



Algebraic numbers, hyperbolicity, and density modulo one

A. Gorodnik*, S. Kadyrov

School of Mathematics, University of Bristol, Bristol BS8 1TW, UK

ARTICLE INFO

Article history:

Received 1 September 2011

Revised 2 May 2012

Accepted 2 May 2012

Available online 15 July 2012

Communicated by David Goss

Keywords:

Density modulo one

Multiplicatively independent numbers

Compact abelian group

Higher-rank abelian action

ABSTRACT

We prove the density of the sets of the form

$$\{\lambda_1^m \mu_1^n \xi_1 + \cdots + \lambda_k^m \mu_k^n \xi_k: m, n \in \mathbb{N}\}$$

modulo one, where λ_i and μ_i are multiplicatively independent algebraic numbers satisfying some additional assumptions. The proof is based on analysing dynamics of higher-rank actions on compact abelian groups.

© 2012 Elsevier Inc. All rights reserved.

1. Introduction

The aim of this paper is to generalise the following theorem of B. Kra [4]:

Theorem 1.1. *Let $p_i, q_i \geq 2, i = 1, \dots, k$, be integers such that*

- (a) *each pair (p_i, q_i) is multiplicatively independent,¹*
- (b) *for all $i \neq j$, $(p_i, q_i) \neq (p_j, q_j)$.*

Then for all real numbers $\xi_i, i = 1, \dots, k$, with at least one of ξ_i 's irrational, the set

$$\left\{ \sum_{i=1}^k p_i^n q_i^m \xi_i: m, n \in \mathbb{N} \right\}$$

is dense modulo one.

* Corresponding author.

E-mail addresses: a.gorodnik@bristol.ac.uk (A. Gorodnik), shirali.kadyrov@bristol.ac.uk (S. Kadyrov).

¹ A pair (λ, μ) is called *multiplicatively independent* if $\lambda^m \neq \mu^n$ for all $(m, n) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.

We prove an analogous results with p_i and q_i being algebraic numbers. For this we need to introduce the notion of hyperbolicity. For any prime p (including $p = \infty$), let $\overline{\mathbb{Q}}_p$ denote the algebraic closure of $\mathbb{Q}_p$. In particular, $\overline{\mathbb{Q}}_\infty = \mathbb{C}$. A semigroup Σ consisting of algebraic numbers will be called *hyperbolic* provided that for every prime p (including $p = \infty$), if there is a field embedding $\theta : \mathbb{Q}(\Sigma) \rightarrow \overline{\mathbb{Q}}_p$ such that

$$\theta(\Sigma) \not\subseteq \{|z|_p \leq 1\},$$

then for all field embeddings $\theta : \mathbb{Q}(\Sigma) \rightarrow \overline{\mathbb{Q}}_p$, we have

$$\theta(\Sigma) \not\subseteq \{|z|_p = 1\}.$$

For example, if $\alpha > 1$ is a real algebraic integer, then the semigroup $\langle \alpha \rangle$ is hyperbolic provided that none of the Galois conjugates of α have absolute value one.

The algebraic closure of the field of rational numbers $\mathbb{Q}$ will be denoted by $\overline{\mathbb{Q}}$. Our main result is the following:

Theorem 1.2. *Let $\lambda_i, \mu_i, i = 1, \dots, k$, be real algebraic numbers satisfying $|\lambda_i|, |\mu_i| > 1$ such that*

- (a) *each pair (λ_i, μ_i) is multiplicatively independent,*
- (b) *for all $i \neq j$, $\theta \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and $u \in \mathbb{N}$, $(\theta(\lambda_i)^u, \theta(\mu_i)^u) \neq (\lambda_j^u, \mu_j^u)$,*
- (c) *each semigroup $\langle \lambda_i, \mu_i \rangle$ is hyperbolic.*

Then for all real numbers $\xi_i, i = 1, \dots, k$, with at least one of ξ_i satisfying $\xi_i \notin \mathbb{Q}(\lambda_i, \mu_i)$, the set

$$\left\{ \sum_{i=1}^k \lambda_i^n \mu_i^m \xi_i : m, n \in \mathbb{N} \right\}$$

is dense modulo one.

Previously, D. Berend [3] have investigated the case $k = 1$, and R. Urban [5–7] have proved several partial results when $k = 2$.

