum_{l=0}^{n} a_l x^l \in \mathcal{O}[x]$.

A *generalized number system over* $\mathcal{O}$ (GNS for short) is a pair $(p, \mathcal{D})$, where $p \in \mathcal{O}[x]$ is monic, $p_0 \neq 0$ and $\mathcal{D} \subset \mathcal{O}$ is a complete residue system modulo $p(0)$. The polynomial p is called *basis* of this number system, $\mathcal{D}$ is called its set of *digits*.

Let $\mathcal{F}$ be a bounded fundamental domain for the action of $\mathbb{Z}^k$ on $\mathbb{R}^k$, *i.e.*, a set that satisfies $\mathbb{R}^k = \mathcal{F} + \mathbb{Z}^k$ without overlaps. Such a fundamental domain defines a set of digits in a natural way. Indeed, let $\alpha \in \mathcal{O}$ be given. Define

$$D_{\mathcal{F},\alpha} = \left\{ \tau \in \mathcal{O} \, : \, \frac{\tau}{\alpha} = \sum_{j=1}^{k} r_j \omega_j, \, (r_1, \ldots, r_k) \in \mathcal{F} \right\}. \tag{1}$$

Lemma 1. *The set $D_{\mathcal{F},\alpha}$ is a complete residue system modulo α.*

Lemma 2. *Let $(p, \mathcal{D})$ be a GNS over $\mathcal{O}$. Then there is a bounded fundamental domain $\mathcal{F}$ for the action of $\mathbb{Z}^k$ on $\mathbb{R}^k$ such that $\mathcal{D} = D_{\mathcal{F},p(0)}$.*

If the polynomial p is clear from the context we will use the abbreviation $D_{\mathcal{F},p(0)} = D_{\mathcal{F}}$.

A fixed fundamental domain $\mathcal{F}$ defines a whole class of GNS, namely,

$$\mathcal{G}_{\mathcal{F}} := \{(p, D_{\mathcal{F}}) \ : \ p \in \mathcal{O}[x]\}.$$

We consider some special choices of $\mathcal{F}$ corresponding to families $\mathcal{G}_{\mathcal{F}}$ studied in the literature.

• *Classical CNS* Let $\mathbb{K} = \mathbb{Q}$ and $\mathcal{O} = \mathbb{Z}$. Choose $\mathcal{F} = [0,1)$ which obviously is a fundamental domain of $\mathbb{Z}$ acting on $\mathbb{R}$. We look at the class $\mathcal{G}_{\mathcal{F}} := \{(p, D_{\mathcal{F}}) \,:\, p \in \mathbb{Z}[x]\}$. For an integer $\alpha \geq 2$ we have

$$D_{\mathcal{F},\alpha} = \left\{\tau \in \mathbb{Z} \,:\, \frac{\tau}{\alpha} = r, r \in [0,1)\right\} = \{0, \ldots, |\alpha| - 1\},$$

which is the digit set of a canonical number system.

If, however, $\alpha \leq -2$ then

$$D_{\mathcal{F},\alpha} = \left\{\tau \in \mathbb{Z} \,:\, \frac{\tau}{\alpha} = r, r \in [0,1)\right\} = \{\alpha+1, \ldots, 0, \} = -\{0, \ldots, |\alpha|-1\}.$$

- *Symmetric CNS* $(p, \mathcal{D})$ is a symmetric CNS if $p \in \mathbb{Z}[x]$ and

$$\mathcal{D} = \Big[-\frac{|p(0)|}{2}, \frac{|p(0)|-1}{2} \Big) \cap \mathbb{Z}.$$

These number systems were studied for instance by Akiyama and Scheicher (2007), Brunotte (2009), Kátai (1995) and Scheicher, Surer, Thuswaldner and van de Woestijne (2014). They are equal to the class $\mathcal{G}_{\mathcal{F}} := \{(p, D_{\mathcal{F}}) \ : \ p \in \mathbb{Z}[x]\}$ with $\mathcal{F} = [-\frac{1}{2}, \frac{1}{2})$ of GNS.

