Number systems over general orders

Evertse, J.H.; Győry, K.; Pethö, A.; Thuswaldner, J.M.

Acta Math. Hungar., **159** (**1**) (2019), 187–205
https://doi.org/10.1007/s10474-019-00958-x
First published online June 25, 2019

NUMBER SYSTEMS OVER GENERAL ORDERS

J.-H. EVERTSE[1], K. GYŐRY[2,*,†], A. PETHŐ[3,4,‡] and J. M. THUSWALDNER[5,§]

[1]Mathematical Institute, Leiden University, P.O. Box 9512, 2300 RA Leiden, The Netherlands
e-mail: evertse@math.leidenuniv.nl

[2]Institute of Mathematics, University of Debrecen, P.O. Box 400, H-4002 Debrecen, Hungary
e-mail: gyory@science.unideb.hu

[3]Department of Computer Science, University of Debrecen, P.O. Box 12, H-4010 Debrecen, Hungary

[4]Faculty of Science, University of Ostrava, Dvořákova 7, 70103 Ostrava, Czech Republic
e-mail: Petho.Attila@inf.unideb.hu

[5]Chair of Mathematics and Statistics, University of Leoben, Franz-Josef-Strasse 18, A-8700 Leoben, Austria
e-mail: Joerg.Thuswaldner@unileoben.ac.at

(Received September 28, 2018; revised April 11, 2019; accepted April 13, 2019)

Abstract. Let $\mathcal{O}$ be an order, that is a commutative ring with 1 whose additive structure is a free $\mathbb{Z}$-module of finite rank. A *generalized number system* (GNS for short) over $\mathcal{O}$ is a pair $(p, \mathcal{D})$ where $p \in \mathcal{O}[x]$ is monic with constant term $p(0)$ not a zero divisor of $\mathcal{O}$, and where $\mathcal{D}$ is a complete residue system modulo $p(0)$ in $\mathcal{O}$ containing 0. We say that $(p, \mathcal{D})$ is a GNS over $\mathcal{O}$ with the finiteness property if all elements of $\mathcal{O}[x]/(p)$ have a representative in $\mathcal{D}[x]$ (the polynomials with coefficients in $\mathcal{D}$). Our purpose is to extend several of the results from a previous paper of Pethő and Thuswaldner, where GNS over orders of number fields were considered. We prove that it is algorithmically decidable whether or not for a given order $\mathcal{O}$ and GNS $(p, \mathcal{D})$ over $\mathcal{O}$, the pair $(p, \mathcal{D})$ admits the finiteness property. This is closely related to work of Vince on matrix number systems.

Let $\mathcal{F}$ be a fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$ and $p \in \mathcal{O}[X]$ a monic polynomial. For $\alpha \in \mathcal{O}$, define $p_\alpha(x) := p(x + \alpha)$ and $\mathcal{D}_{\mathcal{F},p(\alpha)} := p(\alpha)\mathcal{F} \cap \mathcal{O}$. Under mild conditions we show that the pairs $(p_\alpha, \mathcal{D}_{\mathcal{F},p(\alpha)})$ are GNS over $\mathcal{O}$ with finiteness property provided $\alpha \in \mathcal{O}$ in some sense approximates a sufficiently large positive rational integer. In the opposite direction we prove under different conditions that $(p_{-m}, \mathcal{D}_{\mathcal{F},p(-m)})$ does not have the finiteness property for each large enough positive rational integer m.

We obtain important relations between power integral bases of étale orders and GNS over $\mathbb{Z}$. Their proofs depend on some general effective finiteness results of Evertse and Győry on monogenic étale orders.

* Corresponding author.

† Research of K. Gy. was supported in part by the OTKA grant NK115479.

‡ Research of A. P. was supported in part by the grant no. 17-02804S of the Czech Grant Agency.

§ Research of J. T. was supported by the FWF grants P27050 and P29910.

Key words and phrases: number system, order, tiling.

Mathematics Subject Classification: 11A63, 11R04.

1. Introduction

Decimal and sexagesimal representations of the positive integers have been used since the times of antiquity. A computer's "native language" consists of the binary strings, which can be interpreted among others as binary representations of integers. Starting with the pioneering work of V. Grünwald [5] many generalizations have been established. For an overview we refer to the papers [1,11] and to the book [4].

In the present paper, $\mathcal{O}$ will denote an order, that is a commutative ring with 1 whose additive group is free abelian of finite rank. We identify $m \in \mathbb{Z}$ with $m \cdot 1$, and thus assume $\mathbb{Z} \subset \mathcal{O}$. The order $\mathcal{O}$ may be given explicitly by a basis $\{1 = \omega_1, \omega_2, \dots, \omega_d\}$ and a multiplication table

$$\omega_i \omega_j = \sum_{l=1}^{d} a_{ijl} \omega_l \quad (i, j = 2, \dots, d) \quad \text{with } a_{ijl} \in \mathbb{Z}, \tag{1.1}$$

satisfying the commutativity and associativity rules. A *generalized number system* over $\mathcal{O}$ (GNS over $\mathcal{O}$ for short) is a pair $(p, \mathcal{D})$, where $p \in \mathcal{O}[x]$ is a monic polynomial such that $p(0)$ is not a zero divisor of $\mathcal{O}$, and where $\mathcal{D}$ is a (necessarily finite) complete residue system of $\mathcal{O}$ modulo $p(0)$ containing 0.

An element $a \in \mathcal{O}[x]$ is *representable in* $(p, \mathcal{D})$ if there exist an integer $L \geq 0$ and $a_0, \dots, a_L \in \mathcal{D}$ such that

$$a \equiv \sum_{j=0}^{L} a_j x^j \pmod{p}, \tag{1.2}$$

i.e., if there is $q \in \mathcal{O}[x]$ such that $a + qp$ has its coefficients in $\mathcal{D}$. Our condition that $p(0)$ not be a zero divisor of $\mathcal{O}$ implies that a representation of $a \pmod{p}$ as in (1.2), if it exists, is unique (except for "leading zeros"). If all $a \in \mathcal{O}[x]$ are representable in $(p, \mathcal{D})$, then $(p, \mathcal{D})$ is called a GNS with the *finiteness property*. This concept was introduced for $\mathcal{O} = \mathbb{Z}$ by Pethő [10] and extended to orders $\mathcal{O}$ in number fields by Pethő and Thuswaldner [11].

GNS over orders may be viewed as special cases of *matrix number systems*, which were introduced by Vince [13]. A matrix number system is a triple (Λ, φ, D), consisting of a free abelian group Λ of finite rank, an injective homomorphism $\varphi\colon \Lambda \to \Lambda$, and a complete residue system D for $\Lambda/\varphi(\Lambda)$ with $0 \in D$. Then a GNS $(p, \mathcal{D})$ over $\mathcal{O}$ may be viewed as a matrix number system with $\Lambda = \mathcal{O}[x]/(p)$, $\varphi\colon f \pmod{p} \mapsto x \cdot f \pmod{p}$, and $D = \mathcal{D}$.

We briefly recall some of the results from the paper [11] of Pethő and Thuswaldner, but reformulate them in terms of the language of the present paper. Let $\mathcal{O}$ be an order of a number field. We embed $\mathcal{O}$ in the $\mathbb{R}$-algebra $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ and view $\mathcal{O}$ as a full rank sublattice of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$. The real innovation of [11] is to consider parametrized classes of GNS over $\mathcal{O}$ determined

by a monic polynomial $p \in \mathcal{O}[x]$ and a fundamental domain $\mathcal{F}$ of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$ with $0 \in \mathcal{F}$, i.e., $\mathcal{F}$ is a subset of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ consisting of precisely one element from every residue class of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ modulo $\mathcal{O}$. More precisely, one considers GNS of the type $(p_\alpha, \mathcal{D}_{\mathcal{F},p(\alpha)})$ $(\alpha \in \mathcal{O})$, where $p_\alpha(x) := p(x+\alpha)$ and $\mathcal{D}_{\mathcal{F},\vartheta} := \vartheta\mathcal{F} \cap \mathcal{O}$ for a non-zero element ϑ of $\mathcal{O}$. In their paper, Pethő and Thuswaldner proved that it is algorithmically decidable whether a given GNS $(p, \mathcal{D})$ over $\mathcal{O}$ has the finiteness property. Under mild conditions on $\mathcal{F}$ they were able to prove that $(p_\alpha, \mathcal{D}_{\mathcal{F},p(\alpha)})$ is a GNS with the finiteness property provided that there is a large positive rational integer m such that $m^{-1}\alpha$ is close to 1 (with respect to any vector norm on $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$). Under different conditions on $\mathcal{F}$ they proved that $(p_{-m}, \mathcal{D}_{\mathcal{F},p(-m)})$ does not have the finiteness property if m is a sufficiently large positive rational integer. These are far reaching generalizations of results of Kovács and Pethő [9]. The purpose of the present paper is to extend the results mentioned above from GNS over orders of number fields to GNS over arbitrary orders. In particular, that for a given GNS the finiteness property is effectively decidable is an easy consequence of general work of Vince [13] on matrix number systems.