In the next section, we introduce a compact abelian group Ω equipped with an action of a commutative semigroup Σ and show that the sequence that appears in the main theorem is closely related to a suitably chosen orbit $\Sigma\omega$ in Ω . More precisely, this sequence is obtained by applying a projection map $\Pi : \Omega \rightarrow \mathbb{R}/\mathbb{Z}$. This construction is analogous to the one of Berend in [3], but in the case $k > 1$, we have to deal with a larger space Ω where the structure of orbits of Σ is not well understood, and this requires several additional arguments. The idea of the proof is to show that the closure $\overline{\Sigma\omega}$ has an additional structure. In Section 3 we show that $\overline{\Sigma\omega}$ contains a torsion point. We note that the hyperbolicity assumption (c) is necessary for existence of a torsion point. Then using a limiting argument in a neighbourhood of this torsion point, we demonstrate in Section 4 that $\Sigma\omega$ approximates arbitrary long line segments. Finally, we complete the proof in Section 5 by showing that the projections under Π of such line segments cover $\mathbb{R}/\mathbb{Z}$. This is where the independence assumption (b) is used.

2. Setting

In this section, we construct a compact abelian group Ω and a commutative semigroup Σ of epimorphisms of Ω . We show that there is a natural projection map $\Pi : \Omega \rightarrow \mathbb{R}/\mathbb{Z}$, and for a suitably chosen $\omega \in \Omega$,

$$\Pi(\Sigma\omega) = \left\{ \sum_{i=1}^k \lambda_i^m \mu_i^n \xi_i : m, n \in \mathbb{N} \right\} \pmod{1}. \quad (1)$$

This reduces the proof of the theorem to analysis of orbit structure of Σ in Ω .

Now we explain the details of this construction. Let K be a number field. We fix a basis $\beta_1, \dots, \beta_r$ of the ring of algebraic integers of K . To every element $\alpha \in K$ we associate a matrix $M(\alpha) = (a_{ji}) \in \text{Mat}_r(\mathbb{Q})$ determined by

$$\alpha \cdot \beta_j = \sum_{i=1}^r a_{ji} \beta_i, \quad 1 \leq j \leq r. \quad (2)$$

Suppose that $M(\alpha) \in \text{Mat}_r(\mathbb{Z}[1/a])$ for some $a \in \mathbb{N}$, and a is minimal with this property. We set

$$\begin{aligned} \tilde{\Omega}_a^r &:= \mathbb{R}^r \times \prod_{p|a} \mathbb{Q}_p^r, \\ \Omega_a^r &= \tilde{\Omega}_a^r / \mathbb{Z}[1/a]^r, \end{aligned}$$

where $\mathbb{Z}[1/a]^r$ is embedded in $\tilde{\Omega}_a^r$ by the map $z \mapsto (z, -z, \dots, -z)$. Then Ω_a^r is a compact abelian group. Every matrix $M \in \text{Mat}_r(\mathbb{Z}[1/a])$ naturally acts on $\tilde{\Omega}_a^r$ diagonally and defines a map

$$M : \Omega_a^r \rightarrow \Omega_a^r.$$

The distribution of orbits of such maps will play a crucial role in this paper.

The following lemma will be useful:

Lemma 2.1. *If a prime p divides a , then there is an embedding $\theta : \mathbb{Q}(\alpha) \rightarrow \overline{\mathbb{Q}}_p$ such that $|\theta(\alpha)|_p > 1$.*

Proof. We write $a = p^n b$ with $\gcd(p, b) = 1$ and set $\beta = b\alpha$. It follows from (2) that for every Galois conjugate $\theta(\beta)$, the multiplication by $p^n \theta(\beta)$ preserves the integral module $\mathbb{Z}\theta(\beta_1) + \dots + \mathbb{Z}\theta(\beta_r)$. Therefore, $p^n \theta(\beta)$ is an algebraic integer, and $|\theta(\beta)|_q \leq 1$ for all Galois conjugates of β and all primes $q \neq p$. Suppose that also $|\theta(\beta)|_p \leq 1$ for all Galois conjugates of β . Then β is an algebraic integer and, in particular,

$$\beta \cdot \beta_j \in \mathbb{Z}\beta_1 + \dots + \mathbb{Z}\beta_r$$

for all j . On the other hand, since a is minimal with the property $M(\alpha) \in \text{Mat}_r(\mathbb{Z}[1/a])$, it follows that

$$\beta \cdot \beta_j \notin \mathbb{Z}\beta_1 + \dots + \mathbb{Z}\beta_r$$

for some j . This contradiction shows that $|\theta(\alpha)|_p = |\theta(\beta)|_p > 1$ for some θ , as required. $\square$