• *The sail* Let $\mathbb{K} = \mathbb{Q}(\sqrt{-D})$ with $D \in \{1, 2, 3, 7, 11\}$ be an Euclidean quadratic field with ring of integers $\mathcal{O}$ and set

$$\omega = \begin{cases} \sqrt{-D}, & \text{if } -D \equiv 2, 3 \pmod 4, \\ \frac{1+\sqrt{-D}}{2}, & \text{otherwise.} \end{cases}$$

Defining

$$\mathcal{F}_\omega = \left\{ (r_1, r_2) \in \mathbb{R}^2 \ : \ |r_1 + r_2\omega| < 1, |r_1 - 1 + r_2\omega| \geq 1, \ -\frac{1}{2} \leq r_2 < \frac{1}{2} \right\}$$

(this set looks a bit like a sail) one immediately checks that in Pethő and Varga (2017) the class of GNS $\mathcal{G}_\mathcal{F} := \{(p, D_\mathcal{F}) \ : \ p \in \mathcal{O}[x]\}$ with $\mathcal{F} = \mathcal{F}_\omega$ is investigated.
Using the modified fundamental domain

$$\mathcal{F}_\omega = \left\{ (r_1, r_2) \in \mathbb{R}^2 \ : \ ||(r_1, r_2)||_2 < 1, ||(r_1 - 1, r_2)||_2 \geq 1, \ -\frac{1}{2} \leq r_2 < \frac{1}{2} \right\}$$

even yields a class of GNS for any imaginary quadratic number field.

• *The square* The last example is the number systems over $\mathbb{Z}[i]$ studied by Jacob and Reveilles (1995) and Brunotte, Kirschenhofer and Thuswaldner (2011). They correspond to the class $\mathcal{G}_{\mathcal{F}} := \{(p, D_{\mathcal{F}}) : p \in \mathcal{O}[x]\}$ of GNS with $K = \mathbb{Q}(i)$, $\mathcal{O} = \mathbb{Z}[i]$, and $\mathcal{F} = [0,1)^2$.

We call $\mathbf{z}' \in \mathbb{Z}^k$ a *neighbor* of $\mathbf{z} \in \mathbb{Z}^k$ if $\mathcal{F} + \mathbf{z}$ "touches" $\mathcal{F} + \mathbf{z}'$, *i.e.*, if $(\overline{\mathcal{F}} + \mathbf{z}) \cap (\overline{\mathcal{F}} + \mathbf{z}') \neq \emptyset$. Let $\mathcal{N}$ be the set of neighbors of $\mathbf{0}$. We need the following easy result.

Lemma 3. *The set of neighbors of $\mathcal{F}$ contains a basis of the lattice $\mathbb{Z}^k$.*

Let $(p, \mathcal{D})$ be a GNS and $a \in \mathcal{O}[x]$. We say that a admits a finite digit representation if there exist $\ell \in \mathbb{N}$ and $d_0, \dots, d_{\ell-1} \in \mathcal{D}$ such that

$$a \equiv \sum_{j=0}^{\ell-1} d_j x^j \pmod{p}.$$

If $d_{\ell-1} \neq 0$ or $\ell = 0$ then ℓ is called the *length* of the representation of a. It will be denoted by $L(a)$.

Let $(p, \mathcal{D})$ be a GNS and set

$$R(p, \mathcal{D}) := \left\{ a \in \mathcal{O}[x] \, : \, a \equiv \sum_{j=0}^{\ell-1} d_j x^j \pmod{p} \text{ with } \ell \in \mathbb{N} \text{ and } d_0, \dots, d_{\ell-1} \in \mathcal{D} \right\}.$$

The GNS $(p, \mathcal{D})$ has the *finiteness property* if $R(p, \mathcal{D}) = \mathcal{O}[x]$.

Proposition 4. *Let $(p, \mathcal{D})$ be a GNS with finiteness property. Then all roots of each conjugate polynomial $p^{(j)}(x)$, $j \in \{1, \dots, k\}$, lie outside the closed unit disk.*

Proof. Basic idea: if the pair $(p, \mathcal{D})$ is a DNS with finiteness property in $\mathcal{O}[x]$ then $(p^{(j)}, \mathcal{D}^{(j)})$ is a DNS with finiteness property in $\mathcal{O}^{(j)}[x]$ for all $j = 1, \ldots, k$. If $|\alpha| < 1$ for a root of $p^{(j)}[x]$ then $\mathbb{N} \subseteq \mathcal{O}[x]$ leads to a contradiction.
If $|\alpha| = 1$ for a root of $p^{(j)}[x]$ then it is a root of unity, and this leads to a contradiction. $\square$

Adapting the proof of Akiyama and Rao (2004) or Pethő (2006) to orders one can prove the following algorithmic criterion for checking the finiteness property of a given GNS $(p, \mathcal{D})$.

