Pisot numbers, Salem numbers, and generalised polynomials

Jakub Byszewski, Jakub Konieczny

PISOT NUMBERS, SALEM NUMBERS, AND GENERALISED POLYNOMIALS

JAKUB BYSZEWSKI AND JAKUB KONIECZNY

Abstract. We study sets of integers that can be defined by the vanishing of a generalised polynomial expression. We show that this includes sets of values of linear recurrent sequences of Salem type and some linear recurrent sequences of Pisot type. To this end, we introduce the notion of a generalised polynomial on a number field. We establish a connection between the existence of generalised polynomial expressions for sets of values of linear recurrent sequences and for subsemigroups of multiplicative groups of number fields.

1. Introduction

Generalised polynomials are expressions built up from ordinary polynomials with the use of the integer part function, addition, and multiplication. In contrast with ordinary polynomials, generalised polynomial sequences can be bounded or even finitely-valued without being constant. For instance, for any irrational $\alpha \in (0,1)$ and any real β, the generalised polynomial map g given by

$$g(n) = \lfloor \alpha(n+1) + \beta \rfloor - \lfloor \alpha n + \beta \rfloor \tag{1}$$

defines a Sturmian sequence, which takes on only the values 0 and 1, with density $1-\alpha$ and α, respectively. We define generalised polynomial sets to be the level sets of such maps. Equivalently, a generalised polynomial set $E \subseteq \mathbb{Z}$ is a set such that the characteristic function $1_E \colon \mathbb{Z} \to \{0,1\}$ is a generalised polynomial map.

It turns out that some sets of arithmetical or combinatorial interest are generalised polynomial sets. One example is the set of Fibonacci numbers, in which case an appropriate generalised polynomial can be constructed using the relation between the Fibonacci numbers and the golden mean together with some classical properties of continued fractions. It is a difficult problem to determine the extent to which this generalises to sequences $(n_i)_{i=0}^{\infty}$ that satisfy a linear recurrence

$$n_{i+m} = \sum_{j=0}^{m-1} a_j n_{i+j}, \quad i \geqslant 0, \tag{2}$$

for some $a_0, \dots, a_{m-1} \in \mathbb{Z}$. One result in this direction concerns linear recurrent sequences whose characteristic polynomial is the minimal polynomial of a Pisot number. Recall that the characteristic polynomial of the recurrence (2) is $X^m - \sum_{j=0}^{m-1} a_j X^j$, a (Galois) conjugate of an algebraic number β is any root of the minimal polynomial of β over $\mathbb{Q}$, and a *Pisot number* (or a Pisot–Vijayaraghavan number) is a real algebraic number β such that $\beta > 1$, but all conjugates α of β except for β itself satisfy $|\alpha| < 1$. An algebraic number is a *unit* if both the number and its reciprocal are algebraic integers. An algebraic number is *totally real* if all of its conjugates are real. The Dirichlet's unit theorem implies that for a real algebraic number β, the group of units $\mathcal{O}^*_{\mathbb{Q}(\beta)}$ in $\mathbb{Q}(\beta)$ has rank 1 if and only if β is either quadratic, or cubic and not totally real. The following theorem has been proved in many cases in [BK18, Thm. B] and in full generality in [AK22].

Theorem 1.1. *Let β be a Pisot unit such that $\mathcal{O}^*_{\mathbb{Q}(\beta)}$ has rank 1 and let $(n_i)_{i=0}^{\infty}$ be an integer-valued linear recurrent sequence with characteristic polynomial the minimal polynomial of β. Then the set $\{n_i \mid i \in \mathbb{N}_0\}$ is generalised polynomial.*

Date: February 12, 2023.

2010 *Mathematics Subject Classification.* Primary: 11R06, 11J54, Secondary: 11D61, 11J87 .

Key words and phrases. Pisot numbers, Salem numbers, generalised polynomials, bracket words, linear recurrent sequences, S-unit equation, Skolem–Mahler–Lech theorem.

It seems considerably more difficult to prove results in the opposite direction, that is, to establish that the set of values of a certain linear recurrent sequence is not generalised polynomial. Essentially the only known examples of such sequences have been obtained in [Kon21], where it is shown that the set $\{k^i \mid i \in \mathbb{N}_0\}$ is not generalised polynomial for any integer $k \geqslant 2$. Note that k is a Pisot *number*, but it is not a Pisot *unit*.

In this paper, we obtain several extensions of Theorem 1.1. The first of them concerns Salem numbers. Recall that a real algebraic number β is a *Salem number* if $\beta > 1$, all conjugates α of β except for β itself satisfy $|\alpha| \leqslant 1$, and there exists at least one conjugate α with $|\alpha| = 1$. If β is a Salem number, then $1/\beta$ is a conjugate of β, and for all remaining conjugates α we have $|\alpha| = 1$ [Smy15, Lem. 1]. For background on Salem numbers, we refer to [BDGGH$^+$92] and [Smy15].

Theorem A. *Let β be a Salem number and let $(n_i)_{i=0}^{\infty}$ be an integer-valued linear recurrent sequence with characteristic polynomial the minimal polynomial of β. Then the set $\{n_i \mid i \in \mathbb{N}_0\}$ is generalised polynomial.*

The proof of this result is most naturally phrased in terms of the notion of a *generalised polynomial map on a number field*. A number field K is a finite extension of $\mathbb{Q}$, and generalised polynomials on K can be defined in terms of the coordinates of an element in some $\mathbb{Q}$-basis of K; for example, a generalised polynomial map g on $\mathbb{Q}(\sqrt{2})$ is of the form $g(x + y\sqrt{2}) = h(x, y)$, where h is a generalised polynomial expression in two variables x, y taking values in $\mathbb{Q}$. We carefully introduce this concept in Section 2. Once the notion has been introduced, it is rather immediate to see that the set $\{\beta^i \mid i \in \mathbb{N}_0\}$ of powers of a Salem number β is a generalised polynomial subset of $\mathbb{Q}(\beta)$, and Theorem A can be deduced from this.

The special role of Pisot and Salem numbers in diophantine approximation is well recognized, even as many of the characterisations of Pisot and Salem numbers by their diophantine properties remain conjectural. In the context of generalised polynomials, we believe that Theorems 1.1 and A should provide an essentially complete list of linear recurrent sequences whose set of values is generalised polynomial, and, similarly, an essentially complete list of algebraic numbers β such that the set of powers $\{\beta^i \mid i \in \mathbb{N}_0\}$ is a generalised polynomial subset of $\mathbb{Q}(\beta)$. The following result elucidates the connection between these two questions.

Theorem B. *Let β be an algebraic integer. Suppose that there exists an integer-valued sequence $(n_i)_{i=0}^{\infty}$ with characteristic polynomial the minimal polynomial of β that is not identically zero and is such that the set $\{n_i \mid i \in \mathbb{N}_0\}$ is generalised polynomial. Then the set $\left\{\beta^i \;\middle|\; i \in \mathbb{N}_0\right\}$ is a generalised polynomial subset of $\mathbb{Q}(\beta)$.*

The interest in the above result arises from the fact that it is likely easier to show that the set of powers of an algebraic number is not generalised polynomial than to show that the corresponding result holds for the set of values of a linear recurrent sequence. In particular, the methods of [Kon21] relied strongly on the fact that the set of powers of an integer k forms a semigroup, and could conceivably be generalised.

Returning to Pisot numbers, we observe that we can strengthen the result obtained in Theorem 1.1. We say that a set E is *hereditarily generalised polynomial* or that a generalised polynomial set is *hereditary* if each subset $E' \subseteq E$ is generalised polynomial (this notion applies to generalised polynomial subsets of integers, number fields, etc.). The following result shows that the the sets considered in Theorem 1.1 are in fact hereditary. In particular, any set consisting of Fibonacci numbers is generalised polynomial.

Theorem C. *Let β be a Pisot unit such that $\mathcal{O}^*_{\mathbb{Q}(\beta)}$ has rank 1, and let $(n_i)_{i=0}^{\infty}$ be an integer-valued linear recurrent sequence with characteristic polynomial the minimal polynomial of β. Let I be an arbitrary subset of $\mathbb{N}_0$. Then the set $\{n_i \mid i \in I\}$ is generalised polynomial.*

The above result has the following counterpart for sets of powers of β.

Theorem D. *Let β be a Pisot unit such that $\mathcal{O}^*_{\mathbb{Q}(\beta)}$ has rank 1. Let I be an arbitrary subset of $\mathbb{N}_0$. Then the set $\left\{\beta^i \;\middle|\; i \in I\right\}$ is a generalised polynomial subset of $\mathbb{Q}(\beta)$.*

In light of Theorems C and D, the following question arises naturally.

Question 1.2. Are the generalised polynomial sets considered in Theorem A hereditary?

It would be interesting to determine more generally which generalised polynomial sets are hereditary. Since a generalised polynomial subset of the integers always has density, no positive density generalised polynomial set of integers can be hereditary (see Section 7 for details), and so the question is only interesting

for sets with density zero. The task of disproving that a set is hereditarily generalised polynomial is made difficult by the fact that most tools available for showing that a given set $E \subseteq \mathbb{Z}$ with density zero is not generalised polynomial also yield the same conclusion for all supersets E' of E with density zero (see e.g. [BK18, Thm. 3.1]). Nevertheless, it is not true that every generalised polynomial set of density zero is hereditary.

Theorem E. *There exists a set $E \subseteq \mathbb{Z}$ of density zero that is generalised polynomial but is not hereditary.*

In the context of this paper, it is natural to consider generalised polynomial expressions with variables taking rational, rather than integer, values. This corresponds to the notion of a generalised polynomial subset of $\mathbb{Q}$ (rather than $\mathbb{Z}$). In the introduction we have for simplicity stated the main results for subsets of $\mathbb{Z}$, rather than $\mathbb{Q}$. This distinction is of no significance for Theorems A and C, since any rational-valued linear recurrent sequence whose characteristic polynomial has integer coefficients is a rational multiple of an integer-valued sequence. This is not the case, however, for Theorem B, and the formulation of this result in Theorem 6.1 below is genuinely more general, and applies also to sequences of rational numbers such as $(3^i/2^i)_{i=0}^{\infty}$; the corresponding $\beta = 3/2$ is an algebraic number, but not an algebraic integer.

The plan of the paper is as follows. In Section 2, we introduce the notion of a generalised polynomial map on a number field as well as its basic properties. In Sections 3 and 4, we study linear recurrent sequences arising from Pisot numbers, and we prove Theorems D (see Theorem 3.3) and C (see Theorem 4.4). In Section 5, we obtain a similar result for Salem numbers (Theorem A, see Theorem 5.4). In Section 6, we use trace maps and finiteness results for S-unit equations to prove Theorem B. Finally, in Section 7, we construct an example of a generalised polynomial subset of $\mathbb{Z}$ that is not hereditary (Theorem E, see Theorem 7.1).

Notation. We let $\mathbb{N} = \{1, 2, 3, \dots\}$ denote the set of positive integers and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ the set of nonnegative integers. For a real number x, we let $\lfloor x \rfloor$, $\lceil x \rceil = -\lfloor -x \rfloor$, and $\lfloor x \rceil = \lfloor x + 1/2 \rfloor$ denote the floor, the ceiling, and the nearest integer. We also let $\{x\} = x - \lfloor x \rfloor$ and $\|x\|_{\mathbb{R}/\mathbb{Z}} = \min\{\{x\}, 1 - \{x\}\}$ denote the fractional part and the distance to the nearest integer. All of these expressions are generalised polynomials in x.