Now we adopt this construction to our setting. Let K_i be a number field of degree r_i that contains λ_i and μ_i , and let $A_i = M(\lambda_i)$ and $B_i = M(\mu_i)$ be the matrices in $\text{Mat}_{r_i}(\mathbb{Z}[1/a_i])$ defined as above, where $a_i \in \mathbb{N}$ is minimal with this property. We denote by Σ_i the commutative semigroup generated by A_i and B_i . This semigroup acts on $\tilde{\Omega}_{a_i}^{r_i}$ and $\Omega_{a_i}^{r_i}$. We also consider the semigroup

$$\Sigma := \{(A_1^n B_1^m, \dots, A_k^n B_k^m) : m, n \in \mathbb{N}\}$$

generated by $A := (A_1, \dots, A_k)$ and $B := (B_1, \dots, B_k)$ that naturally acts on

$$\Omega := \prod_{i=1}^k \Omega_{a_i}^{r_i}.$$

We denote by $\pi : \tilde{\Omega} := \prod_{i=1}^k \tilde{\Omega}_{a_i}^{r_i} \rightarrow \Omega$ the corresponding projection map. We write

$$\tilde{\Omega} = \prod_{i=1}^k \prod_{j=1}^{h_i} \mathbb{Q}_{p_{ij}}^{r_i}$$

where $p_{i1} = \infty, \dots, p_{ih_i}$ are the primes dividing a_i (here we write $\mathbb{Q}_\infty = \mathbb{R}$). We denote by $\{e_{ijl}\}$ the standard basis of $\tilde{\Omega}$, and introduce a projection map

$$\Pi : \tilde{\Omega} \rightarrow \mathbb{R}/\mathbb{Z} : \sum_{i,j,l} s_{ijl} e_{ijl} \mapsto \sum_{i,j} \{s_{ij1}\}_{p_{ij}} \pmod{1}, \quad (3)$$

where $\{x\}_\infty$ denotes the usual fractional part, and $\{x\}_p$ denotes the p -adic fractional part. Namely, for $x = \sum_{u=-N}^\infty x_u p^u \in \mathbb{Q}_p$, we set $\{x\}_p = \sum_{u=-N}^{-1} x_u p^u$. It is easy to check Π is continuous, and

$$\Pi \left(\prod_{i=1}^k \mathbb{Z}[1/a_i]^{r_i} \right) = 0 \pmod{1}.$$

Hence, Π also defines a map $\Omega \rightarrow \mathbb{R}/\mathbb{Z}$.

It follows from the definition of $A_i = M(\lambda_i)$ and $B_i = M(\mu_i)$ that they have a joint eigenvector $v_i \in \mathbb{R}^{r_i}$ with eigenvalues λ_i and μ_i respectively. Let us assume for now that the first coordinate of v_i is nonzero. Then we normalise v_i so that this coordinate is one. We set

$$v = \prod_{i=1}^k (\xi_i v_i, 0, \dots, 0) \in \tilde{\Omega} \quad \text{and} \quad \omega = \pi(v) \in \Omega.$$

Then it follows from the definition of Π that (1) holds.

Although this construction may be applied to any choices of the number fields K_i , it is most convenient to choose these fields to be of the smallest size, and we adopt an idea from [1]. For every $i = 1, \dots, k$, we pick $l_i \in \mathbb{N}$ so that $\mathbb{Q}(\lambda_i^{l_i}, \mu_i^{l_i}) = \bigcap_{l=1}^\infty \mathbb{Q}(\lambda_i^l, \mu_i^l)$, and we set $l_0 = \prod_{i=1}^k l_i$. Then $\mathbb{Q}(\lambda_i^{l_0}, \mu_i^{l_0}) = \bigcap_{l=1}^\infty \mathbb{Q}(\lambda_i^l, \mu_i^l)$. We observe that the numbers $\lambda_i^{l_0}$ and $\mu_i^{l_0}$ are satisfying the assumptions Theorem 1.2, and if we prove the claim of the theorem for these numbers, then the theorem would follow for λ_i 's and μ_i 's as well. Hence, from now on we assume that $l_0 = 1$ and take $K_i = \mathbb{Q}(\lambda_i, \mu_i)$.