Outline of the paper. Let $\mathcal{O}$ be an arbitrary order. In Section 2 we show that the finiteness property of a given GNS $(p, \mathcal{D})$ over $\mathcal{O}$ is effectively decidable by applying some of Vince's results on matrix number systems [13]. In Section 3 we define the digit sets $\mathcal{D}_{\mathcal{F},\vartheta}$ using fundamental domains $\mathcal{F}$ of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$ and prove a sufficient condition for a GNS over $\mathcal{O}$ to admit the finiteness property (cf. Theorem 3.4). In Section 4 we prove that if $p \in \mathcal{O}[x]$ and the fundamental domain $\mathcal{F}$ satisfies some mild condition then the pairs $(p_\alpha, \mathcal{D}_{\mathcal{F},p(\alpha)})$ are always GNS with the finiteness property provided that there is a large positive rational integer m such that $m^{-1}\alpha$ is close to 1 (this is the content of Theorem 4.1).

Section 5 is devoted to GNS without the finiteness property. The main result is Theorem 5.2 which states that $(p_{-m}, \mathcal{D}_{\mathcal{F},p(-m)})$ does not have the finiteness property for all large enough positive rational integers m.

Using some general effective finiteness results of Evertse and Győry [4, Corollary 8.4.7] on monogenic orders in étale algebras (cf. also Proposition 6.1 in Section 6 below), we obtain important relations between power integral bases and number systems in étale orders (see Theorem 6.2), which in turn can be interpreted as GNS over $\mathbb{Z}$.

2. Connection with matrix number systems

Recall that a matrix number system is a triple (Λ, φ, D), consisting of a free abelian group Λ of finite rank, an injective $\mathbb{Z}$-linear homomorphism $\varphi\colon \Lambda \to \Lambda$, and a complete residue system D for $\Lambda/\varphi(\Lambda)$, containing $\mathbf{0}$. The rank of this matrix number system is the rank of Λ, and its determinant is the cardinality of $\Lambda/\varphi(\Lambda)$ (which is equal to the absolute value of the

determinant of φ). Denote by χ_φ the characteristic polynomial of φ, i.e., $\det(x \cdot \mathrm{id} - \varphi)$. This characteristic polynomial is monic of degree equal to the rank of Λ, with coefficients in $\mathbb{Z}$ and non-zero constant term $\pm \det \varphi$.

We say that (Λ, φ, D) has the finiteness property if every $\mathbf{v} \in \Lambda$ can be expressed as a finite sum $\sum_{i=0}^{L} \varphi^i \mathbf{d}_i$, with $\mathbf{d}_i \in D$ for $i = 0, \ldots, L$. Such systems were introduced by Vince [13] (he used a different terminology). We recall some of Vince's results.

Let (Λ, φ, D) be a matrix number system. Here, and similarly in other situations below, we identify elements of Λ with their images in the real vector space $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ under the canonical embedding. Thus, we view Λ as a lattice (discrete subgroup of maximal rank) in $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$, and if $\{\mathbf{a}_1, \ldots, \mathbf{a}_d\}$ is a $\mathbb{Z}$-basis of Λ, it is also an $\mathbb{R}$-vector space basis of $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$. We endow $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ with a vector norm $\| \cdot \|$; this induces a norm on Λ.

PROPOSITION 2.1 (Vince [13, p. 508, Proposition 4]). *Assume that (Λ, φ, D) has the finiteness property. Then χ_φ is expansive, i.e., all its complex roots have absolute value > 1.*

Assume henceforth that χ_φ is expansive. For $\mathbf{v} \in \Lambda$, we define the sequences $(\mathbf{v}_i)_{i=0}^{\infty}$ in Λ and $(\mathbf{d}_i)_{i=0}^{\infty}$ in D inductively by

$$\mathbf{v}_0 := \mathbf{v};$$

$$\mathbf{d}_i \in D \text{ is the representative of } \mathbf{v}_i (\mathrm{mod}\ \varphi(\Lambda)),$$

$$\mathbf{v}_{i+1} := \varphi^{-1}(\mathbf{v}_i - \mathbf{d}_i) \quad (i = 0, 1, 2, \ldots).$$

In an appropriate completion of Λ we can now write $\mathbf{v} = \sum_{i=0}^{\infty} \varphi^i \mathbf{d}_i$ and call this the (φ, D)-expansion of $\mathbf{v}$. Vince [13, p. 511 Algorithm A and p. 512, Lemma 2] observes that there is an effectively computable number $C > 0$ depending on $\Lambda, \varphi, D, \mathbf{v}$ such that $\|\mathbf{v}_i\| \le C$ for all i. This implies that the sequences $(\mathbf{v}_i)_{i=0}^{\infty}$ and $(\mathbf{d}_i)_{i=0}^{\infty}$ are ultimately periodic, where for both sequences the sum of the lengths of the preperiod and period is bounded above by the number R of points in Λ of norm at most C. Further, it is clear that $\mathbf{v}$ has a finite (φ, D)-expansion $\mathbf{v} = \sum_{i=0}^{L} \varphi^i \mathbf{d}_i$ if and only if $\mathbf{v}_i = \mathbf{d}_i = \mathbf{0}$ for $i > L$. So we may take $L < R$. This shows that for given $\mathbf{v} \in \Lambda$, we can effectively decide whether it has a finite (φ, D)-expansion, and if such an expansion exists, it has length $\le R$.

The following result implies that it can be effectively decided whether (Λ, φ, D) has the finiteness property.

PROPOSITION 2.2 (Vince [13, p. 513, Theorem 4]). *Let (Λ, φ, D) be a matrix number system. There is an effectively computable number $C' > 0$ depending on Λ, φ, D such that the following are equivalent*:

(i) *(Λ, φ, D) has the finiteness property*;

(ii) χ_φ *is expansive, and every* $\mathbf{v} \in \Lambda$ *with* $\|\mathbf{v}\| \le C'$ *has a finite* (φ, D)*-expansion.*

We now specialize the above to generalized number systems. Let $\mathcal{O}$ be an order, and $(p, \mathcal{D})$ a GNS over $\mathcal{O}$.

Let $\mathcal{D}[x]$ denote the set of polynomials with coefficients in $\mathcal{D}$, and $R(p, \mathcal{D})$ the set of $a \in \mathcal{O}[x]$ such that $a \equiv b \pmod p$ for some $b \in \mathcal{D}[x]$.

With the usual identification of an element of $\mathcal{O}$ with its canonical image in the $\mathbb{R}$-algebra $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$, we view $\mathcal{O}$ as a full rank lattice in $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$.

We endow the $\mathbb{R}$-algebra $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ with a vector norm $\|\cdot\|$. For instance, fixing a $\mathbb{Z}$-module basis $\{1 = \omega_1, \omega_2, \dots, \omega_d\}$ of $\mathcal{O}$, we can express every $\alpha \in \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ as $\sum_{i=1}^d x_i \omega_i$ for some $x_1, \dots, x_d \in \mathbb{R}$ and we may take $\|\alpha\| := \max_i |x_i|$. The elements of $\mathcal{O}$ are those with $x_1, \dots, x_d \in \mathbb{Z}$, hence for given C, the set of $\alpha \in \mathcal{O}$ with $\|\alpha\| \le C$ is finite and effectively determinable. But in what follows the choice of norm does not matter. We define the norm $\|a\|$ of $a \in \mathcal{O}[x]$ to be the maximum of the norms of its coefficients.

As already mentioned in Section 1, we can view the GNS $(p, \mathcal{D})$ as a matrix number system (Λ, φ, D), where $\Lambda = \mathcal{O}[x]/(p)$, $\varphi\colon f \pmod p \mapsto x \cdot f \pmod p$ and $D = \mathcal{D}$. To see this, observe that $\Lambda/\varphi(\Lambda) \cong \mathcal{O}[x]/(p, x) \cong \mathcal{O}/p(0)\mathcal{O}$, so that indeed $\mathcal{D}$ is a complete residue system for $\Lambda/\varphi(\Lambda)$. Further, one easily verifies that a congruence $a \equiv \sum_{i=0}^L d_i x^i \pmod p$ translates into $a \pmod p = \sum_{i=0}^L \varphi^i d_i$. Using what we observed above for matrix number systems, this shows that for given $a \in \mathcal{O}[x]$ it can be decided effectively whether it has a finite expansion $\sum_{i=0}^L d_i x^i \pmod p$. Further, $(p, \mathcal{D})$ has the finiteness property if and only if $(\Lambda, \varphi, \mathcal{D})$ has the finiteness property.