Acknowledgements. The authors wish to thank Boris Adamczewski for helpful comments. The first-named author was supported by National Science Centre, Poland grant number 2018/29/B/ST1/01340. The second-named author works within the framework of the LABEX MILYON (ANR-10-LABX-0070) of Université de Lyon, within the program "Investissements d'Avenir" (ANR-11-IDEX-0007) operated by the French National Research Agency (ANR).

2. Generalised polynomial maps on number fields

In this section, we introduce the notion of a generalised polynomial map in a couple of related contexts, that is, for maps defined on finite dimensional real vector spaces and for maps defined on number fields. The latter notion is new, and we carefully discuss its basic properties.

2.1. **Finite-dimensional real vector spaces.** Let V be a finite dimensional real vector space. The class of real-valued generalised polynomial maps $f \colon V \to \mathbb{R}$ is the smallest class of functions containing constant maps and linear functionals, and closed under addition, multiplication, and taking the integer part of a map, that is, replacing f by the map $\lfloor f \rfloor$ given by $\lfloor f \rfloor(x) = \lfloor f(x) \rfloor$.

A complex-valued map $f \colon V \to \mathbb{C}$ is a generalised polynomial map if the real and imaginary parts of f are real-valued generalised polynomial maps. We can give an equivalent characterisation of this class as follows. Let $\lfloor \cdot \rfloor_{\mathbb{C}} \colon \mathbb{C} \to \mathbb{Z}[i]$ be the complex integer part (or complex floor), defined by the formula $\lfloor z \rfloor_{\mathbb{C}} = \lfloor \operatorname{Re} z \rfloor + i \lfloor \operatorname{Im} z \rfloor$. One then easily checks that the class of generalised polynomial maps $f \colon V \to \mathbb{C}$ is the smallest class of functions containing complex-valued constant maps, (real-valued) linear functionals, and closed under addition, multiplication, and taking the complex integer part of a map, that is, replacing f by the map $\lfloor f \rfloor_{\mathbb{C}}$ given by $\lfloor f \rfloor_{\mathbb{C}}(x) = \lfloor f(x) \rfloor_{\mathbb{C}}$.

2.2. **Number fields.** In this subsection we introduce the notion of a generalised polynomial map defined on a number field. Even if a number field K is given as a subfield of the complex (or real) numbers, these maps are *not* defined as restrictions of generalised polynomial maps on $\mathbb{C}$; instead, this class consists, roughly speaking, of a much wider family of maps that can be expressed using the basic algebraic operations (addition and multiplication), the (complex) floor function, complex constants, and arbitrary embeddings of K into

the complex numbers. Since the floor function and the fractional part function can easily be expressed in terms of each other, replacing the floor with the fractional part leads to an alternative definition of the same class. An example of a generalised polynomial map on $K = \mathbb{Q}(\sqrt{2})$ is given by $a + b\sqrt{2} \mapsto \{a - b\sqrt{2}\}$. This map cannot be obtained as a restriction to $\mathbb{Q}(\sqrt{2})$ of a generalised polynomial map on $\mathbb{R}$ since it has infinitely many discontinuities in the interval $(0, 1)$, which is not possible for a generalised polynomial map on $\mathbb{R}$.

We now state the definition. Let K be a number field. Consider the real vector space $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$ with the embedding $\iota\colon K \to K_{\mathbb{R}}, \iota(x) = x \otimes 1$. Describing this embedding ι concretely, we get the usual map

$$K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \quad x \mapsto (\sigma_1(x), \dots, \sigma_{r_1}(x), \tau_1(x), \dots, \tau_{r_2}(x)),$$

where $\sigma_1, \dots, \sigma_{r_1}$ are all the real embeddings of K, and $\tau_1, \overline{\tau_1}, \dots, \tau_{r_2}, \overline{\tau}_{r_2}$ are all the complex embeddings of K, grouped in pairs. A map $f\colon K \to \mathbb{C}$ is a generalised polynomial map if there exists a generalised polynomial map $\widetilde{f}\colon K_{\mathbb{R}} \to \mathbb{C}$ (defined on the finite dimensional real vector space $K_{\mathbb{R}}$) such that $f = \widetilde{f} \circ \iota$. For a number field L (regarded as a subfield of $\mathbb{C}$) by a generalised polynomial map $f\colon K \to L$ we simply mean a generalised polynomial map $f\colon K \to \mathbb{C}$ whose image $f(K)$ is contained in L.

In the following proposition we list some basic properties of generalised polynomial maps on number fields.

Proposition 2.1. *Let K be a number field.*

(i) The class of generalised polynomial maps $f\colon K \to \mathbb{C}$ is the smallest class that contains constant maps, field embeddings $\sigma\colon K \to \mathbb{C}$, and is closed under addition, multiplication, and taking the complex integer part.

(ii) A map $f\colon K \to \mathbb{C}$ is a generalised polynomial on K if and only if its real and imaginary parts are generalised polynomial maps on K.

(iii) If $f\colon K \to \mathbb{C}$ is a generalised polynomial map on K and $\varphi\colon \mathbb{C} \to \mathbb{C}$ is any field automorphism of $\mathbb{C}$, then $\varphi \circ f\colon K \to \mathbb{C}$ is also a generalised polynomial map on K.

(iv) If $f\colon K \to \mathbb{C}$ is a generalised polynomial map on K and $g\colon L \to K$ is a generalised polynomial map on a number field L taking values in K, then $f \circ g\colon L \to \mathbb{C}$ is a generalised polynomial map on L.

(v) If $f\colon K \to L$ is a generalised polynomial map on K taking values in a number field L and $\alpha_1, \dots, \alpha_m$ is a basis of L over $\mathbb{Q}$, then there exist generalised polynomial maps $f_i\colon K \to \mathbb{Q}$ on K such that $f = \sum_i \alpha_i f_i$.

(vi) If $f\colon K \to \mathbb{C}$ is a generalised polynomial map on K, then the map $g\colon K \to \mathbb{C}$ given by

$$g(x) = \begin{cases} 1 & \text{if } f(x) = 0; \\ 0 & \text{otherwise} \end{cases}$$

is a generalised polynomial on K.

Proof. The claims in (i) and (ii) follow from a similar claim for generalised polynomial maps on $K_{\mathbb{R}}$.

To prove (iii), fix an automorphism φ of $\mathbb{C}$, and consider the class of maps $f\colon K \to \mathbb{C}$ such that $\varphi \circ f$ is a generalised polynomial map on K. It is clear that this class contains constant maps, field embeddings, and is closed under addition, multiplication, and the complex integer part $\lfloor\cdot\rfloor_{\mathbb{C}}$ (the latter property is due to the fact that $\sigma \circ \lfloor f \rfloor_{\mathbb{C}}$ is either $\lfloor f \rfloor_{\mathbb{C}}$ or $\overline{\lfloor f \rfloor_{\mathbb{C}}}$, depending on whether $\sigma(i) = i$ or $\sigma(i) = -i$). Thus, the claim follows from (i).

To prove (iv), fix a generalised polynomial map $g\colon L \to K$ and consider the family of maps $f\colon K \to \mathbb{C}$ such that $f \circ g$ is a generalised polynomial map on L. Using (i), (iii) and the fact that each complex embedding of K can be extended to an automorphism of $\mathbb{C}$, we verify that this family contains all generalised polynomial maps on K.

To prove (v), we regard L as a subfield of $\mathbb{C}$. Let $\sigma_1, \dots, \sigma_m$ denote all the embeddings of L into $\mathbb{C}$, and extend them in an arbitary way to automorphisms of $\mathbb{C}$ (denoted by the same letter). We can uniquely write f in the form $f = \sum_i \alpha_i f_i$ for some maps $f_i : K \to \mathbb{Q}$. We need to prove that f_i are generalised polynomial maps on K. Applying the automorphism σ_j to the above equality, we get

$$\sigma_j \circ f = \sum_i \sigma_j(\alpha_i) f_i, \qquad 1 \leqslant j \leqslant m.$$

The matrix $[\sigma_j(\alpha_i)]_{1 \leqslant i,j \leqslant m}$ is nonsingular (see e.g. [Lan02, VI, §4]), and inverting the matrix, we can write f_i as linear combinations of $\sigma_j \circ f$. Thus, the fact that f_i are generalised polynomial maps on K follows from (i) and (iii).

To prove (vi), note first that (ii) reduces the claim to the case where f takes real values (with the map g equal to the product of the maps corresponding to the real and imaginary parts of f). A real number y is zero if and only if both y and $\sqrt{2}y$ are integers; thus,

$$g(x) = \lfloor 1 - \{f(x)\} \rfloor \cdot \lfloor 1 - \{\sqrt{2}f(x)\} \rfloor,$$

and so g is a generalised polynomial map. □

2.3. **Sets of algebraic numbers.** We say that a subset S of a number field K is a generalised polynomial subset of K if its characteristic function $1_S \colon K \to \mathbb{R}$ is a generalised polynomial map on K. We should pose a warning here: sometimes, one talks about generalised polynomial subsets of $\mathbb{R}$ or $\mathbb{C}$; these are defined as the zero sets of generalised polynomial maps defined on (real vector spaces) $\mathbb{R}$ or $\mathbb{C}$. However, even when the number field K is given as a subfield of $\mathbb{R}$ or $\mathbb{C}$, these notions do not coincide! In fact, in the above sense no number field K is a generalised polynomial subset of $\mathbb{C}$, while a number field K is clearly a generalised polynomial subset of itself. Of course, a generalised polynomial subset of $\mathbb{R}$ that happens to be contained in a number field K (for example, $\mathbb{Q}$) is a generalised polynomial subset of K. For this reason, in this paper we shall not talk about generalised polynomial subsets of $\mathbb{R}$ or $\mathbb{C}$, but only about generalised polynomial subsets of number fields (or, later, algebraic numbers).

Since $1_{S\cap T} = 1_S 1_T$ and $1_{K\setminus S} = 1_K - 1_S$, the class of generalised polynomial subsets of K is closed under finite unions, finite intersections, and complements. Proposition 2.1(vi) says that the zero set of a generalised polynomial map $f \colon K \to \mathbb{C}$ is a generalised polynomial set. Moreover, whether a set is generalised polynomial or not is invariant under translation, applying a bijective $\mathbb{Q}$-linear map (or, more generally, a generalised polynomial bijection $K \to K$ with generalised polynomial inverse), as well as adding or removing finitely many elements. In the following proposition we list some examples of generalised polynomial subsets of number fields.

Proposition 2.2. *Let K be a number field. The following subsets of K are generalised polynomial:*

(i) any $\mathbb{Q}$-subvector space V of K;
(ii) any subfield $L \subseteq K$;
(iii) any lattice $\Lambda \subseteq K$;
(iv) the ring $\mathcal{O}_K$ of algebraic integers in K;
(v) the group of units $\mathcal{O}_K^*$;
(vi) any finite index subgroup of $\mathcal{O}_K^*$;
(vii) the set of Pisot units in K;
(viii) the set of Salem numbers in K.

(The statements in (vii) and (viii) only make sense when K is given a subfield of $\mathbb{R}$.)

Proof. For (i), we first note that since the family of generalised polynomial subsets is closed under taking finite intersections, we may assume that V is of codimension 1; moreover, since the notion is stable under applying a bijective $\mathbb{Q}$-linear map, it is sufficient to prove that a single codimension 1 subspace V is generalised polynomial. We may thus choose V to be $\{x \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(x) = 0\}$, in which case the claim follows from Proposition 2.1(vi), since $\mathrm{Tr}_{K/\mathbb{Q}}$ is a generalised polynomial map on K. This proves (i), and (ii) is an immediate corollary.