Theorem 5. *Let* $\mathbb{K}$ *be a number field of degree* k *and let* $\mathcal{O}$ *be an order in* $\mathbb{K}$*. Let* $(p, \mathcal{D})$ *be a GNS over* $\mathcal{O}$*. There exists a constant* $C = C(p, \mathcal{D})$ *such that* $(p, \mathcal{D})$ *is a GNS with finiteness property if and only if the polynomial* $\prod_{i=1}^{k} p^{(i)}(x)$ *is expansive and*

$$\{a \in \mathcal{O}[x] \ : \ \deg a < \deg p \text{ and } H(a) \leq C\} \subset R(p, \mathcal{D}).$$

Theorem 5 implies that the GNS property is algorithmically decidable. Moreover it makes possible to prove a precise bound for the length of a representation in a GNS $(p, \mathcal{D})$ with finiteness property.

Theorem 6. *Let $\mathbb{K}$ be a number field of degree k and let $\mathcal{O}$ be an order in $\mathbb{K}$. Let $(p, \mathcal{D})$ be a GNS over $\mathcal{O}$. Denote by $\alpha_{i\ell}$ the zeros of $p^{(i)}(x)$, $i = 1, \ldots, k$, $\ell = 1, \ldots, \deg p$. If p is separable and $(p, \mathcal{D})$ satisfies the finiteness property then there exists a constant $C_1 = C_1(p, \mathcal{D})$ such that*

$$L(a) \leq \max\left\{\frac{\log|a^{(i)}(\alpha_{i\ell})|}{\log|\alpha_{i\ell}|} \;:\; i = 1, \ldots, k,\, \ell = 1, \ldots, \deg p\right\} + C_1$$

holds for all $a \in \mathcal{O}[x]$.

3. General criterion for the finiteness property

There exist some easy-to-state sufficient conditions for the finiteness property of a CNS $(p, \mathcal{D})$ in the case $\mathcal{O} = \mathbb{Z}$, see B. Kovács (1981), Akiyama and Pethő (2002), Scheicher and Thuswaldner (2004), or Pethő and Varga (2017).

In each of these results $|p(0)|$ dominates over the other coefficients of p. In general, $\mathcal{O}$ does not have a natural ordering. However, inclusion properties of some sets can be used to express dominance of coefficients in $\mathcal{O}$.

For $p(x) = x^n + p_{n-1}x^{n-1} + \cdots + p_0 \in \mathcal{O}[x]$ let $(p, \mathcal{D})$ be a GNS and let $\mathcal{F}$ be an associated fundamental domain. Set (letting $p_n = 1$)

$$\Delta = \left\{ \sum_{j=1}^{k} \eta_j \omega_j \ : \ (\eta_1, \ldots, \eta_k) \in \mathcal{N} \right\} \quad \text{and} \quad Z = \left\{ \sum_{j=1}^{n} \delta_j p_j \ : \ \delta_j \in \Delta \right\}, \tag{2}$$

and note that, since $\mathcal{F}$ is bounded, these sets are finite.

Theorem 7. *Let* $p(x) = x^n + p_{n-1}x^{n-1} + \cdots + p_0 \in \mathcal{O}[x]$ *and* $(p, \mathcal{D})$ *be a GNS. Let* $\mathcal{F}$ *be an associated fundamental domain and define* Δ *and* Z *as in* (2). *Assume that the following conditions hold:*

(i) $Z + \mathcal{D} \subset \bigcup_{\delta \in \Delta} (\mathcal{D} + p_0 \delta)$,

(ii) $Z \subset \mathcal{D} \cup (\mathcal{D} - p_0)$,

(iii) $\left\{ \sum_{j \in J} p_j \ : \ J \subseteq \{1, \ldots, n\} \right\} \subseteq \mathcal{D}$.