We may view $\mathcal{O}[x]$ as a free $\mathbb{Z}[x]$-module of finite rank, and $a \mapsto p \cdot a$ as a $\mathbb{Z}[x]$-linear map from $\mathcal{O}[x]$ to itself. The determinant of this $\mathbb{Z}[x]$-linear map is a monic polynomial in $\mathbb{Z}[x]$, which we denote by Np.

LEMMA 2.3. $Np = \chi_\varphi$.

PROOF. Let $d = \operatorname{rank} \mathcal{O}$, $n = \deg p$. Pick a $\mathbb{Z}$-basis $1 = \omega_1, \omega_2, \dots, \omega_d$ of $\mathcal{O}$. Let $p = x^n + p_{n-1}x^{n-1} + \cdots + p_0$. For $i = 0, \dots, n-1$, let P_i be the matrix of the $\mathbb{Z}$-linear map $\alpha \mapsto p_i\alpha$ from $\mathcal{O}$ to $\mathcal{O}$ with respect to the basis of $\mathcal{O}$ just chosen. Clearly, $\{\omega_i x^j : i = 1, \dots, d,\ j = 0, \dots, n-1\}$ is a $\mathbb{Z}$-basis of $\Lambda = \mathcal{O}[x]/(p)$. A straightforward computation shows that the matrix of φ with respect to this basis is

$$\begin{pmatrix} 0 & \cdots & 0 & -P_0 \\ I & & 0 & -P_1 \\ & \ddots & & \vdots \\ 0 & & I & -P_{n-1} \end{pmatrix},$$

where each entry represents a $d \times d$ integer matrix and I denotes the identity matrix of order d. Hence

$$\chi_\varphi = \begin{vmatrix} xI & & & P_0 \\ -I & xI & & P_1 \\ & \ddots & & \vdots \\ & & -I & xI + P_{n-1} \end{vmatrix} = \begin{vmatrix} 0 & \cdots & 0 & x^n I + x^{n-1} P_{n-1} + \cdots + P_0 \\ -I & & 0 & * \\ & \ddots & & \vdots \\ 0 & & -I & * \end{vmatrix}$$

$$= \det(x^n I + x^{n-1} P_{n-1} + \cdots + x P_1 + P_0) = Np. \quad \square$$

Using division with remainder, it follows that every element of $\Lambda = \mathcal{O}[x]/(p)$ can be represented by a polynomial in $\mathcal{O}[x]$ of degree $< n$. Using this and Lemma 2.3, the following effective finiteness criterion for a GNS having the finiteness property is a straightforward translation of Proposition 2.2.

THEOREM 2.4. *Let $(p, \mathcal{D})$ be a GNS over $\mathcal{O}$ with $\deg p = n \geq 1$. Then there is an effectively computable number C'', depending on $\mathcal{O}$, p and $\mathcal{D}$, such that the following are equivalent*:

(i) *$(p, \mathcal{D})$ has the finiteness property*;

(ii) *the polynomial Np is expansive, and every $a \in \mathcal{O}[x]$ with $\|a\| \leq C''$, $\deg a < n$ belongs to $R(p, \mathcal{D})$.*

If $\mathcal{O}$ is an order in a number field K, $p = x^n + p_{n-1}x^{n-1} + \cdots + p_0 \in \mathcal{O}[x]$, and $\alpha \mapsto \alpha^{(i)}$ $(i = 1, \ldots, d)$ are the embeddings of K in $\mathbb{C}$, then $Np = \prod_{i=1}^{d}(x^n + p_{n-1}^{(i)}x^{n-1} + \cdots + p_0^{(i)})$. Thus Theorem 2.4 is a generalization of Theorem 2.9 of Pethő and Thuswaldner [11].

3. Digit sets defined by fundamental domains

Let $\mathcal{O}$ be an order of rank d. We view $\mathcal{O}$ as a full rank sublattice of the $\mathbb{R}$-algebra $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$. We frequently use the simple fact that an element $\vartheta \in \mathcal{O}$ is not a zero divisor of $\mathcal{O}$ if and only if it is invertible in $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ (consider the map $\alpha \mapsto \vartheta\alpha$).

Recall that a fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$ is a subset of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ containing precisely one element from every residue class of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ modulo $\mathcal{O}$. For a fundamental domain $\mathcal{F}$ for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$ with $0 \in \mathcal{F}$ and $\vartheta \in \mathcal{O}$ which is not a zero divisor, we define

$$\mathcal{D}_{\mathcal{F},\vartheta} := \vartheta\mathcal{F} \cap \mathcal{O} = \left\{ \alpha \in \mathcal{O} : \vartheta^{-1}\alpha \in \mathcal{F} \right\}.$$

The following two lemmas are easy generalizations of [11, Lemmas 2.3, 2.4].

LEMMA 3.1. *Let $\mathcal{F}$ be a fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$ with $0 \in \mathcal{F}$ and $\vartheta \in \mathcal{O}$ not a zero divisor. Then $\mathcal{D}_{\mathcal{F},\vartheta}$ is a complete residue system for $\mathcal{O}$ modulo ϑ containing* 0.

PROOF. Let $\alpha \in \mathcal{O}$. Then $\vartheta^{-1}\alpha = \xi + \beta$ with $\xi \in \mathcal{F}$ and $\beta \in \mathcal{O}$. Thus, $\alpha = \vartheta\xi + \vartheta\beta$ with $\vartheta\xi \in \mathcal{D}_{\mathcal{F},\vartheta}$. If δ_1, δ_2 are two elements of $\mathcal{D}_{\mathcal{F},\vartheta}$ with $\delta_1 - \delta_2 \in \vartheta\mathcal{O}$, then $\vartheta^{-1}\delta_1, \vartheta^{-1}\delta_2$ are elements of $\mathcal{F}$ whose difference lies in $\mathcal{O}$, so $\delta_1 = \delta_2$. This proves Lemma 3.1. □

LEMMA 3.2. *Let $\vartheta \in \mathcal{O}$ not be a zero divisor and let $\mathcal{D}$ be a complete residue system for $\mathcal{O}$ modulo ϑ with $0 \in \mathcal{D}$. Then there is a bounded fundamental domain $\mathcal{F}$ of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$ such that $\mathcal{D} = \mathcal{D}_{\mathcal{F},\vartheta}$.*

PROOF. Let $1 = \omega_1, \omega_2, \ldots, \omega_d$ be a $\mathbb{Z}$-basis of $\mathcal{O}$, and set $\mathcal{G} := \{u_1\vartheta^{-1}\omega_1 + \cdots + u_d\vartheta^{-1}\omega_d : 0 \le u_j < 1,\ j = 1, \ldots d\}$. Then $\mathcal{G}$ is a bounded fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\vartheta^{-1}\mathcal{O}$ with $0 \in \mathcal{G}$. The set

$$\mathcal{F} := \bigcup_{\delta \in \mathcal{D}} (\vartheta^{-1}\delta + \mathcal{G})$$

is obviously bounded. We see that it satisfies the other requirements of the lemma. First observe that

$$\mathcal{D}_{\mathcal{F},\vartheta} = \vartheta\mathcal{F} \cap \mathcal{O} = \bigcup_{\delta \in \mathcal{D}} (\delta + \vartheta\mathcal{G}) \cap \mathcal{O} = \mathcal{D},$$

for $(\delta + \vartheta\mathcal{G}) \cap \mathcal{O} = \{\delta\}$ for every $\delta \in \mathcal{O}$ since $\vartheta\mathcal{G}$ is a fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$ containing 0.

It remains to show that $\mathcal{F}$ is a fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$. We can express any $\eta \in \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ as $\eta = \xi + \vartheta^{-1}\alpha$ with $\xi \in \mathcal{G}$, $\alpha \in \mathcal{O}$, and we have $\alpha = \delta + \vartheta\beta$ with $\delta \in \mathcal{D}$, $\beta \in \mathcal{O}$, thus,

$$\eta = (\vartheta^{-1}\delta + \xi) + \beta = \zeta + \beta \quad \text{with } \zeta \in \mathcal{F},\ \beta \in \mathcal{O}.$$

Further, if ζ_1, ζ_2 are elements of $\mathcal{F}$ with $\zeta_1 - \zeta_2 \in \mathcal{O}$, then writing $\zeta_i = \vartheta^{-1}\delta_i + \xi_i$ with $\delta_i \in \mathcal{D}$, $\xi_i \in \mathcal{G}$ for $i = 1, 2$, we see that

$$\zeta_1 - \zeta_2 = \vartheta^{-1}(\delta_1 - \delta_2) + (\xi_1 - \xi_2).$$

Thus, $\xi_1 - \xi_2 \in \vartheta^{-1}\mathcal{O}$, hence $\xi_1 = \xi_2$, hence $\vartheta^{-1}(\delta_1 - \delta_2) \in \mathcal{O}$, therefore $\delta_1 = \delta_2$, and finally, $\zeta_1 = \zeta_2$. So indeed $\mathcal{F}$ is a bounded fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$. □

We choose any vector norm on $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ and endow $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ with the corresponding topology; this topology does not depend on the chosen norm. Given a subset $\mathcal{S}$ of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$, we denote by $\overline{\mathcal{S}}$ the closure of $\mathcal{S}$ with respect to this topology.