For (iii), choose a basis $v_1, \dots, v_m$ of Λ, and extend it to a basis $v_1, \dots, v_n$ of $K_{\mathbb{R}}$. Let $v_1^*, \dots, v_n^*$ denote the dual basis, i.e. linear maps $v_i^* \colon K_{\mathbb{R}} \to \mathbb{R}$ such that $v_i^*(v_i) = 1$ and $v_i^*(v_j) = 0$ for $1 \leqslant i, j \leqslant m$ with $i \neq j$. Then Λ is the common set of zeros of the generalised polynomial maps $\{v_1^*\}, \{v_2^*\}, \dots \{v_m^*\}, v_{m+1}^*, v_{m+2}^*, \dots, v_n^*$. Item (iv) follows directly from (iii) since $\mathcal{O}_K$ is a lattice.

For (v), we characterise the units as algebraic integers α of norm $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 1$.For (vi), let H be a subgroup of $\mathcal{O}_K^*$ of finite index. By Chevalley's theorem [Che51, Thm. 1], H is a congruence subgroup, meaning that $H = \mathcal{O}_K^* \cap \Lambda$ for some Λ that is a union of finitely many cosets of a lattice. It remains to recall that $\mathcal{O}_K^*$ and Λ are generalised polynomial.

For (vii), we characterize Pisot units α in K by requiring that: i) α be a unit; ii) α be positive; and iii) $|\sigma(\alpha)|^2 = \sigma(\alpha)\overline{\sigma}(\alpha)$ lie in the interval $(0, 1)$ for all nonidentity embeddings $\sigma \colon K \to \mathbb{C}$. The fact that the first two conditions define a generalised polynomial subset follows from (v), since positive units form a subgroup of the group of units of index 2; the last condition defines the common zero set of the generalised polynomial maps $n \mapsto \lfloor \sigma(n)\overline{\sigma}(n) \rfloor$ (with the element 0 removed).

For (vii), we similarly characterise Salem numbers α in K by requiring that i) α be a unit; ii) α be positive; iii) $|\sigma(\alpha)|^2 = 1$ for all but two embeddings σ; iv) $1/\alpha$ be an algebraic conjugate of α. For the first three conditions, we apply the same reasoning as before. The fourth condition says that there exist two embeddings σ and τ of K is $\mathbb{C}$ with $\sigma(\alpha) = \tau(\alpha)^{-1}$, which is also easily expressed in terms of generalised polynomial maps. □

It is worthwhile to note that the set of Pisot *numbers* is in general not a generalised polynomial subset; in fact, when $K = \mathbb{Q}$, the set of Pisot numbers is simply the set of integers $\geqslant 2$, which is not generalised polynomial; this can be inferred, for instance, from the general fact that for a generalised polynomial set $E \subseteq \mathbb{Z}$ the limit $|E \cap [M, M+N)|/N$ converges uniformly in M as $N \to \infty$; cf. [Kon21, Ex. B.2]. On the other hand, the set of Pisot numbers and their negatives is a generalised polynomial subset (by a similar argument as for Pisot units).

Let $\mathbb{Q}^{\mathrm{alg}}$ denote the field of algebraic numbers. We say that a subset S of $\mathbb{Q}^{\mathrm{alg}}$ is generalised polynomial if $S \cap K$ is a generalised polynomial subset of K for every number field K. From Proposition 2.2 we get that if S is itself a subset of some number field L, then S is a generalised polynomial subset of $\mathbb{Q}^{\mathrm{alg}}$ if and only if it is a generalised polynomial subset of L. Proposition 2.2 also immediately implies the following result.

Proposition 2.3. *The following sets of algebraic numbers are generalised polynomial:*

(*i*) *the ring of algebraic integers;*
(*ii*) *the group of algebraic units;*
(*iii*) *the set of Pisot units;*
(*iv*) *the set of Salem numbers.*

3. Pisot numbers: Number fields

In this section we prove Theorem D. We begin with a basic observation.

Lemma 3.1. *Let β be a Pisot unit and let $K = \mathbb{Q}(\beta)$. Assume that $\mathcal{O}_K^*$ has rank 1. Then the set $\{\beta^i \mid i \in \mathbb{N}_0\}$ is a generalised polynomial subset of K.*

Proof. The set $\{\beta^i \mid i \in \mathbb{Z}\}$ is a finite-index subgroup of the group of units $\mathcal{O}_K^*$, and hence it is a generalised polynomial subset of K by Proposition 2.2(vi). The set of all Pisot units in K is also generalised polynomial by Proposition 2.2(vii). It remains to observe that the intersection of these two sets is $\{\beta^i \mid i \in \mathbb{N}\}$. □

For technical reasons, it is easier to prove Theorem D in the case where β is sufficiently large. Thus, we will first prove an analogous result with β replaced with a sufficiently large power β^m.

Proposition 3.2. *Let β be a Pisot unit and let $K = \mathbb{Q}(\beta)$. Assume that $\mathcal{O}_K^*$ has rank 1. Then there exists m_0 such that for every integer $m \geqslant m_0$ and set $I \subseteq \mathbb{N}_0$, the set $\{\beta^{im} \mid i \in I\}$ is a generalised polynomial subset of K.*

Proof. Since β is a Pisot number, we can find $\rho > 1$ such that $\rho < \beta$ and for all conjugates α of β other than β itself we have $|\alpha| < 1/\rho$. Let $m \geqslant m_0$ be a large integer, where $m_0 > 0$ remains to be determined in the course of the argument, and let $\gamma := \beta^m$. Consider the real number

$$\xi = \sum_{i \in I} \frac{\beta}{\gamma^i}. \tag{3}$$

For any integer i, the trace $\mathrm{Tr}_{K/\mathbb{Q}}(\beta^i)$ is an integer. This implies that $\|\beta^i\|_{\mathbb{R}/\mathbb{Z}} = O(1/\rho^i)$ for $i \geqslant 0$; on the other hand, for $i \leqslant 0$ we trivially have $\|\beta^i\|_{\mathbb{R}/\mathbb{Z}} = O(1/\rho^{|i|})$. Thus, for $i, j \in \mathbb{N}$, we have the estimates

$$\left\|\beta\gamma^{j-i}\right\|_{\mathbb{R}/\mathbb{Z}} = \left\|\beta^{1+m(j-i)}\right\|_{\mathbb{R}/\mathbb{Z}} = \begin{cases} \|\beta\|_{\mathbb{R}/\mathbb{Z}} & \text{if } i = j; \\ O(1/\rho^{m|i-j|}) & \text{if } i \neq j, \end{cases} \tag{4}$$

where the constant implicit in the $O(\cdot)$-notation depends on β, but not on m. As a consequence, taking the sum over all $i \in I$, we obtain

$$\left\|\gamma^j \xi\right\|_{\mathbb{R}/\mathbb{Z}} = 1_I(j)\,\|\beta\|_{\mathbb{R}/\mathbb{Z}} + O\Big(\sum_{i \in I \setminus \{j\}} 1/\rho^{m|i-j|}\Big) = 1_I(j)\,\|\beta\|_{\mathbb{R}/\mathbb{Z}} + O\left(1/\rho^m\right). \tag{5}$$

Assume that m is large enough so that the error term in (5) is strictly smaller than $\|\beta\|_{\mathbb{R}/\mathbb{Z}}/3$. Then for every $j \in \mathbb{N}$ we have the equivalence

$$j \in I \quad \text{if and only if} \quad \left\|\gamma^j \xi\right\|_{\mathbb{R}/\mathbb{Z}} \geqslant \frac{2}{3}\|\beta\|_{\mathbb{R}/\mathbb{Z}}. \tag{6}$$

Let $g\colon K \to \{0,1\}$ be given by

$$g(x) = \begin{cases} 1 & \text{if } \left\|\gamma^j x\right\|_{\mathbb{R}/\mathbb{Z}} \in \left[\frac{2}{3}\|\beta\|_{\mathbb{R}/\mathbb{Z}}, \frac{1}{2}\right]; \\ 0 & \text{otherwise.} \end{cases}$$

We deduce from Proposition 2.1(vi) that g is a generalised polynomial map. By Lemma 3.1, the set $\left\{\gamma^i \;\middle|\; i \in \mathbb{N}_0\right\}$ is a generalised polynomial subset of K. It follows from the preceding discussion that for all $x \in \left\{\gamma^i \;\middle|\; i \in \mathbb{N}_0\right\}$ we have $g(x) = 1$ if and only if $x \in \left\{\gamma^i \;\middle|\; i \in I\right\} = \left\{\beta^{im} \;\middle|\; i \in I\right\}$. □

Theorem 3.3 (= Theorem D)**.** *Let β be a Pisot unit such that $\mathcal{O}^*_{\mathbb{Q}(\beta)}$ has rank 1. Let I be an arbitrary subset of $\mathbb{N}_0$. Then the set $\left\{\beta^i \;\middle|\; i \in I\right\}$ is a generalised polynomial subset of $\mathbb{Q}(\beta)$.*

Proof. Let m be an integer that is sufficiently large for the conclusion of Proposition 3.2 to hold. Since generalised polynomial sets are closed under finite unions, it suffices to show that for each $0 \leqslant a < m$, the set $\left\{\beta^i \;\middle|\; i \in I,\ i \equiv a \bmod m\right\}$ is generalised polynomial. Since generalised polynomial sets are also invariant under dilation, we may freely assume that $a = 0$. The statement now follows from Proposition 3.2. □

Remark 3.4. Similar techniques could also be applied in the situation where β is an arbitrary Pisot unit without assumming that the unit group $\mathcal{O}^*_{\mathbb{Q}(\beta)}$ has rank 1. However, in this case we no longer know whether or not the set $\left\{\beta^i \;\middle|\; i \in \mathbb{N}_0\right\} \subseteq \mathbb{Q}(\beta)$ is generalised polynomial. As a consequence, we would only obtain a relative result; namely, for each set $I \subseteq \mathbb{N}_0$, the set $\left\{\beta^i \;\middle|\; i \in I\right\}$ is a generalised polynomial subset of $\left\{\beta^i \;\middle|\; i \in \mathbb{N}_0\right\}$. In other words, there exists a generalised polynomial set $S \subseteq \mathbb{Q}(\beta)$ such that for $i \in \mathbb{N}_0$ we have $\beta^i \in S$ if and only if $i \in I$. Since it is not clear how interesting this generalisation is, we do not go into the details at this point.

4. Pisot numbers: Integers

In this section, we prove Theorem C. We first recall a well known fact on linear recurrent sequences.

Lemma 4.1. *Let β be an algebraic number, let $K = \mathbb{Q}(\beta)$, and let $m = [K : \mathbb{Q}]$ be the degree of β. Let $(n_i)_{i=0}^{\infty}$ be a linear recurrent sequence with rational values and with characteristic polynomial the minimal polynomial of β.*

(i) There exists a unique $x \in K$ such that

$$n_i = \mathrm{Tr}_{K/\mathbb{Q}}(\beta^i x) \quad \text{for all } i \geqslant 0.$$

(ii) Assume moreover that $(n_i)_{i=0}^{\infty}$ is not identically zero. Suppose that $(n'_i)_{i=0}^{\infty}$ is another linear recurrent sequence with characteristic polynomial the minimal polynomial of β and taking values in some extension L of $\mathbb{Q}$. Then the sequence $(n'_i)_{i=0}^{\infty}$ can be written as a linear combination of the sequences $(n_{i+j})_{i=0}^{\infty}$, $0 \leqslant j < m$, with coefficients in L.