Then $(p, \mathcal{D})$ *has the finiteness property.*

Lemma 8. *Let* $(p, \mathcal{D})$ *be a GNS. The conditions*

(iv) $0 \in R(p, \mathcal{D})$,

(v) *for each* $a \in R(p, \mathcal{D})$ *and each* $\alpha \in \Delta$ *we have* $a + \alpha \in R(p, \mathcal{D})$ *are equivalent to* $(p, \mathcal{D})$ *having the finiteness property.*

Proof. Main steps:

• Observe $\{\pm\omega_1, \dots, \pm\omega_k\} \subset R(p, \mathcal{D})$, hence, by induction we have $\sum_{j=0}^{k} u_j \omega_j \in R(p, \mathcal{D})$ for all $u_j \in \mathbb{Z}$ by (iv) and (v), *i.e.*, $\mathcal{O} \subseteq R(p, \mathcal{D})$. Hence all zero degree polynomials in $\mathcal{O}[x]$ belong to $R(p, \mathcal{D})$.

• Use induction on the degree of the polynomials in $\mathcal{O}[x]$.

$\square$

Scats of the proof of Theorem 7. Lemma 8 (iv) is satisfied because $0 \in \mathcal{D}$ holds by (iii).
We derive Lemma 8 (v) from our conditions. Let $a \in R(p, \mathcal{D})$ and $\alpha \in \Delta$ be given. We have to show that $a(x) + \alpha \in R(p, \mathcal{D})$.

Since $a \in R(p, \mathcal{D})$ we may write $a(x) \equiv \sum_{j=0}^{\infty} d_j x^j \pmod{p}$ with $d_0, \ldots, d_{\ell-1} \in \mathcal{D}, d_j = 0$ for $j > \ell$. Since $\alpha + d_0 \in Z + \mathcal{D}$ (i) implies that there is $\delta_0 \in \Delta$ and $b_0 \in \mathcal{D}$ such that $\alpha + d_0 = b_0 - \delta_0 p_0$. Adding $\delta_0 p(x)$ to $a(x) + \alpha$ thus yields

$$a(x) + \alpha \equiv b_0 + \sum_{j=1}^{\infty} (d_j + \delta_0 p_j) x^j \pmod{p}. \tag{3}$$

Assume that

$$a(x)+\alpha \equiv \sum_{j=0}^{t} b_j x^j + \sum_{j=t+1}^{\infty} (d_j + \delta_0 p_j + \delta_1 p_{j-1} + \cdots + \delta_t p_{j-t}) x^j \pmod{p} \quad (4)$$

for some $t \geq 0$ with $b_j \in \mathcal{D}$ and $\delta_j \in \Delta$ for $0 \leq j \leq t$. The coefficient of x^{t+1} in (4) is $d_{t+1} + s$ with

$$s = \delta_0 p_{t+1} + \delta_1 p_t + \cdots + \delta_t p_1.$$

As $p_j = 0$ for $j > n$ the sum s has at most n nonzero summands, thus $s \in Z$ and, $d_{t+1} + s \in \mathcal{D} + Z$. Now there exists $b_{t+1} \in \mathcal{D}$ and $\delta_{t+1} \in \Delta$ such that

$$d_{t+1} + s = b_{t+1} - \delta_{t+1} p_0.$$

Adding $\delta_{t+1} p(x) x^{t+1}$ to (4) finishes the induction argument.

If $t \geq \ell - 1$ in (4). Then $d_j = 0, j \geq t + 1$ and the coefficient of x^j has the form $\delta_0 p_j + \delta_1 p_{j-1} + \cdots + \delta_t p_{j-t} \in Z$. By (ii) this implies $\delta_0 p_j + \delta_1 p_{j-1} + \cdots + \delta_t p_{j-t} \in \mathcal{D} \cup (\mathcal{D} - p_0)$. This entails that $\delta_j \in \{0, 1\}$ for $j \geq t+1$. Hence, if $t \geq \ell - 1 + n$ for each of the nonzero summands of $\delta_0 p_j + \delta_1 p_{j-1} + \cdots + \delta_t p_{j-t}$ the coefficient δ_i equals 1 and thus the sum belongs to $\mathcal{D}$ by (iii). $\square$

4. The finiteness property for large constant terms

Notations:

- $(M)_\varepsilon$ ε-neighborhood of a set $M \subset \mathbb{R}^k$,
- int$_+$ is the interior taken w.r.t. the subspace topology on $\{(r_1, \ldots, r_k) \in \mathbb{R}^k \ : \ r_1 \geq 0\}$. The symbol int$_-$ is defined by replacing $r_1 \geq 0$ with $r_1 \leq 0$.