Let $\mathcal{F}$ be a fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$ with $0 \in \mathcal{F}$ and such that $\mathcal{F}$ is bounded. We call two elements α, β of $\mathcal{O}$ *$\mathcal{F}$-neighbours* of one another if $(\alpha + \overline{\mathcal{F}}) \cap (\beta + \overline{\mathcal{F}}) \neq \emptyset$. Let $\Delta_{\mathcal{F}} \subset \mathcal{O}$ be the set of all $\mathcal{F}$-neighbours of 0; this set contains in particular 0 itself. Further, if $\alpha \in \Delta_{\mathcal{F}}$, then so is $-\alpha$.

LEMMA 3.3. *The set of $\mathcal{F}$-neighbors $\Delta_{\mathcal{F}}$ of 0 contains a $\mathbb{Z}$-basis of $\mathcal{O}$.*

PROOF. See [11, Lemma 2.6] for the case that $\mathcal{O}$ is an order in a number field. The proof given there works in the same way for arbitrary orders, replacing $\mathbb{Z}^k$, $\mathcal{N}$ by $\mathcal{O}$, $\Delta_{\mathcal{F}}$. □

Let $p = x^n + p_{n-1}x^{n-1} + \cdots + p_0 \in \mathcal{O}[x]$ such that p_0 is not a zero divisor of $\mathcal{O}$, and put $p_n := 1$. We define the set

$$Z_{\mathcal{F},p} := \left\{ \sum_{j=1}^{n} \delta_j p_j : \delta_j \in \Delta_{\mathcal{F}} \right\}. \tag{3.1}$$

THEOREM 3.4. *Let $(p, \mathcal{D})$, with $p = x^n + p_{n-1}x^{n-1} + \cdots + p_0 \in \mathcal{O}[x]$ be a GNS over $\mathcal{O}$ and let $\mathcal{F}$ be a bounded fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$ with $\mathcal{D}_{\mathcal{F},p_0} = \mathcal{D}$. Assume that the following conditions hold (setting $p_n := 1$):*

(i) $Z_{\mathcal{F},p} + \mathcal{D} \subset \bigcup_{\delta \in \Delta_{\mathcal{F}}} (\mathcal{D} + p_0\delta)$,

(ii) $Z_{\mathcal{F},p} \subset \mathcal{D} \cup (\mathcal{D} - p_0)$,

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

Then $(p, \mathcal{D})$ is a GNS over $\mathcal{O}$ with the finiteness property.

PROOF. See [11, Theorem 3.1] for a proof in the case that $\mathcal{O}$ is an order in a number field. The proof carries over without modifications to arbitrary orders. □

REMARK 3.5. For $p \in \mathbb{Z}[x]$ denote by $L(p)$ the sum of the absolute values of the coefficients of p. Akiyama and Rao [2, Theorem 3.2] as well as Scheicher and Thuswaldner [12, Theorem 5.8] proved that if p is a monic polynomial with non-negative integer coefficients and such that $L(p) < 2p(0)$ then $\big(p, \{0, 1, \ldots, p(0) - 1\}\big)$ is a GNS over $\mathbb{Z}$ with the finiteness property. We show that Theorem 3.4 is a generalization of this assertion.

Indeed, with $\mathcal{O} = \mathbb{Z}$ the set $\mathcal{F} = [0, 1)$ is a fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$. Moreover

$$\mathcal{D}_{\mathcal{F},p(0)} = p(0) \cdot [0, 1) \cap \mathbb{Z} = \{0, 1, \ldots, p(0) - 1\},$$

which we denote by $\mathcal{D}$. We have $\Delta_{\mathcal{F}} = \{-1, 0, 1\}$, thus

$$\bigcup_{\delta \in \Delta_{\mathcal{F}}} (\mathcal{D} + p(0)\delta) = [-p(0), 2p(0) - 1] \cap \mathbb{Z} \tag{3.2}$$

and

$$\mathcal{D} \cup (\mathcal{D} - p(0)) = [-p(0), p(0) - 1] \cap \mathbb{Z}. \tag{3.3}$$

Let $p = p_n x^n + p_{n-1} x^{n-1} + \cdots + p_0$ with $p_n = 1$. As all coefficients of p are non-negative we have

$$\max\big\{\, |w| : w \in Z_{\mathcal{F},p} \big\} = \sum_{j=1}^{n} p_j = L(p) - p(0) < p(0)$$

by our assumption. This together with (3.3) implies immediately (ii). We have also the inequalities

$$-p(0) + 1 \le \min Z_{\mathcal{F},p} + \mathcal{D} < \max Z_{\mathcal{F},p} + \mathcal{D} \le 2p(0) - 2.$$

Comparing this with (3.2) we obtain (i). Finally let $J \subseteq \{1, \dots, n\}$. Then $0 \le \sum_{j \in J} p_j \le p(0) - 1$, thus (iii) holds too and our claim is proved.

4. The finiteness property for large constant terms

B. Kovács [8, Section 3] proved that if $p(x) \in \mathbb{Z}[x]$ is monic and irreducible, then $p(x + m)$ is a CNS polynomial for all sufficiently large integers m. Pethő [10] pointed out that the irreducibility assumption is not essential. Pethő and Thuswaldner [11] proved a generalization of Kovács' result for GNS over orders in algebraic number fields. In this section, we generalize their result further to GNS over arbitrary orders.

Let $\mathcal{O}$ be an order of rank d. We endow $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ with a submultiplicative vector norm $\|\cdot\|$, i.e., $\|\alpha \cdot \beta\| \le \|\alpha\| \cdot \|\beta\|$ for $\alpha, \beta \in \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$. For instance, if we choose a $\mathbb{Z}$-basis $\{1 = \omega_1, \omega_2, \dots, \omega_d\}$ of $\mathcal{O}$, then it is also an $\mathbb{R}$-basis of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$, and we may represent $\alpha \in \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ by the matrix M_α of the linear map $x \mapsto \alpha \cdot x$ with respect to this basis. Then we may choose as norm $\|\alpha\| = \sum_{i,j} |a_{ij}|$ where the a_{ij} are the entries of M_α. But in fact, in our arguments below, the choice of the submultiplicative norm does not matter.

For a subset $S \subset \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ and $\varepsilon > 0$, we define the ε-neighborhood of S by

$$(S)_\varepsilon := \big\{ \xi \in \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R} : \|\xi - \eta\| < \varepsilon \text{ for some } \eta \in S \big\}.$$

Let $\mathcal{F}$ be a bounded fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$ with $0 \in \mathcal{F}$. Let $p \in \mathcal{O}[x]$ be a monic polynomial of degree n. For $\alpha \in \mathcal{O}$ we define $p_\alpha(x) := p(x + \alpha)$. Let $\mathcal{G}_{p,\mathcal{F}}$ be the family of GNS, consisting of those pairs $(p_\alpha, \mathcal{D}_{\mathcal{F},p(\alpha)})$ such that $p(\alpha)$ is not a zero divisor of $\mathcal{O}$.

With this notation we prove the following theorem on $\mathcal{G}_{p,\mathcal{F}}$, which is a generalization of [11, Theorem 4.1]. As usual, we identify $r \in \mathbb{R}$ with $r \cdot 1$ where 1 is the unit element of $\mathcal{O}$, and thus view $\mathbb{R}$ as a subfield of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$.

THEOREM 4.1. *Let $\mathcal{O}$ be an order, $p \in \mathcal{O}[x]$ a monic polynomial of degree n, and $\mathcal{F}$ a bounded fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$. Choose a submultiplicative norm $\|\cdot\|$ on $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$. Suppose that there is $\varepsilon > 0$ such that*

$$\{\xi \in \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R} : \|\xi\| < \varepsilon\} \subset \mathcal{F} \cup (\mathcal{F} - 1); \tag{4.1}$$

$$\{\xi \in \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R} : \text{there is } r \in \mathbb{R} \text{ with } 0 < r < \varepsilon,\ \|r^{-1}\xi - 1\| < \varepsilon\} \subset \mathcal{F}. \tag{4.2}$$

Then there is $\eta > 0$ such that $(p_\alpha, \mathcal{D}_{\mathcal{F},p(\alpha)})$ is a GNS with the finiteness property whenever

$$\alpha \in \mathcal{O}, \quad \|m^{-1}\alpha - 1\| < \eta \text{ for some rational integer } m > \eta^{-1}. \tag{4.3}$$

The somewhat more complicated condition (4.2) means that $\mathcal{F}$ contains a cone emanating from 0 around a small piece of the positive real line.