Proof. The vector space V of all rational-valued linear recurrent sequences with characteristic polynomial the minimal polynomial of β is clearly m-dimensional. Since all sequences of the form $(\mathrm{Tr}_{K/\mathbb{Q}}(\beta^i x))_{i=0}^{\infty}$ lie in this space, (i) follows from the nondegeneracy of the bilinear map $(x, y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy)$. To prove (ii), write $(n'_i)_{i=0}^{\infty}$ as an L-linear combination of sequences in V, and apply (i). □

An elementary but key fact about integer-valued sequences satisfying a Pisot linear recurrence is that each successive term can be computed by a simple generalised polynomial formula involving only the previous term. We record this in the following lemma.

Lemma 4.2. *Let $(n_i)_{i=0}^{\infty}$ be an integer-valued sequence satisfying a linear recurrence whose characteristic polynomial is the minimal polynomial of a Pisot number β. Then for each $j \geqslant 0$ there exists some i_0 such that for all integers $i \geqslant i_0$ we have $n_{i+j} = \left\lfloor \beta^j n_i \right\rceil$.*

Proof. Lemma 4.1(i) allows us to write the sequence $(n_i)_{i=0}^{\infty}$ in the form

$$n_i = \sum_{\alpha} c_\alpha \alpha^i, \tag{7}$$

where the sum runs over all conjugates α of β, and c_α are complex constants. Since β is Pisot, we have $\alpha^i \to 0$ as $i \to \infty$ for each $\alpha \neq \beta$, and hence

$$n_i - c_\beta \beta^i \to 0 \quad \text{as } i \to \infty. \tag{8}$$

It follows that

$$n_{i+j} - \beta^j n_i \to 0 \quad \text{as } i \to \infty. \tag{9}$$

Thus, $n_{i+j} = \lfloor \beta^j n_i \rceil$ for sufficiently large i. □

Lemma 4.2 allows us to pass between the terms of any two linear recurrent sequences satisfying the same Pisot linear recurrence by applying a generalised polynomial map.

Proposition 4.3. *Let β be a Pisot number and let $K = \mathbb{Q}(\beta)$. Let $(n_i)_{i=0}^{\infty}$ and $(n'_i)_{i=0}^{\infty}$ be two sequences taking values in $\mathbb{Q}(\beta)$ and satisfying a linear recurrence whose characteristic polynomial is the minimal polynomial of β. Assume also that $(n_i)_{i=0}^{\infty}$ is not identically zero. Then there exists a generalised polynomial map $g\colon \mathbb{Q}(\beta) \to \mathbb{Q}(\beta)$ such that $g(n_i) = n'_i$ for all but finitely many positive integers i.*

Proof. Replacing n_i with $\mathrm{Tr}_{K/\mathbb{Q}}(\xi n_i)$ for suitably chosen $\xi \in K$, we may freely assume that n_i are integers for all i. Let m denote the degree of β. By Lemma 4.1(ii), we may express $(n'_i)_{i=0}^{\infty}$ as

$$n'_i = \sum_{j=0}^{m-1} w_j n_{i+j} \quad \text{for all } i \in \mathbb{N}_0,$$

where $w_j \in K$, $0 \leqslant j < m$, are some coefficients. It follows from Lemma 4.2 that

$$n'_i = \sum_{j=0}^{m-1} w_j \lfloor \beta^j n_i \rceil \quad \text{for all sufficiently large } i.$$

Thus, we may take $g(n) = \sum_{j=0}^{m-1} w_j \lfloor \beta^j n \rceil$. □

We can now prove the following result, which is a slightly stronger version of Theorem C.

Theorem 4.4. *Let β be a Pisot unit such that $\mathcal{O}^*_{\mathbb{Q}(\beta)}$ has rank 1, and let $(n_i)_{i=0}^{\infty}$ be a linear recurrent sequence of rational numbers with characteristic polynomial the minimal polynomial of β. Let I be an arbitrary subset of $\mathbb{N}_0$. Then the set $\{n_i \mid i \in I\}$ is a generalised polynomial subset of $\mathbb{Q}$.*

Proof. We may assume that $(n_i)_{i=0}^{\infty}$ is not identically zero. It follows from Proposition 4.3 that there exists a generalised polynomial map $g\colon \mathbb{Q} \to \mathbb{Q}(\beta)$ such that $g(n_i) = \beta^i$ for all sufficiently large i. The set $\{\beta^i \mid i \in I\} \subseteq \mathbb{Q}(\beta)$ is a generalised polynomial set by Theorem 3.3, and the set $\{n_i \mid i \in \mathbb{N}_0\}$ is generalised polynomial by Theorem 1.1. The claim follows from the fact that the class of generalised polynomial sets is stable under taking preimages by generalised polynomial maps, finite intersections, and finite modifications. □

5. Salem numbers

In this section, we prove Theorem A. As we have already pointed out, the notion of a generalised polynomial subset is preserved by applying a bijective generalised polynomial map with generalised polynomial inverse. The following lemma records a similar principle, but allowing for the inverse to be defined on a case-by-case basis.

Lemma 5.1. *Let K and L be number fields, let $S \subseteq K$ be a generalised polynomial set, and let $f\colon K \to L$ and $g_1, g_2, \ldots, g_r\colon L \to K$ be generalised polynomial maps. Suppose that for each $x \in S$ there exists $1 \leqslant i \leqslant r$ such that $g_i(f(x)) = x$. Then $f(S)$ is a generalised polynomial subset of L.*

Proof. Let $1 \leqslant i \leqslant r$ and put

$$S_i := \{x \in S \mid g_i(f(x)) = x\}.$$

It follows from Proposition 2.1(vi) that S_i is a generalised polynomial subset of K. We claim that

$$f(S_i) = \{y \in L \mid g_i(y) \in S_i,\ f(g_i(y)) = y\}. \tag{10}$$

Indeed, if $y \in f(S_i)$, say $y = f(x)$ for some $x \in S_i$, then $g_i(y) = g_i(f(x)) = x \in S_i$ and $f(g_i(y)) = f(g_i(f(x))) = f(x) = y$. Conversely, if $y \in L$, $g_i(y) \in S_i$ and $y = f(g_i(y))$ then clearly $y \in f(S_i)$. From (10) we deduce that $f(S_i)$ is a generalised polynomial subset of L. Since $f(S) = \bigcup_{i=1}^{r} f(S_i)$, we conclude that $f(S)$ is a generalised polynomial subset of L. □

For linear recurrent sequences of Pisot type, we proved that one can pass between the corresponding terms of the sequences using a generalised polynomial map (see Proposition 4.3). For linear recurrent sequences of Salem type an analogous result holds if we allow instead the use of a finite family of generalised polynomial maps.

Proposition 5.2. *Let β be a Salem number and let L be the splitting field of the minimal polynomial of β. Let $(n_i)_{i=0}^{\infty}$ be a sequence of rational numbers satisfying a linear recurrence whose characteristic polynomial is the minimal polynomial of β. Assume that $(n_i)_{i=0}^{\infty}$ is not identically zero. Then there exists a finite family $\{g_c\}_{c\in\mathcal{C}}$ of generalised polynomial maps $g_c\colon \mathbb{Q} \to L$ such that for each $i \in \mathbb{N}_0$ there exists $c \in \mathcal{C}$ such that $g_c(n_i) = \beta^i$.*

Proof. Let $i \in \mathbb{N}_0$. Using Lemma 4.1(i), we can write n_i in the form $n_i = \mathrm{Tr}_{\mathbb{Q}(\beta)/\mathbb{Q}}(\beta^i x)$ for some $x \in \mathbb{Q}(\beta)$, which allows us to express n_i in the form

$$n_i = \sum_{\alpha} w_\alpha \alpha^i,$$

where the sum runs over all conjugates α of β and $w_\alpha \in L$ are constants. Since w_α are images of x by embeddings of $\mathbb{Q}(\beta)$ into $\mathbb{C}$, and since $x \neq 0$ (otherwise the sequence $(n_i)_{i=0}^{\infty}$ would be identically zero), we see that w_α are all nonzero. Since all $\alpha \neq \beta$ have absolute value 1 or $1/\beta \leqslant 1$, we have for each $j \in \mathbb{N}_0$ the estimate

$$\begin{aligned} \left|\lfloor \beta^j n_i \rfloor - n_{i+j}\right| &\leqslant 1 + \left|\beta^j \sum_{\alpha} w_\alpha \alpha^i - \sum_{\alpha} w_\alpha \alpha^{i+j}\right| \\ &\leqslant 1 + \sum_{\alpha\neq\beta} |w_\alpha| \left(\beta^j + 1\right) = O(\beta^j), \end{aligned}$$

with the implicit constant depending on β and the sequence $(n_i)_{i=0}^{\infty}$, but not on j. It follows that there exist constants $c_j^{(i)} \in \mathbb{Z}$ with $\left|c_j^{(i)}\right| = O(\beta^j)$ such that

$$\lfloor \beta^j n_i \rfloor - c_j^{(i)} = n_{i+j} = \sum_{\alpha} w_\alpha \alpha^{i+j}. \tag{11}$$

Let m be the degree of β and consider the following system of linear equations in x_α and y_j:

$$y_j = \sum_{\alpha} w_\alpha \alpha^j x_\alpha \quad \text{for } 0 \leqslant j < m. \tag{12}$$

Note that (12) holds for $x_\alpha = \alpha^i$ and $y_j = \lfloor \beta^j n_i \rfloor - c_j^{(i)}$. The determinant of the matrix $(w_\alpha \alpha^j)_{\alpha,j}$ is nonzero as the product of w_α (which are nonzero) and a Vandermonde's determinant. Thus (12) has a unique solution, say

$$x_\alpha = \sum_{j=0}^{m-1} \gamma_{j,\alpha} y_j, \tag{13}$$

where $\gamma_{j,\alpha} \in L$ are some constants. Put $C_j := \max_i \left|c_j^{(i)}\right| = O(\beta^j)$. Consider the set

$$\mathcal{C} = \left\{(c_j)_{j=0}^{2d-1} \;\middle|\; c_j \in \mathbb{Z},\ |c_j| \leqslant C_j \text{ for all } 0 \leqslant j < m\right\} \tag{14}$$

and for each $c = (c_j)_{j=0}^{2d-1} \in \mathcal{C}$ the generalised polynomial

$$g_c(n) = \sum_{j=0}^{m-1} \gamma_{j,\alpha} \left(\lfloor \beta^j n \rfloor - c_j \right). \tag{15}$$

It follows from the preceding discussion that $\beta^i = g_c(n_i)$ for $c \in \mathcal{C}$ given by $c_j := c_j^{(i)}$, $0 \leqslant j < m$. □

Lemma 5.3. *Let K be a number field and let $\beta \in K$ be a Salem number. Then $\left\{\beta^j \;\middle|\; j \in \mathbb{N}_0\right\} \subseteq K$ is a generalised polynomial subset of K.*

Proof. The set of Salem numbers in $\mathbb{Q}(\beta)$ is of the form $\{\gamma^i \mid i \in \mathbb{N}\}$ for some Salem number γ [Sal45, p. 169]. From Chevalley's theorem we deduce that the group $\langle\beta\rangle$ is a congruence subgroup of $\langle\gamma\rangle$, and hence there exists some Λ that is a union of finitely many cosets of a lattice with the property that $\langle\beta\rangle = \langle\gamma\rangle \cap \Lambda$. The fact that $\left\{\beta^j \;\middle|\; j \in \mathbb{N}_0\right\}$ is generalised polynomial follows then from Proposition 2.2. □

We can now deduce the following result, which is a slightly stronger version of Theorem A.