Theorem 9. *Let* $\mathbb{K}$ *be a number field of degree* k *and let* $\mathcal{O}$ *be an order in* $\mathbb{K}$*. Let a monic polynomial* $p \in \mathcal{O}[x]$ *and a bounded fundamental domain* $\mathcal{F}$ *for the action of* $\mathbb{Z}^k$ *on* $\mathbb{R}^k$ *be given. Suppose that*

- $\mathbf{0} \in \mathrm{int}(\mathcal{F} \cup (\mathcal{F} - \mathbf{e}_1))$*, where* $\mathbf{e}_1 = (1, 0, \ldots, 0)$ *and*
- $\mathbf{0} \in \mathrm{int}_+(\mathcal{F})$*.*

Then there is $\eta > 0$ *such that* $(p(x + \alpha), D_{\mathcal{F}})$ *has the finiteness property whenever* $\alpha = m_1\omega_1 + \cdots + m_k\omega_k \in \mathcal{O}$ *satisfies* $\max\{1, |m_2|, \ldots, |m_k|\} < \eta m_1$*.*

If $\mathcal{F}$ *satisfies the conditions of Theorem 9 the set* $\{(p, \mathcal{D}_{\mathcal{F},p(0)}\}$ *contains infinitely many GNS with finiteness property.*

Scats of the proof of Theorem 9. Choose $\varepsilon > 0$ so small that $(\{\mathbf{0}\})_\varepsilon \subseteq \mathrm{int}(\mathcal{F} \cup (\mathcal{F} - \mathbf{e}_1))$ and $(\mathcal{F})_\varepsilon \cap (\mathcal{F} + \mathbf{z}) = \emptyset$ for each $\mathbf{z} \notin \mathcal{N}$.

Write $p(x+\alpha) = x^n + p_{n-1}(\alpha)x^{n-1} + \cdots + p_0(\alpha)$. Then there exist $p_{jl}(\alpha) \in \mathbb{Z}$ such that

$$p(x+\alpha) = \sum_{j=1}^{k} \Big(\delta_{j1}x^n + p_{j,n-1}(\alpha)x^{n-1} + \cdots + p_{j0}(\alpha)\Big)\,\omega_j$$

with δ_{ij} being the Kronecker symbol. It is easy to see that $p_{10}(\alpha)$ grows faster than all the other coefficients if $\eta \to 0$.

More precisely, we have

$$p_{jl}(\alpha) \ll \eta p_{10}(\alpha),\ (j,l) \neq (1,0),\ 1 \leq j \leq k,\ 0 \leq l < n. \tag{5}$$

Moreover,

$$p_{jl}(\alpha) \ll \eta p_{1l}(\alpha), \qquad 2 \leq j \leq k,\ 0 \leq l < n, \tag{6}$$

and

$$p_{1l}(\alpha) \geq 0 \tag{7}$$

for $0 \leq l < n$ and η small, i.e. if m_1 large enough.

Let now $\zeta \in Z$ be given. Then by the definition of Z the estimates in (5) imply that $\zeta = \zeta_1\omega_1 + \cdots + \zeta_k\omega_k$ with

$$\zeta_j \ll \eta p_{10}(\alpha), \quad 1 \leq j \leq k. \tag{8}$$

Next we show that $\zeta + D_{\mathcal{F}} \subset \bigcup_{\delta \in \Delta}(D_{\mathcal{F}} + p_0(\alpha)\delta)$ and $\zeta \in D_{\mathcal{F}} \cup (D_{\mathcal{F}} - p_0(\alpha))$ holds for small η.