REMARK 4.2. This implies that if $\mathcal{F}$ is a fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ satisfying (4.1) and (4.2), then the family $\mathcal{G}_{\mathcal{F}}$ contains infinitely many GNS with the finiteness property.

REMARK 4.3. Condition (4.3) cannot be weakened to say $\|\alpha\|$ being sufficiently large. For instance, let $\mathcal{O}$ be an order in a number field K not equal to $\mathbb{Q}$ or an imaginary quadratic field, and choose any bounded fundamental domain $\mathcal{F}$ with $0 \in \mathcal{F}$ for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$. For $\alpha \in \mathcal{O}$ define $\|\alpha\|$ to be the maximum of the absolute values of the conjugates of α. This defines a submultiplicative norm on $\mathcal{O}$, which we extend to $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$. Let $p \in \mathbb{Z}[x]$ be a monic polynomial with $p(0) = 0$. For $\alpha \in \mathcal{O}$, denote by $\alpha^{(1)}, \ldots, \alpha^{(d)}$ the conjugates of α. Then $Np_\alpha = \prod_{i=1}^{d} p(x + \alpha^{(i)})$. If one of the conjugates of α has absolute value ≤ 1 then Np_α is not expansive and hence $(p_\alpha, \mathcal{D}_{\mathcal{F},p(\alpha)})$ cannnot have the finiteness property. But $\mathcal{O}$ has elements α with one of the conjugates of absolute value ≤ 1 and $\|\alpha\|$ arbitrarily large.

We assume that $\operatorname{rank} \mathcal{O} = d$, $\deg p = n$. By Taylor's formula,

$$p_\alpha(x) = x^n + p_{n-1}(\alpha)x^{n-1} + \cdots + p_0(\alpha) \tag{4.4}$$

where $p_j(\alpha) := \frac{p^{(j)}(\alpha)}{j!}$ for $j = 0, \ldots, n-1$. Note that $p_j(\alpha) \in \mathcal{O}$ for $j = 0, \ldots, n-1$.

By expressions $O(r)$, with r a positive real, we denote elements ξ of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ such that $\|\xi\| \leq C \cdot r$, where C is a constant depending only on $\mathcal{O}$, p, $\mathcal{F}$ and $\|\cdot\|$.

We start with a simple lemma.

LEMMA 4.4. *For η sufficiently small in terms of $\mathcal{O}, \mathcal{F}, p, \|\cdot\|$ we have the following: if $\alpha \in \mathcal{O}$ satisfies* (4.3) *for some positive integer m, then*

$$p_j(\alpha) = \tbinom{n}{j} m^{n-j}(1 + O(\eta)) \quad \text{for } j = 0, \ldots, n-1,$$

and $p(\alpha)$ is not a zero divisor of $\mathcal{O}$, i.e., invertible in $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$.

PROOF. Write $\alpha = m + \beta$. Then $\|\beta\| < \eta m$ and $m > \eta^{-1}$. Assume $\eta < 1$ as we may. Then since p is monic of degree n, we have

$$\begin{aligned} p_0(\alpha) = p(\alpha) &= p(m) + O(\beta m^{n-1} + \beta^2 m^{n-2} + \cdots + \beta^n) \\ &= m^n + O(m^{n-1} + \beta m^{n-1} + \beta^2 m^{n-2} + \cdots + \beta^n) \\ &= m^n + O(\eta m^n) = m^n(1 + O(\eta)), \end{aligned}$$

using (4.3). Here the constants implied by the O-terms depend on the norms of the coefficients of p. The identities for $j > 0$ are proved in the same manner. To prove that $p(\alpha)$ has an inverse in $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$, write $\frac{p(\alpha)}{m^n} = 1 + \gamma$. Assuming η is sufficiently small we have $\|\gamma\| < 1$. The series $(1+\gamma)^{-1} = \sum_{k=0}^{\infty} (-1)^k \gamma^k$ converges in $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$, since $\|\gamma^k\| \le \|\gamma\|^k$ for $k \ge 0$. So $\frac{p(\alpha)}{m^n}$ is invertible in $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$. Hence $p(\alpha)$ is invertible in $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$. □

PROOF OF THEOREM 4.1. We proceed to show that if η is sufficiently small, and $\alpha \in \mathcal{O}$ satisfies (4.3), then $(p_\alpha, \mathcal{D}_{\mathcal{F},p(\alpha)})$ satisfies conditions (i), (ii), (iii) of Theorem 3.4, with p_α, $p_j(\alpha)$, $\mathcal{D}_{\mathcal{F},p_\alpha}$ instead of p, p_j, $\mathcal{D}$. This implies that $(p_\alpha, \mathcal{D}_{\mathcal{F},p(\alpha)})$ is a GNS with the finiteness property. We first observe that by the definition of $\mathcal{F}$-neighbours,

$$\overline{\mathcal{F}} \cap \left(\bigcup_{\delta \in \mathcal{O} \setminus \Delta_{\mathcal{F}}} (\mathcal{F} + \delta) \right) = \emptyset.$$

From this fact and the boundedness of $\mathcal{F}$ we infer that after shrinking the ε from conditions (4.1), (4.2) if necessary,

$$(\mathcal{F})_\varepsilon \cap \left(\bigcup_{\delta \in \mathcal{O} \setminus \Delta_{\mathcal{F}}} (\mathcal{F} + \delta) \right) = \emptyset.$$

The set $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ is a disjoint union of all the translates $\mathcal{F} + \delta$ with $\delta \in \mathcal{O}$ since $\mathcal{F}$ is a fundamental domain for $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}/\mathcal{O}$. So in addition to (4.1), (4.2) we have

$$(\mathcal{F})_\varepsilon \subseteq \bigcup_{\delta \in \Delta_{\mathcal{F}}} (\mathcal{F} + \delta). \tag{4.5}$$

We observe that if there is $\varepsilon > 0$ for which (4.1), (4.2) and (4.5) hold, then it can be chosen to depend only on $\mathcal{O}$, $\mathcal{F}$, p and $\|\cdot\|$.

Let $\alpha \in \mathcal{O}$ satisfy (4.3) for some positive integer m, where η is a real that is sufficiently small in terms of $\mathcal{O}$, $\mathcal{F}$, p, $\|\cdot\|$. Note that condition (i)

of Theorem 3.4 (with $p, p_j, \mathcal{D}$ replaced by p_α, $p_j(\alpha), \mathcal{D}_{\mathcal{F},p(\alpha)} = p(\alpha)\mathcal{F} \cap \mathcal{O}$) is equivalent to

$$\left(\sum_{j=1}^{n} \delta_j p_j(\alpha)\right) + p(\alpha)\mathcal{F} \cap \mathcal{O} \subset \bigcup_{\delta \in \Delta_{\mathcal{F}}} \big(p(\alpha)\delta + p(\alpha)\mathcal{F} \cap \mathcal{O}\big)$$

for all $\delta_j \in \Delta_{\mathcal{F}}$ for $j = 1, \dots, n$. This follows, once we have established that

$$\left(\sum_{j=1}^{n} \delta_j p_j(\alpha)\right) + p(\alpha)\mathcal{F} \subset \bigcup_{\delta \in \Delta_{\mathcal{F}}} \big(p(\alpha)\delta + p(\alpha)\mathcal{F}\big)$$

which in turn is equivalent to

$$\left(\sum_{j=1}^{n} \delta_j \cdot \frac{p_j(\alpha)}{p(\alpha)}\right) + \mathcal{F} \subset \bigcup_{\delta \in \Delta_{\mathcal{F}}} \big(\mathcal{F} + \delta\big) \tag{4.6}$$

for all $\delta_j \in \Delta_{\mathcal{F}}$, $j = 1, \dots, n$. Here we have used that by Lemma 4.4 $p(\alpha)$ has an inverse in $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$. So in order to deduce (i) of Theorem 3.4 it suffices to deduce (4.6). But from Lemma 4.4 and condition (4.3) it follows that

$$\sum_{j=1}^{n} \delta_j \cdot \frac{p_j(\alpha)}{p(\alpha)} = O(m^{-1}) = O(\eta) \tag{4.7}$$

and for η sufficiently small in terms of $\mathcal{O}$, $\mathcal{F}$, p, $\|\cdot\|$ and ε, the left-hand side has norm smaller than ε. So (4.6) follows from (4.5). Hence condition (i) of Theorem 3.4 is satisfied.