Theorem 5.4. *Let β be a Salem number and let $(n_i)_{i=0}^{\infty}$ be a linear recurrent sequence of rational numbers with characteristic polynomial the minimal polynomial of β. Then the set $\{n_i \mid i \in \mathbb{N}_0\}$ is a generalised polynomial subset of $\mathbb{Q}$.*

Proof. Let $K = \mathbb{Q}(\beta)$ and let L be the splitting field of the minimal polynomial of β. We may suppose that the sequence $(n_i)_{i=0}^{\infty}$ is not identically zero. Using Lemma 4.1(i), we write the sequence $(n_i)_{i=0}^{\infty}$ in the form $n_i = \mathrm{Tr}_{K/\mathbb{Q}}(\beta^i x)$ for some $x \in K$. Let $S = \left\{\beta^j \;\middle|\; j \in \mathbb{N}_0\right\} \subseteq K$, let $f\colon L \to \mathbb{Q}$ be the map given on K by $f(y) = \mathrm{Tr}_{K/\mathbb{Q}}(yx)$, and extended arbitrarily to a generalised polynomial map on L, and let $g_c\colon \mathbb{Q} \to L$ be the maps satisfying the claim of Proposition 5.2. The result follows by applying Lemma 5.1 to S, f, and $\{g_c\}_{c\in\mathcal{C}}$. □

6. Generalised polynomial sets of powers

In this section, we prove the following result, which is a stronger variant of Theorem B.

Theorem 6.1. *Let β be an algebraic number. Suppose that there exists a linear recurrent sequence $(n_i)_{i=0}^{\infty}$ of rational numbers with characteristic polynomial the minimal polynomial of β that is not identically zero and is such that the set of values $\{n_i \mid i \in \mathbb{N}_0\}$ is a generalised polynomial subset of $\mathbb{Q}$. Then the set $\left\{\beta^i \;\middle|\; i \in \mathbb{N}_0\right\}$ is a generalised polynomial subset of $\mathbb{Q}(\beta)$.*

Since the proof is somewhat lengthy and technical, we first sketch the main idea. Let $K = \mathbb{Q}(\beta)$. The sequence $(n_i)_{i=0}^{\infty}$ can be written in the form

$$n_i = \mathrm{Tr}_{K/\mathbb{Q}}(\beta^i z)$$

for some $z \in K$. Let X be the set of values of $(n_i)_{i=0}^{\infty}$; by assumption, X is a generalised polynomial subset of $\mathbb{Q}$. We consider the set Y of all elements $x \in K$ such that $\mathrm{Tr}_{K/\mathbb{Q}}(\beta^k xz)$ belongs to X for a large finite number of values of k, $0 \leqslant k < N$. Such a set is clearly a generalised polynomial subset of K. We might expect that any $x \in Y$ is necessarily of the form $x = \beta^i$ for some $i \geqslant 0$; if true, this would conclude the proof. Unfortunately, while this claim is quite close to being true, some caveats apply. First, some nondegeneracy conditions are required for β; the claim is usually false if β is a root of unity, e.g. for $\beta = i$, $z = 1$, in which case

$$X = \{-2, 0, 2\} \qquad \text{and} \qquad Y = \{\pm 1, \pm i, \pm(1+i), \pm(1-i)\}$$

provided that $N \geqslant 2$. Perhaps less obviously, the claim is also false when β has a conjugate of the form $\omega\beta$ with ω a root of unity, e.g. for $\beta = \sqrt{2}$, $z = 1$, in which case

$$X = \{0\} \cup \{2^{i+1} \mid i \in \mathbb{N}_0\} \qquad \text{and} \qquad Y = \{0\} \cup \{2^i \mid i \in \mathbb{N}_0\} \cup \{2^{i-1}\sqrt{2} \mid i \in \mathbb{N}_0\} \cup \{2^i + 2^{j-1}\sqrt{2} \mid i, j \in \mathbb{N}_0\}$$

provided that $N \geqslant 2$. Second, the claim is false for a different reason if β and β^{-1} are conjugate, e.g. for $\beta = 2 + \sqrt{3}$, $z = 1$, in which case $\mathrm{Tr}_{K/\mathbb{Q}}(\beta^i) = \mathrm{Tr}_{K/\mathbb{Q}}(\beta^{-i})$ and one can show that

$$Y = \{\beta^i \mid i \in \mathbb{Z}\}$$

provided that $N \geqslant 3$. Finally, a finite number of exceptions are possible, namely $x = 0$ and $x = \beta^i$ for some negative values of i. Nevertheless, with these three situtations properly accounted for, the claim becomes correct. To prove these results, we need to study when the values of traces coincide along certain geometric progressions.

We begin by recalling two well known facts, whose proofs we include for lack of appropriate reference.

Lemma 6.2. *Let β and γ be conjugate algebraic numbers that are neither zero nor roots of unity. Let k and l be nonzero integers such that $\beta^k = \gamma^l$. Then $k = \pm l$ and $\gamma = \omega\beta^{\pm 1}$ for some root of unity ω.*

Proof. Let σ be an automorphism of the Galois closure of $\mathbb{Q}(\beta)$ that maps β to γ. For each integer t we have $\sigma^t(\beta^l) = \sigma^{t-1}(\beta^k)$. Hence, setting n to be the order of σ and applying n times the automorphism σ to β^{l^n}, we get

$$\beta^{l^n} = \sigma^n(\beta^{l^n}) = \beta^{k^n}.$$

Since β is neither zero nor a root of unity, it follows that $l = \pm k$. Thus, $(\beta\gamma^{\mp 1})^k = 1$, and $\beta\gamma^{\mp 1}$ is a root of unity. □

Lemma 6.3. *Let β be a nonzero algebraic number, let m denote the degree of β, let $K = \mathbb{Q}(\beta)$, and let $\gamma, x, y \in K$.*

(i) Suppose that $\mathrm{Tr}_{K/\mathbb{Q}}(\beta^i x) = \mathrm{Tr}_{K/\mathbb{Q}}(\beta^i y)$ for $0 \leqslant i < m$. Then $x = y$.

(ii) Suppose that $\mathrm{Tr}_{K/\mathbb{Q}}(\beta^i x) = \mathrm{Tr}_{K/\mathbb{Q}}(\gamma^i y)$ for $0 \leqslant i < 2m$ and that $x \neq 0$. Then there exists an automorphism σ of K such that $\sigma(\beta) = \gamma$ and $\sigma(x) = y$.

Proof. Item (i) follows from the fact that $\mathrm{Tr}_{K/\mathbb{Q}}$ induces a nondegenerate quadratic form on K. Hence, it remains to prove (ii).

Let $r, s \in \mathbb{Q}[\![T]\!]$ be the generating functions associated to the sequences $(\mathrm{Tr}_{K/\mathbb{Q}}(\beta^i x))_{i=0}^{\infty}$ and $(\mathrm{Tr}_{K/\mathbb{Q}}(\gamma^i y))_{i=0}^{\infty}$, that is,

$$r = \sum_{i \geqslant 0} \mathrm{Tr}_{K/\mathbb{Q}}(\beta^i x) T^i, \qquad s = \sum_{i \geqslant 0} \mathrm{Tr}_{K/\mathbb{Q}}(\gamma^i y) T^i.$$

Since these sequences are linear recurrent and satisfy the same linear recurrences as $(\beta^i)_{i=0}^{\infty}$ and $(\gamma^i)_{i=0}^{\infty}$, respectively, we may write $r = p/f$, $s = q/g$, where f is the minimal polynomial of β, g is the minimal polynomial of γ, and $p, q \in \mathbb{Q}[X]$ are polynomials of degree $\deg p < \deg f = m$, $\deg q < \deg g \leqslant m$. Our assumption guarantees that $pg - qf = fg(r - s)$, regarded as a power series in T, is divisible by T^{2m}. Since $pg - qf$ is also a polynomial of degree $< 2m$, we conclude that it is the zero polynomial, and hence $r = s$. Since r is not identically zero, it follows that $f = g$, and so β and γ are conjugate. Let σ the automorphism of K such that $\sigma(\beta) = \gamma$. Then

$$\mathrm{Tr}_{K/\mathbb{Q}}(\gamma^i \sigma(x)) = \mathrm{Tr}_{K/\mathbb{Q}}(\beta^i x) = \mathrm{Tr}_{K/\mathbb{Q}}(\gamma^i y).$$

The equality $\sigma(x) = y$ now follows from (i). □

We will use two fundamental (and related) results: the finiteness of the number of solutions of the S-unit equation and the Skolem–Mahler–Lech theorem. The first of these results was proved by Evertse [Eve84] and van der Poorten–Schlickewei [vdPS91]. In the formulation of [vdPS91, Thm. 2] it says that if K is a field of characteristic zero, G is a finitely generated subgroup of the multiplicative group of K, and $a_1, \ldots, a_m$ are nonzero elements of K, then the equation

$$\sum_{i=1}^{n} a_i g_i = 0$$

has, up to scaling, only finitely many solutions $(g_i)_{i=1}^n$ with $g_i \in G$ such that no proper sub-sum $\sum_{i \in I} a_i g_i$, $\emptyset \neq I \subsetneq \{1, \ldots, m\}$, vanishes; here, considering solutions up to scaling means that we identify solutions (g_i) and (g_i') such that g_i/g_i' is indepedent of i. The Skolem–Mahler–Lech theorem [Sko34, Lec53, Mah56] says that the set of zeros of a linear recurrent sequence over a field of characteristic zero is a union of a finite set and finitely many arithmetic progressions. This implies that a non-constant linear recurrent sequence whose characteristic polynomial is the minimal polynomial of an algebraic number β has only finitely many zeros provided that β satisfies the following nondegeneracy property:

(†) $\qquad \alpha/\alpha'$ is not a root of unity for all conjugates $\alpha \neq \alpha'$ of β.

(Alternatively, this could also be deduced directly from the S-unit equation.) Moreover, the number of zeros is bounded by a constant that depends only on the field $\mathbb{Q}(\beta)$ [Sch96, Thm. 1.1].

The property (†) will appear several times in the remainder of this section. We note that (†) is equivalent to saying that $\mathbb{Q}(\beta) = \mathbb{Q}(\beta^d)$ for all $d \in \mathbb{N}$. (This is because the set of conjugates of β^d is equal to the set of d-th powers of conjugates of β.) Moreover, for each algebraic number γ, there exists an integer $d \in \mathbb{N}$ such that (†) holds for $\beta = \gamma^d$.

Proposition 6.4. *Let β be an algebraic number satisfying (†), let $K = \mathbb{Q}(\beta)$, and let $a_0, \dots, a_m \in K$. Then for all but finitely many nonnegative integer solutions $(n_0, n_1, \dots, n_m) \in \mathbb{N}_0^{m+1}$ of*

$$\mathrm{Tr}_{K/\mathbb{Q}}\left(\sum_{i=0}^{m} a_i \beta^{n_i}\right) = 0 \tag{16}$$

there exists a nonempty subset I of $\{0, 1, \dots, m\}$ such that

$$\sum_{i \in I} a_i \beta^{n_i} = 0. \tag{17}$$

Additionally, if β has no conjugates of the form $\omega\beta^{-1}$ with ω a root of unity, then the same conclusion holds for solutions $(n_0, n_1, \dots, n_m) \in \mathbb{Z}^{m+1}$.