Since $\zeta \in Z$ is arbitrary we have shown that there is $\eta_1 > 0$ with

$$Z + D_{\mathcal{F}} \subset \bigcup_{\delta \in \Delta} (D_{\mathcal{F}} + p_0(\alpha)\delta) \qquad \text{for } \eta < \eta_1 \tag{9}$$

and

$$Z \subset D_{\mathcal{F}} \cup (D_{\mathcal{F}} - p_0(\alpha)) \qquad \text{for } \eta < \eta_1. \tag{10}$$

This implies conditions (i) and (ii) of Theorem 7.

If we choose $\zeta' = \sum_{j \in J} p_j(\alpha)$ for some $J \subseteq \{1, \ldots, n\}$, there exist $r'_1, \ldots, r'_k \in \mathbb{Q}$ with

$$\frac{\zeta'}{p_0(\alpha)} = r'_1\omega_1 + \cdots + r'_k\omega_k.$$

and, hence, writing $\zeta' = \zeta'_1\omega_1 + \cdots + \zeta'_k\omega_k$, we get

$$\zeta'_1\omega_1 + \cdots + \zeta'_k\omega_k = (r'_1\omega_1 + \cdots + r'_k\omega_k)(p_{10}(\alpha)\omega_1 + \cdots + p_{k0}(\alpha)\omega_k). \tag{11}$$

Then we derive

$$||(r'_1, \ldots, r'_k)||_\infty < \varepsilon \qquad \text{for } \eta \text{ small enough.} \tag{12}$$

Observing that

$$\zeta'_j \ll \eta\zeta'_1 \qquad (2 \leq j \leq k) \tag{13}$$

and $\zeta'_1 > 0$ for $\eta \to 0$ we can conclude

$$r'_1 > 0 \qquad \text{for } \eta \text{ small enough.} \tag{14}$$

Thus there is $\eta_2 > 0$ with

$$\left\{ \sum_{j \in J} p_j(\alpha) \ : \ J \subseteq \{1, \ldots, n\} \right\} \subseteq D_{\mathcal{F}} \qquad \text{for } \eta < \eta_2. \tag{15}$$

This shows that also condition (iii) of Theorem 7 is stisfied.

Summing up we see that Theorem 7 holds with $\eta = \min\{\eta_1, \eta_2\}$.

$\square$

Theorem 9 immediately admits the following corollary.

Corollary 10. *Let $\mathbb{K}$ be a number field of degree k and let $\mathcal{O}$ be an order in $\mathbb{K}$. Let a monic polynomial $p \in \mathcal{O}[x]$ and a bounded fundamental domain $\mathcal{F}$ for the action of $\mathbb{Z}^k$ on $\mathbb{R}^k$ be given. If $\mathbf{0} \in \mathrm{int}(\mathcal{F})$ then there is $\eta > 0$ such that $(p(x+\alpha), D_{\mathcal{F}})$ has the finiteness property whenever $\alpha = m_1\omega_1 + \cdots + m_k\omega_k \in \mathcal{O}$ satisfies $\max\{1, |m_2|, \ldots, |m_k|\} < \eta |m_1|$.*

Under the conditions of Theorem 9

$\exists\, M \in \mathbb{N}:\ (p(x{+}m), \mathcal{F})$ *is a GNS with finiteness property for* $m \geq M$,

while under the more restrictive conditions of Corollary 10

$\exists\, M \in \mathbb{N}:\ (p(x{\pm}m), \mathcal{F})$ *is a GNS with finiteness property for* $m \geq M$.

The next Corollary answers partially a question of Akiyama.

Corollary 11. *Let* $\mathbb{K}$ *be a number field of degree* k *and let* $\mathcal{O}$ *be an order in* $\mathbb{K}$*. Let a monic polynomial* $p \in \mathcal{O}[x]$ *and a bounded fundamental domain* $\mathcal{F}$ *for the action of* $\mathbb{Z}^k$ *on* $\mathbb{R}^k$ *be given. Suppose that* $\mathbf{0} \in \operatorname{int}(\mathcal{F})$ *then there is* $\eta > 0$ *such that* $(p(x) \pm \alpha, D_{\mathcal{F}})$ *has the finiteness property whenever* $\alpha = m_1\omega_1 + \cdots + m_k\omega_k \in \mathcal{O}$ *satisfies* $\max\{1, |m_2|, \ldots, |m_k|\} < \eta|m_1|$*.*