The main advantage of this construction is the following lemma:

Lemma 2.2. *There exists $C_i \in \Sigma_i$ such that the characteristic polynomial of C_i^u is irreducible over $\mathbb{Q}$ for every $u \in \mathbb{N}$.*

Proof. This follows from [1, Lemma 4.2]. Indeed, since $\mathbb{Q}(\lambda_i, \mu_i) = \bigcap_{l=1}^{\infty} \mathbb{Q}(\lambda_i^l, \mu_i^l)$, by this lemma there exists σ_i in the semigroup generated by λ_i and μ_i such that $\mathbb{Q}(\sigma_i^n) = \mathbb{Q}(\lambda_i, \mu_i)$ for all $n \in \mathbb{N}$. Since the matrix $C_i^n = M(\sigma_i^n) \in \text{Mat}_{r_i}(\mathbb{Z}[1/a_i])$ has an eigenvalue σ_i^n of degree r_i over $\mathbb{Q}$, the claim follows. $\square$

We denote by v_{il} , $1 \leq l \leq r_i$, the eigenvectors of the matrix C_i . Since all the eigenvalues of C_i are distinct, it follows that v_{il} 's are also eigenvectors of the whole semigroup Σ_i . For $D \in \Sigma_i$, we denote by $\lambda_{il}(D)$ the corresponding eigenvalue. In particular, we set $\lambda_{il} = \lambda_{il}(A_i)$ and $\mu_{il} = \lambda_{il}(B_i)$. We choose the indices, so that $\lambda_{i1} = \lambda_i$ and $\mu_{i1} = \mu_i$. Since the characteristic polynomial of C_i is irreducible, all the eigenvectors of v_{il} , $1 \leq l \leq r_i$, are conjugate under the Galois action, and it follows that their coordinates with respect to the standard basis are nonzero.

It follows from Lemma 2.2 that $\lambda_{il_1}(C_i)^u \neq \lambda_{il_2}(C_i)^u$ for all $l_1 \neq l_2$ and $u \in \mathbb{N}$. Hence, in particular,

$$(\lambda_{il_1}^u, \mu_{il_1}^u) \neq (\lambda_{il_2}^u, \mu_{il_2}^u) \quad \text{for all } l_1 \neq l_2 \text{ and } u \in \mathbb{N}. \quad (4)$$

We also introduce an eigenbasis for the space $\tilde{\Omega}$. Let L_{ij} be the splitting field of the matrix C_i over $\mathbb{Q}_{p_{ij}}$. We set

$$V = \prod_{i=1}^r \prod_{j=1}^{h_i} V_{ij} \quad \text{where } V_{ij} = L_{ij}^{r_i}.$$

We denote by v_{ijl} , $l = 1, \dots, r_i$, the basis of the factor V_{ij} consisting of eigenvectors of C_i chosen as above. Then v_{ijl} with $i = 1, \dots, k$, $j = 1, \dots, h_i$, $l = 1, \dots, r_i$ forms a basis of V consisting of eigenvectors of Σ . In these notation,

$$v = \sum_{i=1}^k \xi_i v_{i11} \quad \text{and} \quad \omega = \pi(v).$$

We normalise the eigenvectors v_{ijl} so that their first coordinates with respect the standard bases of $L_{ij}^{r_i}$ are equal to one. Then the projection map Π is given by

$$\Pi \left(\sum_{i,j,l} c_{ijl} v_{ijl} \right) = \sum_{i,j,l} \{c_{ijl}\}_{p_{ij}} \pmod{\mathbb{Z}}. \quad (5)$$

3. Existence of torsion elements

In this section we investigate existence of torsion elements in closed Σ -invariant subsets of Ω and prove

Proposition 3.1. *Every closed Σ -invariant subset of Ω contains a torsion element.*

We start the proof with a lemma that generalises [1, Proposition 4.1], which dealt with toral automorphisms. Given a topological semigroup Σ_0 acting on a topological space Ω_0 , we say that a subset M of Ω_0 is Σ_0 -minimal if it is non-empty, closed, Σ_0 -invariant, and minimal with respect to these properties.

Lemma 3.2. Every Σ_i -minimal subset of $\Omega_{a_i}^{r_i}$ consists of torsion elements.