Remark 6.5. Before proceeding with the proof, observe that the assumptions in Proposition 6.4 are in fact necessary for the claims to hold. In fact, if β fails to satisfy condition (†), then there exists an integer $d \in \mathbb{N}$ such that $\mathbb{Q}(\beta^d)$ is a proper subfield of K, and we can find some nonzero γ in the kernel of the map $\mathrm{Tr}_{K/\mathbb{Q}(\beta^d)} \colon K \to \mathbb{Q}(\beta^d)$. Let $m = [K : \mathbb{Q}] - 1$, and write γ in the form $\gamma = \sum_{i=0}^{m} a_i \beta^i$, $a_i \in \mathbb{Q}$. For any $n \in \mathbb{N}_0$ we have

$$\mathrm{Tr}_{K/\mathbb{Q}}(\sum_{i=0}^{m} a_i \beta^{i+nd}) = \mathrm{Tr}_{K/\mathbb{Q}}(\beta^{nd}\gamma) = \mathrm{Tr}_{\mathbb{Q}(\beta^d)/\mathbb{Q}}(\beta^{nd}\,\mathrm{Tr}_{K/\mathbb{Q}(\beta^d)}(\gamma)) = 0.$$

Note that no nonempty sub-sum of $\sum_{i=0}^{m} a_i \beta^{i+nd}$ vanishes. This contradicts the first claim of Proposition 6.4.

Now suppose that β has a conjugate of the form $\omega\beta^{-1}$ for some root of unity ω. Then β^d is conjugate to β^{-d} for some $d \in \mathbb{N}$, and so

$$\mathrm{Tr}_{K/\mathbb{Q}}(\beta^{nd} - \beta^{-nd}) = 0$$

for all $n \in \mathbb{N}$. This contradicts the second claim of Proposition 6.4.

Proof of Proposition 6.4. Let $\mathcal{N} \subseteq \mathbb{Z}^{m+1}$ be an arbitrary infinite family of solutions $(n_i)_{i=0}^m$ to (16). We further assume that either $\mathcal{N}$ is a subset of $\mathbb{N}_0^{m+1}$ or that β has no conjugates of the form $\omega\beta^{-1}$ with ω a root of unity. Our aim is to show that under either of these assumptions we can find $(n_i)_{i=0}^m \in \mathcal{N}$ and $\emptyset \neq I \subseteq \{0, 1, \dots, m\}$ such that (17) holds.

Let Σ be the set of all embeddings of K into $\mathbb{C}$. We may rewrite (16) in the form

$$\sum_{(i,\tau) \in \{0,\dots,m\} \times \Sigma} \tau(a_i)\tau(\beta)^{n_i} = 0. \tag{18}$$

For each $(n_i)_{i=0}^m \in \mathcal{N}$, we partition $\{0, \dots, m\} \times \Sigma$ into pairwise disjoint nonempty sets J that are minimal with respect to the property that

$$\sum_{(i,\tau) \in J} \tau(a_i)\tau(\beta)^{n_i} = 0. \tag{19}$$

Applying the pigeon-hole principle and replacing $\mathcal{N}$ with an infinite subset, we may assume that this partition is the same for all $(n_i)_{i=0}^m \in \mathcal{N}$. Let J be a cell in this partition and let I be the set of all $i \in \{0, \dots, m\}$ such that $(i, \tau) \in J$ for at least one $\tau \in \Sigma$. Note that (19) only depends on n_i with $i \in I$. Choosing J in a judicious manner, we can also ensure that the set $\mathcal{N}' = \{(n_i)_{i \in I} \mid (n_i)_{i=0}^m \in \mathcal{N}\}$ is infinite. It follows from the definition of J that all proper sub-sums $\sum_{(i,\tau) \in J'} \tau(a_i)\tau(\beta)^{n_i}$, $\emptyset \neq J' \subsetneq J$, are nonzero for all $(n_i)_{i \in I} \in \mathcal{N}'$.

From the finiteness of the number of solutions of the S-unit equation [vdPS91, Thm. 2], we deduce that the solutions $(n_i)_{i \in I}$ of (19) produce up to scaling only a finite number of values of $(\tau(\beta)^{n_i})_{(i,\tau) \in J}$. Thus, applying

the pigeon-hole principle and replacing $\mathcal{N}'$ with an infinite subset, we may assume that $(\tau(\beta)^{n_i})_{(i,\tau)\in J}$ takes the same value, up to scaling, for all $(n_i)_{i\in I} \in \mathcal{N}'$. It follows that for each $(n_i)_{i\in I}, (n'_i)_{i\in I} \in \mathcal{N}'$ and for each $(i,\tau),(j,\sigma) \in J$ we have $\tau(\beta)^{n'_i-n_i} = \sigma(\beta)^{n'_j-n_j}$. From Lemma 6.2 it follows that

$$n'_i - n_i = \pm\left(n'_j - n_j\right) \qquad \text{and} \qquad \tau(\beta) = \omega\sigma(\beta)^{\pm 1}, \tag{20}$$

where ω is a root of unity that depends on τ and σ.

Identifying K with a subfield of $\mathbb{C}$, we may assume that Σ contains the inclusion map id and that $(i_0, \mathrm{id}) \in J$ for some i_0. In particular, taking $(j,\sigma) = (i_0, \mathrm{id})$ we see that $\tau(\beta) = \omega\beta^{\pm 1}$. Partition J as $J_+ \cup J_-$, where $J_\pm$ is the set of those $(i,\tau) \in J$ for which $\tau(\beta) = \omega\beta^{\pm 1}$.

We claim that our assumptions guarantee that the set J_- is empty. This is immediate if β has no conjugates of the form $\omega\beta^{-1}$ with ω a root of unity. In the second case where $\mathcal{N}'$ is a subset of $\mathbb{N}_0^{m+1}$, we deduce from equation (20) that for all $(n_i)_{i\in I}, (n'_i)_{i\in I} \in \mathcal{N}'$ and all $(i,\tau) \in J$ we have

$$n'_i = \begin{cases} n_i + (n'_{i_0} - n_{i_0}) & \text{if } (i,\tau) \in J_+, \\ n_i - (n'_{i_0} - n_{i_0}) & \text{if } (i,\tau) \in J_-. \end{cases} \tag{21}$$

If J_- were nonempty, this would show that for a given $(n_i)_{i\in I}$ there are only finitely many possibilities for $(n'_i)_{i\in J}$ since $n_i \geqslant n'_{i_0} - n_{i_0} \geqslant -n_{i_0}$ for any i such that $(i,\tau) \in J_-$ for some $\tau \in \Sigma$. This would contradict the fact that $\mathcal{N}'$ is infinite. Thus J_- is empty.

Since β satisfies (†) and since an embedding of K into $\mathbb{C}$ is uniquely determined by its value on β, the set $J = J_+$ takes the form $J = I \times \{\mathrm{id}\}$. Equation (19) now takes the form

$$\sum_{i\in I} a_i \beta^{n_i} = 0,$$

which gives the claim. □

Proposition 6.6. *Let β be an algebraic number satisfying (†), let $K = \mathbb{Q}(\beta)$, and let $Y \subseteq K$ be a finite set. Then there exists an integer N such that for each nonzero $x \in K$, if for each integer k with $0 \leqslant k < N$ there exists $j(k) \in \mathbb{N}_0$ and $y(k) \in Y$ such that*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\beta^k x) = \mathrm{Tr}_{K/\mathbb{Q}}(\beta^{j(k)} y(k)), \tag{22}$$

then there exists an integer $l \in \mathbb{Z}$, $z \in Y$, and an automorphism σ of K and a root of unity ω such that $\sigma(\beta) = \omega\beta^{\pm 1}$ and $x = \beta^l \sigma(z)$.

Proof. Removing if necessary redundant elements of Y, we may assume without loss of generality that the ratio y/y' is not a power of β for any $y, y' \in Y$.

Let N be a large integer, to be determined in the course of the proof. Let $X^m + a_{m-1}X^{m-1} + \cdots + a_0$ be the minimal polynomial of β over $\mathbb{Q}$, and put $a_m = 1$. Note that for any $k \geqslant 0$ we have

$$\sum_{i=0}^{m} a_i \,\mathrm{Tr}_{K/\mathbb{Q}}(\beta^{k+i} x) = 0. \tag{23}$$

For any nonempty proper subset I of $\{0,\ldots,m\}$, the sequence $(f_k^{(I)})_{k=0}^{\infty}$ given by

$$f_k^{(I)} = \sum_{i\in I} a_i \,\mathrm{Tr}_{K/\mathbb{Q}}(\beta^{k+i} x)$$

is a nondegenerate linear recurrence sequence (and is not identically zero by the nondegeneracy of $\mathrm{Tr}_{K/\mathbb{Q}}$), and so by the Skolem–Mahler–Lech Theorem it has only finitely many zeros. By the results of Schlickewei [Sch96, Thm. 1.1], the number of these zeros is bounded by a constant C that depends only on K. Thus, replacing N with $\lfloor (N-C)/(C+1) \rfloor$ and x with $x' = \beta^{k_0} x$ for suitably chosen k_0, we may assume that $f_k^{(I)} \neq 0$ for $0 \leqslant k < N$. Repeating this procedure for all I, we may assume that the sum $\sum_{i\in I} a_i \,\mathrm{Tr}_{K/\mathbb{Q}}(\beta^{k+i} x)$ is nonzero for each $0 \leqslant k < N$ and each nonempty proper subset I of $\{0,\ldots,m\}$.

Combining (22), (23) and the reduction above, for $0 \leqslant k < N - m$ we have

$$\sum_{i=0}^{m} a_i \,\mathrm{Tr}_{K/\mathbb{Q}}(\beta^{j(k+i)} y(k+i)) = 0, \tag{24}$$

and no proper nonempty sub-sum of (24) vanishes. Applying Proposition 6.4 with $a_i' = a_i y_i$ for all possible choices of $(y_i)_{i=0}^m \in Y^{m+1}$, we conclude that there exists a finite set $\mathcal{J} \subseteq \mathbb{N}_0^{m+1}$ such that for each $0 \leqslant k < N - m$ we have

$$\sum_{i=0}^{m} a_i \beta^{j(k+i)} y(k+i) = 0 \tag{25}$$

unless $(j(k+i))_{i=0}^m \in \mathcal{J}$. Furthermore, no proper nonempty sub-sum of (25) vanishes.

As a consequence of Lemma 6.3(i), for each $(j_i)_{i=0}^m \in \mathbb{N}_0^{m+1}$ and $(y_i)_{i=0}^m \in Y^{m+1}$, there exists at most one value of k with $0 \leqslant k < N - m$ such that $(j(k+i))_{i=0}^m = (j_i)_{i=0}^m$ and $(y(k+i))_{i=0}^m = (y_i)_{i=0}^m$. Replacing once more N with $\left\lfloor (N - |\mathcal{J}| \cdot |Y|^{m+1})/(|\mathcal{J}| \cdot |Y|^{m+1} + 1) \right\rfloor$, we may assume that (25) holds for all $0 \leqslant k < N - m$.