By a similar argument as above, it follows that condition (ii) of Theorem 3.4 follows, once we have

$$\sum_{j=1}^{n} \delta_j \cdot \frac{p_j(\alpha)}{p(\alpha)} \in \mathcal{F} \cup (\mathcal{F} - 1) \tag{4.8}$$

for all $\delta_j \in \Delta_{\mathcal{F}}$, $j = 1, \dots, n$. But this clearly follows from (4.7) and (4.1) if η is sufficiently small in terms of $\mathcal{O}$, $\mathcal{F}$, p, $\|\cdot\|$ and ε. This establishes condition (ii) of Theorem 3.4.

Finally, condition (iii) of Theorem 3.4 follows once we have shown that

$$\xi := \sum_{j \in J} \frac{p_j(\alpha)}{p(\alpha)} \in \mathcal{F} \tag{4.9}$$

for every non-empty subset J of $\{1,\dots,n\}$. By Lemma 4.4,

$$\xi = \Big(\sum_{j\in J}\tbinom{n}{j}m^{-j}\Big)(1+O(\eta)). \tag{4.10}$$

Let $r := \sum_{j\in J}\binom{n}{j}m^{-j}$. Assuming η is sufficiently small, and using $m^{-1}\le\eta$ by (4.3), we get $0<r<\varepsilon$ and $\|r^{-1}\xi-1\|<\varepsilon$, which by (4.2) implies $\xi\in\mathcal{F}$. So condition (iii) of Theorem 3.4 is also satisfied.

It follows that $(p_\alpha,\mathcal{D}_{\mathcal{F},p(\alpha)})$ has the finiteness property. □

Theorem 4.1 has the following variation.

THEOREM 4.5. *Let $\mathcal{O}$ be an order, $p\in\mathcal{O}[x]$ a monic polynomial of degree n, and $\mathcal{F}$ a bounded fundamental domain for $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}/\mathcal{O}$. Choose a submultiplicative norm $\|\cdot\|$ on $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}$. Suppose that 0 is an interior point of $\mathcal{F}$. Then there is $\eta>0$ such that $(p_\alpha,\mathcal{D}_{\mathcal{F},p(\alpha)})$ is a GNS with the finiteness property whenever*

$$\alpha\in\mathcal{O},\ \|m^{-1}\alpha-1\|<\eta \text{ for some rational integer } m \text{ with } |m|>\eta^{-1}. \tag{4.11}$$

PROOF. The proof is exactly the same as that of Theorem 4.1, except for the proof of (4.9). To prove this, let $\varepsilon>0$ be such that $\mathcal{F}$ contains all the elements of $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}$ of norm smaller than ε. Pick $\alpha\in\mathcal{O}$ satisfying (4.11). Then estimate (4.10) implies that if η is sufficiently small, then the ξ from (4.9) has norm smaller than ε, hence lies in $\mathcal{F}$. □

REMARK 4.6. Under the conditions of Theorem 4.1 there exists a positive integer N such that $(p_m,\mathcal{D}_{\mathcal{F},p(m)})$ is a GNS with the finiteness property for $m\ge N$, while under the more restrictive conditions of Theorem 4.5 there exists a positive integer N such that $(p_{\pm m},\mathcal{D}_{\mathcal{F},p(\pm m)})$ are GNS with the finiteness property for $m\ge N$.

EXAMPLE 4.7. Let $\mathcal{O}=\mathbb{Z}\times\mathbb{Z}=\mathbb{Z}^2$ with coordinatewise addition and multiplication, zero element $(0,0)$ and unit element $(1,1)$. Note that $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}=\mathbb{R}^2$ with coordinatewise addition and multiplication. Endow $\mathbb{R}^2$ with the maximum norm. Take

$$\begin{aligned}\mathcal{F}&=\big\{(x,y)\in\mathbb{R}^2 : 0\le x<1,\ -\tfrac12\le y-x<\tfrac12\big\}\\&=\big\{x(1,1)+z(0,1) : 0\le x<1,\ -\tfrac12\le z<\tfrac12\big\}.\end{aligned}$$

Then $\mathcal{F}$ is a fundamental domain for $\mathbb{R}^2/\mathbb{Z}^2$. Let $p\in\mathcal{O}[x]$ be a monic polynomial of degree n. The coefficients of p are pairs $(a,b)\in\mathbb{Z}^2$, its leading coefficient being the unit element $(1,1)$ of $\mathbb{Z}^2$. Thus we can write $p=(p_1,p_2)$, where p_1, p_2 are monic polynomials in $\mathbb{Z}[x]$ of degree n. It is easy to see that

if the integer m is large enough then $p_1(m), p_2(m) > 0$ and the corresponding digit set is

$$\mathcal{D}_{\mathcal{F},p(m)} = \big\{(x,y) \in \mathbb{Z}^2 : 0 \le x < p_1(m),\ -\tfrac{1}{2} \le p_2(m)^{-1}y - p_1(m)^{-1}x < \tfrac{1}{2}\big\}.$$

One easily verifies that $\mathcal{F}$ satisfies conditions (4.1), (4.2), but note that the inequality $\|r^{-1}\xi - 1\| < \varepsilon$ in (4.2) has to be interpreted as $\|r^{-1}\xi - (1,1)\| < \varepsilon$, as $(1,1)$ is the unit element of $\mathcal{O}$. So by Theorem 4.1, $(p_m, \mathcal{D}_{\mathcal{F},p(m)})$ has the finiteness property for every sufficiently large m. This means that for every pair of polynomials $a_1, a_2 \in \mathbb{Z}[x]$ there are $L > 0$ and pairs $(d_i, d_i') \in \mathcal{D}_{\mathcal{F},p(m)}$ for $i = 1, \dots, L$, such that

$$a_1 \equiv \sum_{i=0}^{L} d_i x^i \pmod{p_{1,m}}, \quad a_2 \equiv \sum_{i=0}^{L} d_i' x_i \pmod{p_{2,m}},$$

where $p_{i,m}(x) = p_i(x+m)$ for $i = 1, 2$.

EXAMPLE 4.8. Let $\mathcal{O}$, p be as above but now take $\mathcal{F} = [0,1) \times [0,1)$. This $\mathcal{F}$ is a fundamental domain for $\mathbb{R}^2/\mathbb{Z}^2$, but it does not satisfy condition (4.1), so Theorem 4.1 is not directly applicable. However, the corresponding digit set can be expressed as a cartesian product

$$\mathcal{D}_{\mathcal{F},p(m)} = \mathcal{D}_{[0,1),p_1(m)} \times \mathcal{D}_{[0,1),p_2(m)} = \{0, \dots, p_1(m)-1\} \times \{0, \dots, p_2(m)-1\}.$$

The interval $[0,1)$ does satisfy (4.1), (4.2), with $\mathcal{O} = \mathbb{Z}$. So by Theorem 4.1, for every sufficiently large positive integer m, both GNS over $\mathbb{Z}$, $(p_{i,m}, \mathcal{D}_{[0,1),p_i(m)})$ $(i = 1, 2)$ have the finiteness property. Now $(p_m, \mathcal{D}_{\mathcal{F},p(m)})$ is the cartesian product of these two GNS (we assume the meaning of this is obvious), and it easily follows that it has the finiteness property for every sufficiently large integer m.

We will see in the next section that if we impose some other conditions on $\mathcal{F}$, then $(p_{-m}, \mathcal{D}_{\mathcal{F},p(-m)})$ does not have the finiteness property for large m.

EXAMPLE 4.9. Let $\mathcal{O}$, p be as above, but now take $\mathcal{F} = [-\frac{1}{2}, \frac{1}{2}) \times [-\frac{1}{2}, \frac{1}{2})$; then $\mathcal{F}$ is again a fundamental domain for $\mathbb{R}^2/\mathbb{Z}^2$. Let m be a positive integer. Then the corresponding digit set is

$$\mathcal{D}_{\mathcal{F},p(\pm m)} = \Big\{ -\Big\lfloor \frac{|p_1(\pm m)|}{2} \Big\rfloor, \dots, \Big\lfloor \frac{|p_1(\pm m)| - 1}{2} \Big\rfloor \Big\} \times \Big\{ -\Big\lfloor \frac{|p_2(\pm m)|}{2} \Big\rfloor, \dots, \Big\lfloor \frac{|p_2(\pm m)| - 1}{2} \Big\rfloor \Big\},$$

which is the product of two symmetric digit sets. The zero element $(0,0)$ of $\mathbb{Z}^2$ is obviously an interior point of $\mathcal{F}$, hence, by Theorem 4.5 the pairs $(p_{\pm m}, \mathcal{D}_{\mathcal{F},p(\pm m)})$ are GNS with the finiteness property for all large enough m.