Proof. We consider the decomposition

$$V_{ij} = V_{ij}^{\leq 1} \oplus V_{ij}^{> 1}$$

where

$$V_{ij}^{\leq 1} := \{v_{ijl} : |\lambda_{il}(D)|_{p_{ij}} \leq 1 \text{ for all } D \in \Sigma_i\},$$

$$V_{ij}^{> 1} := \{v_{ijl} : |\lambda_{il}(D)|_{p_{ij}} > 1 \text{ for some } D \in \Sigma_i\}.$$

In view of Lemma 2.1, the assumption that the semigroup Σ_i is hyperbolic implies that for every i, j, l there exists $D \in \Sigma_i$ such that

$$|\lambda_{il}(D)|_{p_{ij}} \neq 1. \quad (6)$$

Let M be a Σ_i -minimal subset of $\Omega_{a_i}^{r_i}$. Suppose, first, that M is finite. We recall that the action of an element $D \in \Sigma_i$ on $\Omega_{a_i}^{r_i}$ is ergodic provided that it has no roots of unity as eigenvalues. In particular, it follows that $C_i \in \Sigma_i$ is ergodic. Now it follows from [2, Lemma II.15] that M consists of torsion elements.

Suppose that M is infinite. Then $M - M$ contains 0 as an accumulation point. Let $y_n \in \tilde{\Omega}_{a_i}^{r_i}$ be a sequence such that $y_n \rightarrow 0$ and $\pi(y_n) \in M - M$. If

$$y_n \notin V_i^{\leq 1} := \bigoplus_{j=1}^{h_i} V_{ij}^{\leq 1}$$

for infinitely many n , then we may argue exactly as in Case I of [3, p. 252] (with $B = M$). We conclude that $M = \Omega_{a_i}^{r_i}$, which contradicts minimality of M . Hence, it remains to consider the case when every element x in a sufficiently small neighbourhood of 0 in $M - M$ is of the form $\pi(y)$ for some $y \in V_i^{\leq 1}$.

We take an ergodic element $D \in \Sigma_i$ and $M' \subset M$ a D -minimal subset. Then for every $x \in M'$, we have $D^{n_s}(x) \rightarrow x$ along a subsequence n_k . In particular, it follows that for some $n \in \mathbb{N}$,

$$D^n(x) - x = \pi(y) \quad (7)$$

with $y \in V_i^{\leq 1}$. It follows from (6) that there exists an element $E \in \Sigma_i$ such that

$$E^m(y) \rightarrow 0 \quad \text{as } m \rightarrow \infty.$$

Passing to a subsequence, we also obtain

$$E^{m_s}(x) \rightarrow z \in M.$$

Hence, applying E^{m_s} to both sides of (7), we conclude that $D^n(z) = z$, and by [2, Lemma II.15], z is a torsion element. Since M is Σ_i -minimal, it must consist of torsion elements. $\square$

Proof of Proposition 3.1. We denote by $\Omega[\ell]$ the subset of elements whose order divides ℓ . We note that $\Omega[\ell]$ is finite (see [2, Lemma II.13]) and Σ -invariant.

Let M be a Σ -minimal set contained in a given closed Σ -invariant set. We use induction on k . The case when $k = 1$ is handled by Lemma 3.2. In particular, it follows that $p_1(M)$ contains a torsion element of order ℓ_1 , where $p_1 : \Omega \rightarrow \Omega_{a_1}^1$ denotes the projection map. Let

$$N = \left\{ y \in \prod_{i=2}^k \Omega_{a_i}^{r_i} : (x, y) \in M \text{ for some } x \in \Omega_{a_1}^{r_1}[\ell_1] \right\}.$$

Since N is non-empty, invariant, and closed, it follows from the inductive hypothesis that N contains a point y such that $\ell_2 y = 0$ for some $\ell_2 \in \mathbb{N}$. Then M contains (x, y) for some $x \in \Omega_{a_1}^{r_1}[\ell_1]$, and $(x, y) \in \Omega[\ell_1 \ell_2]$. $\square$

From Proposition 3.1, we also deduce

Lemma 3.3. *Let M be a closed Σ -invariant set. Then there exist $s \in \mathbb{N}$ and a torsion point $r \in M$ such that $A^s(r) = B^s(r) = r$.*