It follows from the finiteness of the number of solutions of S-unit equations that the number of $(m+1)$-tuples $(\beta^{j(k+i)} y(k+i))_{i=0}^m$ that satisfy (25), regarded up to scaling, is bounded by a constant C' that depends only on β and Y. Of course, the number of $(m+1)$-tuples $(y(k+i))_{i=0}^m$ is bounded by $|Y|^{m+1}$. Letting $C'' = C' |Y|^{m+1}$ and assuming, as we may, that $N > C'' + m$, we can find k_1, k_2 with $0 \leqslant k_1 < k_2 \leqslant C''$ such that

$$j(k_1+i) - j(k_1) = j(k_2+i) - j(k_2) \qquad \text{and} \qquad y(k_1+i) = y(k_2+i) \tag{26}$$

for all i with $0 \leqslant i \leqslant m$. It follows from (25) that, if for some k we are given $j(k+1) - j(k), \ldots, j(k+m-1) - j(k)$ and $y(k), y(k+1), \ldots, y(k+m-1)$, then we can uniquely determine the value of $\beta^{j(k+m)-j(k)} y(k+m)$, and hence also the values of $j(k+m) - j(k)$ and $y(k+m)$. As a consequence, (26) holds, more generally, for all i with $0 \leqslant i < N - k_2$. Setting $d := k_2 - k_1$ and $e := j(k_2) - j(k_1)$, for all k with $k_1 \leqslant k < N - d$ we have

$$j(k+d) = j(k) + e \qquad \text{and} \qquad y(k+d) = y(k). \tag{27}$$

Iterating (27), we conclude that for any k and $l \geqslant 0$ we have

$$j(k+ld) = j(k) + le, \tag{28}$$

provided that $k_1 \leqslant k < N - ld$. Recalling how $j(k)$ was defined, we conclude from (28) that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\beta^{k+ld} x) = \mathrm{Tr}_{K/\mathbb{Q}}(\beta^{j(k)+le} y(k)). \tag{29}$$

Let μ be the order of the (cyclic) group of roots of unity contained in K. Choose k to be an integer such that $k \geqslant k_1$ and k is divisible by μ. Assume moreover, as we may, that N is sufficiently large so that $k + (2m-1)d < N$. We conclude from (29) and Lemma 6.3(ii) that there exists an automorphism σ of K with $\sigma(\beta^d) = \beta^e$ and $\sigma(\beta^k x) = \beta^{j(k)} y(k)$. By Lemma 6.2 we have $e = \pm d$ and $\sigma(\beta) = \omega \beta^{\pm 1}$ for some root of unity ω. Since k is divisible by μ, we have $\sigma(\beta^k) = \beta^{\pm k}$, and so $\sigma(x) = \beta^{j(k) \mp k} y(k)$. This concludes the proof. □

We have now all the technical tools necessary for the proof of Theorem 6.1.

Proof of Theorem 6.1. We may assume that $\beta \neq 0$. Put $K = \mathbb{Q}(\beta)$ and let X denote the set of values of the sequence $(n_i)_{i=0}^\infty$. If it were the case that $|\tau(\beta)| \leqslant 1$ for all embeddings τ of K into $\mathbb{C}$, then X would be a bounded subset of $\mathbb{Q}$. Since a generalised polynomial map on a bounded real interval has only a finite number of discontinuities, X would then be finite, and β would be a root of unity, in which case the claim would be clear. Thus, we may assume that there exists an embedding τ_0 of K into $\mathbb{C}$ such that $|\tau_0(\beta)| > 1$.

Let $d \in \mathbb{N}$ be the lowest common multiple of the orders of all roots of unity that may occur as quotients or products of two conjugates of β. Then, $\gamma = \beta^d$ satisfies (†) and has no conjugates of the form $\omega \gamma^{-1}$ with ω a root of unity except possibly for $\omega = 1$. Put $M = \mathbb{Q}(\gamma)$

Using Lemma 4.1(i), we choose $z \in K$ so that

$$n_i = \mathrm{Tr}_{K/\mathbb{Q}}(\beta^i z) \quad \text{for all } i \in \mathbb{N}_0.$$

Let $S = \left\{ \mathrm{Tr}_{K/M}(\beta^r z) \;\middle|\; 0 \leqslant r < d \right\}$. Using the transitivity of the trace, we may write each $\mathrm{Tr}_{K/\mathbb{Q}}(\beta^i z)$ in the form

$$\mathrm{Tr}_{K/\mathbb{Q}}(\beta^i z) = \mathrm{Tr}_{M/\mathbb{Q}}(\gamma^j s) \quad \text{for } j = \lfloor i/d \rfloor,\ s = \mathrm{Tr}_{K/M}(\beta^{i-dj} z).$$

Thus, the set X takes the form

$$X = \left\{ \mathrm{Tr}_{M/\mathbb{Q}}(\gamma^i s) \;\middle|\; i \in \mathbb{N}_0,\ s \in S \right\}.$$

Observe that S contains some nonzero element, since otherwise $(n_i)_{i=0}^{\infty}$ would be identically zero.

Claim: The set

$$\{\gamma^l s \mid l \in \mathbb{N}_0,\ s \in S\}$$

is a generalised polynomial subset of M.

Proof: Let N be a large integer, to be determined shortly, and consider the set

$$A = \{x \in M \mid \mathrm{Tr}_{M/\mathbb{Q}}(\gamma^k x) \in X \text{ for all } 0 \leqslant k < N\}.$$

Since X is a generalised polynomial subset of $\mathbb{Q}$, and since the family of generalised polynomial subsets of M is closed under finite intersections and taking preimage by a generalised polynomial map, we see that A is a generalised polynomial subset of M.

It is clear that

$$\left\{\gamma^l s \;\middle|\; l \in \mathbb{N}_0,\ s \in S\right\} \subseteq A.$$

In the opposite direction, observe that if x belongs to A, then for every $0 \leqslant k < N$ there exists some $j(k) \in \mathbb{N}_0$ and $s(k) \in S$ such that

$$\mathrm{Tr}_{M/\mathbb{Q}}(\gamma^k x) = \mathrm{Tr}_{M/\mathbb{Q}}(\gamma^{j(k)} s(k)).$$

Choosing N to be sufficiently large for the claim of Proposition 6.6 to hold, we infer that $x = \gamma^l \sigma(s)$ for some $s \in S$, $l \in \mathbb{Z}$, and automorphism σ of K with $\sigma(\gamma) = \gamma^{\pm 1}$. We will consider two cases depending whether or not γ and γ^{-1} are conjugate.

Case I: (Suppose that γ is not conjugate to γ^{-1}). The above reasoning shows that

$$\left\{\gamma^l s \;\middle|\; l \in \mathbb{N}_0,\ s \in S\right\} \subseteq A \subseteq \left\{\gamma^l s \;\middle|\; l \in \mathbb{Z},\ s \in S\right\}.$$

Suppose that $x = \gamma^l s$ belongs to A for some $l \in \mathbb{Z}$, $l < 0$, $s \in S$. Then in particular

$$\mathrm{Tr}_{M/\mathbb{Q}}(\gamma^l s) = \mathrm{Tr}_{M/\mathbb{Q}}(\gamma^j s') \quad \text{for some } j \in \mathbb{N}_0,\ s' \in S.$$

From the second part of Proposition 6.4 we deduce that there are only finitely many possibilities for x. Indeed, except for finitely many possible values of l, we have one of three possibilities: $\gamma^l s = 0$, in which case $x = 0$; $\gamma^l s = \gamma^j s' \neq 0$, in which case $\gamma^{|l|} \leqslant s/s'$ and hence there are only finitely many possibilities for x; or $\gamma^j s' = 0$, in which case $\mathrm{Tr}_{M/\mathbb{Q}}(\gamma^l s) = 0$, and another application of Proposition 6.4 shows that there are only finitely many possibilities for x. Thus the set $\left\{\gamma^l s \;\middle|\; l \in \mathbb{N}_0,\ s \in S\right\}$ is generalised polynomial since it differs from A only on a finite subset.

Case II: (Suppose that γ is conjugate to γ^{-1}). Let σ be the automorphism of M such that $\sigma(\gamma) = \gamma^{-1}$. Since

$$\mathrm{Tr}_{M/\mathbb{Q}}(\gamma^l s) = \mathrm{Tr}_{M/\mathbb{Q}}(\sigma(\gamma^l s)) = \mathrm{Tr}_{M/\mathbb{Q}}(\gamma^{-l}\sigma(s)),$$

we deduce that

$$\left\{\gamma^l s \;\middle|\; l \in \mathbb{N}_0,\ s \in S\right\} \cup \left\{\gamma^{-N+1-l}\sigma(s) \;\middle|\; l \in \mathbb{N}_0,\ s \in S\right\} \subseteq A \subseteq \left\{\gamma^l s \;\middle|\; l \in \mathbb{Z},\ s \in S \cup \sigma(S)\right\}.$$

Suppose that $x = \gamma^l s$ belongs to A for some $l \in \mathbb{Z}$, $l < 0$, $s \in S$. Then in particular

$$\mathrm{Tr}_{M/\mathbb{Q}}(\gamma^l s) = \mathrm{Tr}_{M/\mathbb{Q}}(\gamma^j s') \quad \text{for some } j \in \mathbb{N}_0,\ s' \in S.$$

On the other hand, we have

$$\mathrm{Tr}_{M/\mathbb{Q}}(\gamma^l s) = \mathrm{Tr}_{M/\mathbb{Q}}(\sigma(\gamma^l s)) = \mathrm{Tr}_{M/\mathbb{Q}}(\gamma^{-l}\sigma(s)).$$

Applying the first part of Proposition 6.4 to the equality

$$\mathrm{Tr}_{M/\mathbb{Q}}(\gamma^{-l}\sigma(s)) = \mathrm{Tr}_{M/\mathbb{Q}}(\gamma^j s'),$$

we deduce as before that except for finitely many possible values of x we have $\sigma(x) = \gamma^{-l}\sigma(s) = \gamma^j s'$, so $x = \gamma^{-j}\sigma(s')$. A similar (simpler) reasoning shows that if $x = \gamma^l \sigma(s)$ belongs to A for some $l \in \mathbb{N}_0$, $s \in S$, then except for finitely many possible values of x we have $x = \gamma^j s'$ for some $j \in \mathbb{N}_0$, $s' \in S$. We conclude that the set

$$A' = \left\{\gamma^l s \;\middle|\; l \in \mathbb{N}_0,\ s \in S\right\} \cup \left\{\gamma^{-l}\sigma(s) \;\middle|\; l \in \mathbb{N}_0, s \in S\right\}$$

is generalised polynomial since it differs from A only on a finite subset. Let C be the generalised polynomial subset of M consisting of the elements $x \in M$ such that $|\tau_0(x)| < 1$. Removing C from A' retains all the elements $x = \gamma^l s$ with $s \in S$, $s \neq 0$, and $l \in \mathbb{N}_0$ sufficiently large, and eliminates $x = 0$ and all the elements

$x = \gamma^{-l}\sigma(s)$ with $s \in S$, and l sufficiently large. Thus, the set $\{\gamma^l s \mid l \in \mathbb{N}_0,\ s \in S\}$ is generalised polynomial since it differs from $A' \setminus C$ only on a finite subset. $\triangle$

Let S_0 be the set obtained from S by performing the following operations: if $0 \in S$, replace S by $S \setminus \{0\}$; replace S by $s^{-1}S$ for some $s \in S$; remove any $s \in S$ such that $s = \gamma^j s'$ for some $j \in \mathbb{N}$, $s' \in S$. We obtain in this manner a finite set S_0 with $0 \notin S_0$, $1 \in S_0$, and such that $D_0 = \{\gamma^l s \mid l \in \mathbb{N}_0,\ s \in S_0\}$ is a generalised polynomial subset of M. Consider the set

$$D_1 = \{x \in M \mid sx \in D_0 \text{ for all } s \in S_0\}.$$

By construction, D_1 is a generalised polynomial subset of M and can be written in the form

$$D_1 = \{\gamma^l s \mid l \in \mathbb{N}_0,\ s \in S_1\}$$

for some finite set S_1 such that $0 \notin S_1$, $1 \in S_1$, and the quotient of two different elements of S_1 is not an integral power of γ. Moreover, we have $|S_1| \leqslant |S_0|$, with equality occuring only if for any $s, s' \in S_0$, the product ss' is equal to $\gamma^t s''$ for some $t \in \mathbb{Z}$ and $s'' \in S_0$. This latter condition is equivalent to the condition that the image of S_0 in the quotient group $M^*/\langle\gamma\rangle$ is closed under multiplication, and hence is a finite group.