5. GNS without the finiteness property

We now prove a negative result on the finiteness property for GNS over arbitrary orders $\mathcal{O}$. We start with a simple lemma that was proved in [11, Lemma 5.1]. We state it here in a more general form.

LEMMA 5.1. *Let $\mathcal{O}$ be an order and $(p,\mathcal{D})$ a GNS over $\mathcal{O}$. If there exist a positive integer h, elements $d_0,d_1,\dots,d_{h-1}$ of $\mathcal{D}$ not all 0 and $q_1,q_2\in\mathcal{O}[x]$ with*

$$\sum_{j=0}^{h-1} d_j x^j = (x^h-1)q_1(x)+q_2(x)p(x), \tag{5.1}$$

then $(p,\mathcal{D})$ does not have the finiteness property.

PROOF. Verbatim the same as the proof of [11, Lemma 5.1]. □

We can now prove the main result of the present section. Recall that $p_{-m}(x):=p(x-m)$ and $\mathcal{D}_{\mathcal{F},p(-m)}:=p(-m)\mathcal{F}\cap\mathcal{O}$. We view $\mathbb{R}$ as a subfield of $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}$ by identifying $r\in\mathbb{R}$ with $r\cdot 1$, where 1 is the unit element of $\mathcal{O}$.

THEOREM 5.2. *Let $\mathcal{O}$ be an order, $\|\cdot\|$ a submultiplicative norm on $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}$, and $\mathcal{F}$ a bounded fundamental domain for $\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R}/\mathcal{O}$ such that $0\in\mathcal{F}$ and there is $\varepsilon>0$ such that*

$$\left\{\xi\in\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{R} : \text{there is } r\in\mathbb{R} \text{ with } 0<r<\varepsilon,\ \|r^{-1}(1-\xi)-1\|<\varepsilon\right\}\subseteq\mathcal{F}. \tag{5.2}$$

Let $p\in\mathcal{O}[x]$ be a monic polynomial. Then there exists a positive integer N such that for every $m>N$, $(p_{-m},\mathcal{D}_{\mathcal{F},p(-m)})$ does not have the finiteness property.

Condition (5.2) means that $\mathcal{F}$ contains a cone emanating from 1, around the piece of the real line consisting of all reals slightly smaller than 1.

PROOF. Let $d=\operatorname{rank}\mathcal{O}$, $n=\deg p$. We claim that if m is a large enough positive rational integer, then $p_{-m}(0)=p(-m)\in\mathcal{D}_{\mathcal{F},p(-m-1)}$.

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

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

By the claim $p(-m)$ belongs to the digit set $\mathcal{D}_{\mathcal{F},p(-m-1)}$ if m is large enough. Applying Lemma 5.1 with $h=1$, $d_0=p(-m)$, $q_1=-s_{m+1}$, $q_2=1$, $p=p_{-m-1}$ and $\mathcal{D}=\mathcal{D}_{\mathcal{F},p(-m-1)}$ we conclude that $(p_{-m-1},\mathcal{D}_{\mathcal{F},p(-m-1)})$ is not a GNS with the finiteness property whenever m is large enough.

Now we turn to prove the claim. Write $p = x^n + p_{n-1}x^{n-1} + \cdots + p_0$. Note that

$$p(-m) = (-m)^n + p_{n-1}(-m)^{n-1} + O(m^{n-2}) \tag{5.3}$$
$$= (-m)^n\big(1 + p_{n-1}m^{-1} + O(m^{-2})\big).$$

This implies that for m sufficiently large, we have $\frac{p(-m)}{(-m)^n} = 1 + \gamma$ with $\|\gamma\| < 1$. The quantity $1 + \gamma$ is invertible in $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ with inverse $1 - \gamma + \gamma^2 - \cdots$, so $p(-m)$ is invertible in $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ and

$$p(-m)^{-1} = (-m)^{-n}(1 - \gamma + \gamma^2 - \cdots) \tag{5.4}$$
$$= (-m)^{-n}\big(1 - p_{n-1}m^{-1} + O(m^{-2})\big).$$

Establishing our claim means proving that $p(-m) \in p(-m-1)\mathcal{F} \cap \mathcal{O}$ for every sufficiently large m. For this, it suffices to show that

$$\frac{p(-m)}{p(-m-1)} \in \mathcal{F} \tag{5.5}$$

for every sufficiently large m. By (5.3) and (5.4) we have

$$\xi_m := \frac{p(-m)}{p(-m-1)}$$
$$= \frac{m^n}{(m+1)^n} \cdot (1 + p_{n-1}m^{-1} + O(m^{-2})) \cdot (1 - p_{n-1}(m+1)^{-1} + O(m^{-2}))$$
$$= \frac{m^n}{(m+1)^n}\big(1 + O(m^{-2})\big) = 1 - n \cdot m^{-1} + O(m^{-2}).$$

It is clear that for every sufficiently large m, ξ_m belongs to the set on the left-hand side of (5.2), hence $\xi_m \in \mathcal{F}$. This establishes assertion (5.5), hence our claim and our theorem. □

Example 5.3. We continue the examination of the GNS given in Examples 4.7, 4.8. As can be verified, the fundamental domains $\mathcal{F}$ from both examples satisfy (5.2) (the inequality $\|r^{-1}(1-\xi) - 1\| < \varepsilon$ being interpreted as $\|r^{-1}(1-\xi) - (1,1)\| < \varepsilon$). Hence in both cases, $(p_{-m}, \mathcal{D}_{\mathcal{F},p(-m)})$ does not have the finiteness property for every sufficiently large m. Of course in the case of Example 4.8, we can alternatively appeal to a Cartesian product type argument.

6. Relation between power integral bases and GNS

The theory of generalized number systems started with investigations in the ring of integers of algebraic number fields (see e.g. Brunotte, Huszti, and

Pethő [3] for an overview and a list of relevant literature). This inspired [11, Theorem 6.2], which states if $\mathcal{O}$ is a monogenic order of a number field, then all but finitely many among the α with $\mathbb{Z}[\alpha] = \mathcal{O}$ generate a number system with the finiteness property in $\mathcal{O}$. (All the exceptions are computable effectively.) This result forms an analogue of Kovács and Pethő [9, Theorem 5] and is based on a result by Győry [6,7] on the monogeneity of orders in number fields. We generalize this to étale $\mathbb{Q}$-algebras.

A finite étale $\mathbb{Q}$-algebra Ω is up to isomorphism a direct product of number fields $\mathbb{K}_1 \times \cdots \times \mathbb{K}_\ell$, with coordinatewise addition and multiplication. The *degree* of Ω is the dimension of Ω as a $\mathbb{Q}$-vector space, notation $[\Omega : \mathbb{Q}]$.

We say that a finite étale $\mathbb{Q}$-algebra Ω is *effectively given*, if it is given in the form $\mathbb{K}_1 \times \cdots \times \mathbb{K}_\ell$, where $\mathbb{K}_1, \ldots, \mathbb{K}_\ell$ are effectively given as finite extensions of $\mathbb{Q}$, e.g., by minimal polynomials of primitive elements. Further, an element $\alpha \in \Omega$ is said to be *effectively given* if in $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ with $\alpha_i \in \mathbb{K}_i$, the element α_i is effectively given as a $\mathbb{Q}$-linear combination of powers of a given primitive element of $\mathbb{K}_i$, see [4, Sections 3.7 and 8.4].

An order of a finite étale $\mathbb{Q}$-algebra Ω is an order $\mathcal{O} \subset \Omega$ with $\operatorname{rank} \mathcal{O} = [\Omega : \mathbb{Q}]$, i.e., $\Omega \cong \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$. An étale order is an order of any finite étale $\mathbb{Q}$-algebra. By the Artin–Wedderburn Theorem, an order is étale if and only if it has no nilpotent elements.

We say that an étale order $\mathcal{O}$ is effectively given if the étale $\mathbb{Q}$-algebra $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ is effectively given, and if a $\mathbb{Z}$-basis of $\mathcal{O}$ is effectively given as a subset of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$.

We say that two elements α, β of an order $\mathcal{O}$ are $\mathbb{Z}$-equivalent, if $\beta = \alpha + u$ for some $u \in \mathbb{Z}$. The order $\mathcal{O}$ is called *monogenic* if $\mathcal{O} = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}$. This is equivalent to $\mathcal{O}$ having a *power integral basis*, i.e., a $\mathbb{Z}$-basis of the form $\{1, \alpha, \ldots, \alpha^{M-1}\}$ where $M = [\Omega : \mathbb{Q}]$.

We recall the following fundamental result.