Proof. We recall that by [2, Lemma II.13] the set $\Omega[\ell]$, is finite. Since this set is clearly Σ -invariant, it follows from Proposition 3.1 that M contains a finite Σ -invariant set N consisting of torsion elements. We pick N to be a minimal set with these properties. Since $A(N) \subset N$ is also Σ -invariant, we conclude that $A(N) = N$ and similarly $B(N) = N$. Then it follows that $A|_N$ and $B|_N$ are bijections of the finite set N , and there exists $s \in \mathbb{N}$ such that $(A|_N)^s = (B|_N)^s = \text{id}$, which implies the lemma. $\square$

4. Approximation of long line segments

Let $\mathcal{Y}'$ denote the set of accumulation points of $\mathcal{Y} := \pi(\Sigma v) = \Sigma \omega$. The aim of this section is to show that one can approximate projections of arbitrary long line segments by points in $\mathcal{Y}'$. For this we recall that $\mathcal{Y}'$ contains a torsion element r (see Proposition 3.1) and apply the action of Σ to a sequence $(x^{(s)})_{s \geq 1}$ contained in $\mathcal{Y}$ and converging to r . To produce nontrivial limits, one needs additional properties of the sequence $x^{(s)}$ that are provided by the following two lemmas.

Lemma 4.1. *For any point $x \in \mathcal{Y}'$ there exists a sequence $x_s \in \mathcal{Y}$ converging to x such that*

$$x^{(s)} = \pi(y^{(s)}) + x \quad \text{with } y^{(s)} \notin V^{\leq 1}, \quad y^{(s)} \rightarrow 0,$$

where $V^{\leq 1} := \prod_{i=1}^k \prod_{j=1}^{h_i} V_{ij}^{\leq 1}$.

Proof. To prove the lemma we use the assumption that $\xi_i \notin \mathbb{Q}(\lambda_i, \mu_i)$ for some $i = 1, \dots, k$.

Let $(x^{(s)})_{s \geq 1}$ be a sequence of distinct points in $\mathcal{Y} = \pi(\Sigma \omega)$ converging to x . We write

$$x^{(s)} = \pi(y^{(s)}) + x,$$

where $y^{(s)}$ is a sequence of points in $\tilde{\Omega}$ converging to zero. More explicitly,

$$x^{(s)} = \pi(A^{m(s)} B^{n(s)} v) = (x_1^{(s)}, \dots, x_k^{(s)})$$

for $m(s), n(s) \in \mathbb{N}$, where $x_i^{(s)} = \pi_i(A_i^{m(s)} B_i^{n(s)} \xi_i v_{i11}) = \pi_i(\lambda_i^{m(s)} \mu_i^{n(s)} \xi_i v_{i11})$.

Recall that we have assumed that $\xi_i \notin \mathbb{Q}(\lambda_i, \mu_i)$ for some $i = 1, \dots, k$. We claim that for this i the sequence $(x_i^{(s)})_{s \geq 1}$ consists of distinct points. Indeed, suppose that $x_i^{(s_1)} = x_i^{(s_2)}$ for some $s_1 \neq s_2$. Then

$$(\lambda_i^{m(s_1)} \mu_i^{n(s_1)} - \lambda_i^{m(s_2)} \mu_i^{n(s_2)}) \xi_i v_{i11} \in \ker(\pi_i).$$

Since the eigenvector v_{i11} cannot be proportional to a rational vector, we conclude that

$$\lambda_i^{m(s_1)} \mu_i^{n(s_1)} = \lambda_i^{m(s_2)} \mu_i^{n(s_2)},$$

and hence $m(s_1) = m(s_2)$ and $n(s_1) = n(s_2)$ because (λ_i, μ_i) is assumed to be multiplicatively independent. Then $x^{(s_1)} = x^{(s_2)}$, which gives a contradiction.

Now if we suppose that $y^{(s)}$ satisfies $y^{(s)} \in V^{\leq 1}$ for all sufficiently large s , then we can apply the argument of Case II in [3, p. 253] to the sequence $\{x_i^{(s)}\}$. This argument yields that $\xi_i \in \mathbb{Q}(\lambda_i, \mu_i)$, which is a contradiction. Hence, by passing to a subsequence, we can arrange that $y^{(s)} \notin V^{\leq 1}$, as required. $\square$

Given a sequence $(y^{(s)})_{s \geq 1}$ as above, we denote by $\mathcal{I}$ the set of indices (i, j, l) such that $y_{ijl}^{(s)} \neq 0$.