If $k=1$*, and* $0<\varepsilon<1$ *then* $\mathcal{F}_\varepsilon=[-\varepsilon,1-\varepsilon)$ *satisfies the conditions of Corollary 11, hence for any* $p\in\mathbb{Z}[x]$ *there exists* $M\in\mathbb{Z}$ *such that* $(p(x)\pm m,\mathcal{F}_\varepsilon)$ *is a GNS with finiteness property in* $\mathbb{Z}[x]$*.*

The assumptions of Theorem 9 hold for $\mathcal{F}_\varepsilon$ *even if* $\varepsilon=0$*. Hence, if all coefficients of* p *are non-negative, then we can conclude* $(p(x)+m,\mathcal{F}_0)$ *is a GNS with finiteness property in* $\mathbb{Z}[x]$*.*

However, if some of the coefficients of p *are negative, then our method fails and, we do not have similar statement. The example* $p=x^2-2x+2$ *shows that* $(p(x)+m,\mathcal{F}_0)$ *is not a GNS with finiteness property in* $\mathbb{Z}[x]$ *for any* $m\geq 0$*.*

If there are infinitely many units in $\mathcal{O}$ then for all $p \in \mathcal{O}[x]$ there exist infinitely many $\alpha \in \mathcal{O}$ such that the constant term of $p(x)+\alpha$, i.e., $p(0)+\alpha$ is a unit, hence $p(x)+\alpha$ is not GNS with finiteness property. Notice that Condition (iii) of Theorem 7 holds under the assumptions of Corollary 11 only if the norm of $p(0)+\alpha$ is large.

5. GNS without finiteness property

We start with a partial generalization of a Theorem of Kovács and Pethő (1991) to polynomials with coefficients of $\mathcal{O}$.

Lemma 12. *Let $(p, \mathcal{D})$ be a GNS. If there exist $h \in \mathbb{N}$, $d_0, d_1, \ldots, d_{h-1} \in \mathcal{D}$ not all equal to 0 and $q_1, q_2 \in \mathcal{O}[x]$ with*

$$\sum_{j=0}^{h-1} d_j x^j = (x^h - 1) q_1(x) + q_2(x) p(x). \tag{16}$$

then $(p, \mathcal{D})$ doesn't have the finiteness property.

Our main result in this section is the following theorem.

Theorem 13. *Let* $\mathbb{K}$ *be a number field of degree* k *and let* $\mathcal{O}$ *be an order in* $\mathbb{K}$. *Let a monic polynomial* $p \in \mathcal{O}[x]$ *and a bounded fundamental domain* $\mathcal{F}$ *for the action of* $\mathbb{Z}^k$ *on* $\mathbb{R}^k$ *be given. Suppose that* $\mathbf{0} \in \mathrm{int}_{-}(\mathcal{F} - \mathbf{e}_1)$. *There exists* $M \in \mathbb{N}$ *such that* $(p(x-m), D_{\mathcal{F}})$ *doesn't have the finiteness property for* $m \geq M$.

Scats of the proof of Theorem 13. For an integer m set $\Pi_m(x) = p(x-m)$. We examine the constant term of $\Pi_m(x)$. We claim that if m is large enough then $\Pi_m(0) = p(-m) \in D_{\mathcal{F},p(-m-1)}$.

Assume that our claim is true. Performing Euclidean division of $\Pi_{m+1}(x)$ by $(x-1)$ we obtain $s_{m+1}(x) \in \mathcal{O}[x]$ such that

$$\Pi_{m+1}(x) = (x-1)s_{m+1}(x) + \Pi_{m+1}(1).$$

As $\Pi_{m+1}(1) = p(-m)$ the last identity is equivalent to

$$p(-m) = (x-1)(-s_{m+1}(x)) + \Pi_{m+1}(x).$$

By the claim $p(-m) \in D_{\mathcal{F},p(-m-1)}$ if m is large enough. Applying Lemma 12 we conclude that $(\Pi_{m+1}, D_{\mathcal{F},p(-m-1)})$ is not a GNS with finiteness property whenever m is large enough.