Continuing this procedure, we obtain a sequence of finite sets $(S_n)_{n=0}^{\infty}$ with $|S_0| \geqslant |S_1| \geqslant \cdots$ and corresponding generalised polynomial sets $D_0 \supset D_1 \supset \cdots$. Let m be such that $|S_m| = |S_{m+1}|$. This means that S_m is such that $0 \notin S_m$, $1 \in S_m$, the quotient of two different elements of S_m is not an integral power of γ, and the image of S_m in $M^*/\langle\gamma\rangle$ is a finite group. It follows that any $s \in S_m$ is a rational power of γ. Let G be the subgroup of M^* generated by S_m and γ. Then G is finitely generated and $\langle\gamma\rangle$ is its subgroup of finite index. Hence, by Chevalley's theorem [Che51, Thm. 1], $\langle\gamma\rangle$ is a congruence subgroup of G, meaning that $\langle\gamma\rangle = G \cap \Lambda$ for some $\Lambda \subseteq M$ that is a union of finitely many cosets of a lattice. Thus, the set

$$D_m \cap \Lambda = \{\gamma^l s \mid l \in \mathbb{N}_0, s \in S_m\} \cap \Lambda = \{\gamma^l \mid l \in \mathbb{N}_0\}$$

is a generalised polynomial subset of M. Since generalised polynomial sets are closed under dilations and finite unions, this also implies that $\{\beta^l \mid l \in \mathbb{N}_0\}$ is a generalised polynomial subset of M, and hence by Proposition 2.2(ii) also of K. $\square$

7. Non-hereditary generalised polynomial setshere

In light of Theorem C, it is natural to ask which generalised polynomial sets of integers are hereditary. It is not hard to see that each set $E \subseteq \mathbb{Z}$ with positive density

$$d(E) := \lim_{N\to\infty} \frac{|E \cap [-N, N]|}{2N+1} > 0 \tag{30}$$

has a subset E' that does not have density, meaning that

$$\liminf_{N\to\infty} \frac{|E \cap [-N, N]|}{2N+1} =: \underline{d}(E) < \overline{d}(E) := \limsup_{N\to\infty} \frac{|E \cap [-N, N]|}{2N+1}.$$

Since the density exists for each generalised polynomial set, no generalised polynomial set with positive density is hereditary. When it comes to sets with zero density, it remains the case that we expect most of them to not be hereditary, but proving this becomes more difficult. However, we can at least show that not all of them are hereditary.

Theorem 7.1. *There exists a generalised polynomial set $E \subseteq \mathbb{Z}$ with $d(E) = 0$ as well as a subset $E' \subseteq E$ that is not a generalised polynomial set.*

Our proof of Theorem E relies on two components from [AK22]. The first ingredient is a polynomial bound on subword complexity of finitely-valued generalised polynomials. Recall that the *subword complexity* p_a of a sequence $a\colon \mathbb{Z} \to \Sigma$ taking values in a finite alphabet Σ is the map that assigns to a positive integer N the number of distinct length-N subsequences of a:

$$p_a(N) := \left|\left\{(a(m+n))_{n=0}^{N-1} \;\middle|\; m \in \mathbb{Z}\right\}\right|. \tag{31}$$

The subword complexity of a sequence $\mathbb{N} \to \Sigma$ is defined analogously. If $|\Sigma| = k$, we have the trivial upper bound $p_a(N) \leqslant k^N$.

Theorem 7.2 ([AK22, Thm. A])**.** *Let $g\colon \mathbb{Z} \to \Sigma$ be a generalised polynomial taking values in a finite set $\Sigma \subseteq \mathbb{R}$. Then there exists a constant $C = C(g) > 0$ such that $p_g(N) = O(N^C)$ as $N \to \infty$.*

The second ingredient is the existence of generalised polynomial sets E with zero density, but with the expression in (30) converging to 0 arbitrarily slowly. The following result was originally stated for subsets of $\mathbb{N}$, but the adaptation to $\mathbb{Z}$ is immediate.

Theorem 7.3 ([AK22, Prop. 8.12])**.** *Let $f\colon \mathbb{N} \to [0,1]$ be a sequence with $f(N) \to 0$ as $N \to \infty$. Then there exists a generalised polynomial set $E \subseteq \mathbb{Z}$ such that $d(E) = 0$ and $|E \cap [0,N)| \geqslant f(N)N$.*

The following consequence of Theorem 7.3, juxtaposed with Theorem 7.2, will almost immediately yield a proof of Theorem E.

Proposition 7.4. *Let $h\colon \mathbb{N} \to [0,1]$ be a sequence with $h(L) \to 0$ as $L \to \infty$. There exists a generalised polynomial set $E \subseteq \mathbb{Z}$ with $d(E) = 0$ and a subset $F \subseteq E$ such that $p_{1_F}(L) \geqslant 2^{h(L)L}$ for all $L \in \mathbb{N}$.*

Proof. Replacing $h(L)$ with $\lceil h(L)L \rceil / L$, we may freely assume that $h(L)L$ is an integer for all $L \in \mathbb{N}$. Let M_L, N_L be sequences of integers satisfying $N_0 = M_0 = 0$ and, for $L \geqslant 1$,

$$N_L := N_{L-1} + L \cdot M_L, \qquad M_L \geqslant \frac{N_{L-1} + 2^{(1+h(L))L} L}{(h(L) - h(L)^2)L}. \tag{32}$$

Let $f\colon \mathbb{N} \to [0,1]$ be a sequence satisfying

$$f(N_L) \geqslant 2h(L) - h(L)^2 \qquad \text{and} \qquad f(N) \to 0 \text{ as } N \to \infty. \tag{33}$$

Let E be a set whose existence is asserted in Theorem 7.3. We will construct F as the intersection of a descending sequence of sets E_L, where $E_0 := E$. Pick a positive integer L. We can decompose the interval $[0, N_L)$ as

$$[0, N_L) = [0, N_{L-1}) \cup \bigcup_{m=0}^{M_L - 1} [N_{L-1} + mL, N_{L-1} + (m+1)L).$$

Let M_L^+ denote the number of integers $m \in [0, M_L)$ such that

$$|E \cap [N_{L-1} + mL, N_{L-1} + (m+1)L)| \geqslant h(L)L,$$

Then

$$f(N_L)N_L \leqslant |E \cap [0, N_L)| \leqslant N_{L-1} + M_L^+ L + M_L h(L) L.$$

Combined with (32) and (33), this implies that

$$M_L^+ \geqslant 2^{(1+h(L))L}.$$

Put $H := 2^{h(L)L}$. Applying the pigeonhole principle, we conclude that there exists a set $A \subseteq [0, L)$ with $|A| \geqslant h(L)L$ and positions $0 \leqslant m_0 < m_1 < \cdots < m_{H-1} < M_L$ such that

$$E \cap [N_{L-1} + m_j L, N_{L-1} + (m_j + 1)L) = N_{L-1} + m_j L + A \quad \text{for all } 0 \leqslant j < H.$$

Let $A_0, A_1, \ldots, A_{H-1}$ be H different subsets of A. Put $B_j := A \setminus A_j$ and

$$E_L := E_{L-1} \setminus \bigcup_{j=0}^{H-1} (N_{L-1} + m_j L + A_j).$$

In particular, for each $0 \leqslant j < H$ we have

$$(E_L - (N_{L-1} + m_j L)) \cap [0, L) = B_j.$$

In particular, 1_{B_j} is a subsequence of 1_{E_L}, and thus the indicator function of E_L has at least $2^{h(L)L}$ length-L subsequences, all of which appear at positions between N_{L-1} and N_L. We put $F := \bigcap_{L=0}^{\infty} E_L$. It follows from the construction above that the subword complexity of F satisfies $p_{1_F}(L) \geqslant 2^{h(L)L}$ for all $L \in \mathbb{N}$. □

Proof of Theorem E. Let $h(L) := 1/\sqrt{L}$, and let E, F be some sets satisfying the claim of Proposition 7.4. Then F is not a generalised polynomial set by Theorem 7.2. □

References

[AK22] B. Adamczewski and J. Konieczny. Bracket words: a generalisation of Sturmian words arising from generalised polynomials, 2022.

[BDGGH+92] M.-J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse, and J.-P. Schreiber. *Pisot and Salem numbers*. Birkhäuser Verlag, Basel, 1992. With a preface by David W. Boyd.

[BK18] J. Byszewski and J. Konieczny. Sparse generalised polynomials. *Trans. Amer. Math. Soc.*, 370(11):8081–8109, 2018.

[Che51] C. Chevalley. Deux théorèmes d'arithmétique. *J. Math. Soc. Japan*, 3:36–44, 1951.

[Eve84] J.-H. Evertse. On sums of S-units and linear recurrences. *Compositio Math.*, 53(2):225–244, 1984.

[Kon21] J. Konieczny. Generalised polynomials and integer powers. *Journal of the London Mathematical Society*, 2021.

[Lan02] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Lec53] C. Lech. A note on recurring series. *Ark. Mat.*, 2:417–421, 1953.

[Mah56] K. Mahler. On the Taylor coefficients of rational functions. *Proc. Cambridge Philos. Soc.*, 52:39–48, 1956.

[Sal45] R. Salem. Power series with integral coefficients. *Duke Math. J.*, 12:153–172, 1945.

[Sch96] H. P. Schlickewei. Multiplicities of recurrence sequences. *Acta Math.*, 176(2):171–243, 1996.

[Sko34] T. Skolem. Ein Verfahren zur Behandlung gewisser exponentialer und Diophantischer Gleichungen. *C.R. VIII Congr. Math., Stockholm (1934)*, pages 163—168, 1934.

[Smy15] C. Smyth. Seventy years of Salem numbers. *Bull. Lond. Math. Soc.*, 47(3):379–395, 2015.

[vdPS91] A. J. van der Poorten and H. P. Schlickewei. Additive relations in fields. *J. Austral. Math. Soc. Ser. A*, 51(1):154–170, 1991.

(J. Byszewski) Faculty of Mathematics and Computer Science, Jagiellonian University, Łojasiewicza 6, 30-348 Kraków, Poland

Email address: jakub.byszewski@uj.edu.pl

(J. Konieczny) Université Claude Bernard Lyon 1, CNRS UMR 5208, Institut Camille Jordan, F-69622 Villeurbanne Cedex, France

Email address: jakub.konieczny@gmail.com