PROPOSITION 6.1. *Let $\mathcal{O}$ be an effectively given étale order. Then it can be decided effectively whether $\mathcal{O}$ is monogenic or not. Further, if $\mathcal{O}$ is monogenic, then there exist only finitely many $\mathbb{Z}$-equivalence classes of $\alpha \in \mathcal{O}$ such that $\mathcal{O} = \mathbb{Z}[\alpha]$, and a complete set of representatives for these classes can be effectively determined.*

Proposition 6.1 does not hold for orders in general. For instance, let $\mathcal{O} = \mathbb{Z}[x]/(x^3)$ and let α denote the residue class of x. Then $\mathcal{O} = \mathbb{Z}[\alpha + b\alpha^2]$ for every $b \in \mathbb{Z}$.

Proposition 6.1 is a special case of a more general effective result of Evertse and Győry [4, Corollary 8.4.7] and allows to generalize the above mentioned [11, Theorem 6.2] from orders in number fields to étale orders.

Let $\mathcal{O}$ be an order. Recall that $\alpha \in \mathcal{O}$ is not a zero divisor of $\mathcal{O}$ if and only if its norm $N(\alpha)$, that is the determinant of the $\mathbb{Z}$-linear map $x \mapsto \alpha x$ from $\mathcal{O}$ to itself, is non-zero. A *number system* for $\mathcal{O}$ is a pair $(\alpha, \mathcal{D})$, where

$\alpha \in \mathcal{O}$ is not a zero divisor, and $\mathcal{D}$ is a complete residue system of $\mathbb{Z}$ modulo $N(\alpha)$. We say that $(\alpha, \mathcal{D})$ has the finiteness property if every element of $\mathcal{O}$ can be written as a finite sum $\sum_{i=0}^{L} d_i \alpha^i$ with $d_i \in \mathcal{D}$ for all i. Note that this implies first that $\mathcal{O}$ is monogenic, and second, that $\mathbb{Z}/N(\alpha)\mathbb{Z} \cong \mathcal{O}/\alpha\mathcal{O}$, so that $\mathcal{D}$ is also a complete residue system of $\mathcal{O}$ modulo α. Clearly, if $p \in \mathbb{Z}[x]$ is the minimal polynomial of α, then $(\alpha, \mathcal{D})$ has the finiteness property if and only if $(p, \mathcal{D})$ is a GNS over $\mathbb{Z}$ with the finiteness property.

For $\alpha \in \mathcal{O}$ such that $\mathcal{O} = \mathbb{Z}[\alpha]$ and a fundamental domain $\mathcal{F}$ for $\mathbb{R}/\mathbb{Z}$ with $0 \in \mathcal{F}$, we define $\mathcal{D}_{\mathcal{F},\alpha} := p(0)\mathcal{F} \cap \mathbb{Z}$, where p is the minimal polynomial of α over $\mathbb{Q}$.

THEOREM 6.2. *Let $\mathcal{O}$ be an étale order. Assume that $\mathcal{O}$ is monogenic. Let a bounded fundamental domain $\mathcal{F}$ for $\mathbb{R}/\mathbb{Z}$ be given. If 0 is an inner point of $\mathcal{F}$ then every $\alpha \in \mathcal{O}$ with $\mathcal{O} = \mathbb{Z}[\alpha]$, with at most finitely many exceptions, gives rise to a number system $(\alpha, \mathcal{D}_{\mathcal{F},\alpha})$ with the finiteness property.*

PROOF. The proof is literally the same as the proof of [11, Theorem 6.2]. □

REMARK 6.3. In [4], a generalization of the above Proposition 6.1 was proved dealing with the relative case as well, i.e., with étale orders of the shape $\mathcal{O} = \mathbb{Z}_{\mathbb{K}}[\alpha]$, where $\mathbb{Z}_{\mathbb{K}}$ is the ring of integers of a number field $\mathbb{K}$. To generalize Theorem 6.2 to this situation would require the generalization of Remark 4.6 to all $m \in \mathcal{O}$ of which all conjugates of m are large enough. By Remark 4.3 such a generalization is only possible for special number fields.

A finite set $\mathcal{D}$ of integers can be a complete residue system modulo at most two integers, namely $\pm|\mathcal{D}|$. This does not hold any more for algebraic number fields with infinitely many units. Indeed, let $\mathbb{K}$ be such a field and $\mathbb{Z}_{\mathbb{K}}$ be its ring of integers. Let $\mathcal{D} \subset \mathbb{Z}$ be given and assume that there exist $\alpha \in \mathbb{Z}_{\mathbb{K}}$ such that $\mathcal{D}$ is a complete residue system modulo α. Then $\mathcal{D}$ is a complete residue system modulo $\alpha\varepsilon$ for each unit $\varepsilon \in \mathbb{Z}_{\mathbb{K}}$. From the next theorem it follows that there are only finitely many $\varepsilon \in \mathbb{Z}_{\mathbb{K}}$ such that the number system $(\alpha\varepsilon, \mathcal{D})$ has the finiteness property.

THEOREM 6.4. *Let $\mathcal{O}$ be an effectively given étale order, and $\mathcal{D}$ a given finite subset of $\mathbb{Z}$ containing 0. Then there exist only finitely many, effectively computable $\alpha \in \mathcal{O}$ such that the number system $(\alpha, \mathcal{D})$ has the finiteness property.*

PROOF. Let $\alpha \in \mathcal{O}$ and $\mathcal{D} \subset \mathbb{Z}$ be such that the number system $(\alpha, \mathcal{D})$ has the finiteness property. The set $\mathcal{D}$ has to be a complete residue system of $\mathcal{O}$ modulo α, which is only possible if $|N(\alpha)| = |\mathcal{D}|$. If there is no such α then we are done. Otherwise, if $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{K}_1 \times \cdots \times \mathbb{K}_\ell$ and $\mathbb{K}_h$ are either the rational or an imaginary quadratic number field for all $h = 1, \ldots, \ell$ then there are only finitely many α with $|N(\alpha)| = |\mathcal{D}|$ and our assertion holds again.

We now assume that there are infinitely many $\alpha \in \mathcal{O}$ such that $|N(\alpha)| = |\mathcal{D}|$. If $(\alpha, \mathcal{D})$ has the finiteness property then there exist for all $\gamma \in \mathcal{O}$ an integer L and $d_i \in \mathcal{D}, i = 0, \ldots, L$ such that

$$\gamma = \sum_{i=0}^{L} d_i \alpha^i,$$

hence $\mathcal{O}$ is monogenic. By Proposition 6.1 there exist only finitely many $\mathbb{Z}$-equivalence classes of $\beta \in \mathcal{O}$ such that $\mathcal{O} = \mathbb{Z}[\beta]$. Hence there is such a β and $u \in \mathbb{Z}$ with $\alpha = \beta + u$. For fixed β there are only finitely many effectively computable $u \in \mathbb{Z}$ with $|N(\beta + u)| = |\mathcal{D}|$, thus the assertion is proved. □

References

[1] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő, and J. M. Thuswaldner, Generalized radix representations and dynamical systems. I, *Acta Math. Hungar.*, **108** (2005), 207–238.

[2] S. Akiyama and H. Rao, New criteria for canonical number systems, *Acta Arith.*, **111** (2004), 5–25.

[3] H. Brunotte, A. Huszti, and A. Pethő, Bases of canonical number systems in quartic algebraic number fields, *J. Théor. Nombres Bordeaux*, **18** (2006), 537–557.

[4] J.-H. Evertse and K. Győry, *Discriminant Equations in Diophantine Number Theory*, New Mathematical Monographs, Vol. 32, Cambridge University Press (Cambridge, 2017).

[5] 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 (decimale), *Giornale di Matematiche di Battaglini*, **23** (1885), 203–221; Errata, p. 367.

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

[7] K. Győry, On polynomials with integer coefficients and given discriminant. IV, *Publ. Math. Debrecen*, **25** (1978), 155–167.

[8] B. Kovács, Canonical number systems in algebraic number fields, *Acta Math. Hungar.*, **37** (1981), 405–407.

[9] B. Kovács and A. Pethő, Number systems in integral domains, especially in orders of algebraic number fields, *Acta Sci. Math. (Szeged)*, **55** (1991), 286–299.

[10] A. Pethő, On a polynomial transformation and its application to the construction of a public key cryptosystem, in: *Computational Number Theory* (Debrecen, 1989), de Gruyter (Berlin, 1991), pp. 31–43.

[11] A. Pethő and J. M. Thuswaldner, Number systems over orders, *Monatsh. Math.*, **187** (2018), 681–704.

[12] K. Scheicher and J. M. Thuswaldner, On the characterization of canonical number systems, *Osaka J. Math.*, **41** (2004), 327–351.

[13] A. Vince, Replicating tesselations, *SIAM J. Disc. Math.*, **6** (1993), 501–521.