Let $p(x) = x^n + p_{n-1}x^{n-1} + \cdots + p_0$. Then

$$\frac{\Pi_m^{(i)}(0)}{\Pi_{m+1}^{(i)}(0)} = 1 - \frac{n}{m} + O(m^{-2}),\ i = 1, \ldots, k. \tag{17}$$

We have on the other hand

$$\frac{\Pi_m^{(i)}(0)}{\Pi_{m+1}^{(i)}(0)} = \sum_{j=1}^{k} r_{mj}\omega_j^{(i)},\ i = 1, \ldots, k. \tag{18}$$

This is a system of linear equations in the unknowns $r_{mj} \in \mathbb{Q}, j = 1, \ldots, k$ with coefficient matrix $(\omega_j^{(i)})_{i,j=1,\ldots,k}$.

Using Cramer's rule we get

$$r_{mj} = O(m^{-1}),\ j = 2, \ldots, k. \tag{19}$$

and

$$r_{m1} = 1 - \frac{n}{m} + O(m^{-2}).$$

This yields that

$$1 - \frac{n}{2m} < r_{m1} < 1 \tag{20}$$

holds for m large, and the claim is proved. $\square$

6. GNS in number fields

Let $\alpha \in \mathcal{O}_{\mathbb{L}}$ and let $\mathcal{N}$ be a complete residue system modulo α. The pair $(\alpha, \mathcal{N})$ is called a *number system in* $\mathcal{O}_{\mathbb{L}}$. If for each $\gamma \in \mathcal{O}_{\mathbb{L}}$ there exist integers $\ell \geq 0$, $d_0, \ldots, d_{\ell-1} \in \mathcal{N}$ such that

$$\gamma = \sum_{j=0}^{\ell-1} d_j \alpha^j$$

then we say that $(\alpha, \mathcal{N})$ has the *finiteness property*. If the digit set is chosen to be $\mathcal{N} = \{0, 1, \ldots, |N_{\mathbb{L}/\mathbb{Q}}(\alpha)| - 1\}$ then $(\alpha, \mathcal{N})$ is called a *canonical number system in* $\mathcal{O}_{\mathbb{L}}$.

Kovács (1981) proved that there exists a canonical number system with finiteness property in $\mathcal{O}_{\mathbb{L}}$ if and only if $\mathcal{O}_{\mathbb{L}}$ admits a power integral bases. Later Kovács and Pethő (1991) proved the stronger result.

Proposition 14. *Let $\mathcal{O}$ be an order in the algebraic number field $\mathbb{L}$. There exist $\alpha_1, \ldots, \alpha_t \in \mathcal{O}$, $n_1, \ldots, n_t \in \mathbb{Z}$, and $N_1, \ldots, N_t$ finite subsets of $\mathbb{Z}$, which are all effectively computable, such that $(\alpha, \mathcal{N}(\alpha))$ is a canonical number system with finiteness property in $\mathcal{O}$ if and only if $\alpha = \alpha_i - h$ for some integers i, h with $1 \leq i \leq t$ and either $h \geq n_i$ or $h \in N_i$.*

From Corollary 10 we derive that for number systems the relation is usually stronger, the theorem of Kovács and Pethő describes a kind of "boundary case" *viz.* a case where $0 \in \partial\mathcal{F}$.

Theorem 15. *Let $\mathbb{L}$ be a number field of degree l and let $\mathcal{O}$ be an order in $\mathbb{L}$. Let $\mathcal{F}$ be a bounded fundamental domain for the action of $\mathbb{Z}$ on $\mathbb{R}$. If $0 \in \mathrm{int}(\mathcal{F})$ then all but finitely many generators of power integral bases of $\mathcal{O}$ form a basis for a number system with finiteness property. Moreover, the exceptions are effectively computable.*

The proof combines a deep result of Győry (1978) with Corollary 10.

The assumption $0 \in \mathrm{int}(\mathcal{F})$ *implies that* $\{-1, 0, 1\} \subseteq D_{\mathcal{F}, p_j(\delta m)}$ *for all* m *large enough. Of course* $-1 \notin \mathcal{N}_0(\alpha + m)$*, hence, the proof of Theorem 15 does not work in the case of canonical number systems. Győry's theorem holds for relative extensions as well. To generalize Theorem 15 to this situation would require the generalization of Corollary 10 to all* $m \in \mathcal{O}$*, such that all conjugates of* m *are large enough. We have no idea how to prove such a result.*

Thank you for your attention!