Lemma 4.2. *In Lemma 4.1, we can pick a sequence $(y^{(s)})_{s \geq 1}$ so that for some $D \in \Sigma$,*

- (i) $|\lambda_{il}(D)|_{p_{ij}} > 1$ for all $(i, j, l) \in \mathcal{I}$,
- (ii) $\lambda_{i_1 l_1}(D) \neq \lambda_{i_2 l_2}(D)$ for all $(i_1, j_1, l_1), (i_2, j_2, l_2) \in \mathcal{I}$ with $(i_1, l_1) \neq (i_2, l_2)$.

Proof. The proof relies on the independence property (b) of the main theorem of the pairs (λ_i, μ_i) .

We pick a sequence $(y^{(s)})_{s \geq 1}$ as in Lemma 4.1 with a minimal set of indices $\mathcal{I}$. Then by [2, Lemma II.7], for any $D \in \Sigma$ we have either $|\lambda_{il}(D)|_{p_{ij}} > 1$ for all $(i, j, l) \in \mathcal{I}$ or $|\lambda_{il}(D)|_{p_{ij}} \leq 1$ for all $(i, j, l) \in \mathcal{I}$. Hence, it follows from the hyperbolicity assumption (c) of the main theorem that either A or B satisfies (i). Without loss of generality, we assume that A satisfies (i). Then there exists $n_0 \in \mathbb{N}$ such that $A^n B$ satisfies (i) for all $n \geq n_0$. Now we show that $D := A^n B$ for some $n \geq n_0$ satisfies (ii), which is equivalent to showing that

$$\lambda_{a_1}^n \mu_{a_1} \neq \lambda_{a_2}^n \mu_{a_2} \quad (8)$$

for all $a_1 \neq a_2$ in the set $\mathcal{J} = \{(i, l) : 1 \leq i \leq k, 1 \leq l \leq r_i\}$. We say that $a_1 \sim a_2$ if there exists $n \in \mathbb{N}$ such that $\lambda_{a_1}^n = \lambda_{a_2}^n$. It is easy to check that this is an equivalence relation and there exists m_0 such that $\lambda_{a_1}^{m_0} = \lambda_{a_2}^{m_0}$ for all a_1 and a_2 in the same equivalence class.

It follows from the independence assumption (b) of the main theorem and (4) that

$$(\lambda_{a_1}^u, \mu_{a_1}^u) \neq (\lambda_{a_2}^u, \mu_{a_2}^u) \quad \text{for all } a_1 \neq a_2 \text{ and } u \in \mathbb{N}.$$

Thus, if a_1 and a_2 belong to the same equivalence class, then $\mu_{a_1}^{m_0} \neq \mu_{a_2}^{m_0}$ and, in particular, $\mu_{a_1} \neq \mu_{a_2}$. This implies that (8) holds within the same equivalence class when n is a multiple of m_0 .

Now we consider the case when $a_1 \neq a_2$ belong to different equivalence classes. If (8) fails for n' and n'' , then

$$\lambda_{a_1}^{n'-n''} = \lambda_{a_2}^{n'-n''},$$

and $n' = n''$. Hence, in this case (8) may fail only for finitely many n 's. Hence, if we take n to be a sufficiently large multiple of m_0 , then both (i) and (ii) hold. $\square$

We apply the argument of [2, Section II.3] to the sequence $(y^{(s)})_{s \geq 1}$ and $D \in \Sigma$ constructed in Lemma 4.2. This yields the following lemma (cf. [2, Lemma II.11]).

We say that a set Y is an ϵ -net for the set X if for every $x \in X$ there exists $y \in Y$ within distance ϵ from x .

Lemma 4.3. Assume that Υ' contains a torsion point r fixed by Σ . Then there exist $D \in \Sigma$, a prime p , $\mathcal{J} \subset \{(i, j, l) \in \mathcal{I}: p_{ij} = p\}$, $c_b \neq 0$ with $b \in \mathcal{J}$ in a finite extension of $\mathbb{Q}_p$, $u \in \tilde{\Omega}$ and t_m satisfying

$$\begin{aligned} t_m \left(\max_{b \in \mathcal{J}} |\lambda_b(D)|_p \right)^m &\rightarrow \infty \quad \text{when } p = \infty, \\ p^{-t_m} \left(\max_{b \in \mathcal{J}} |\lambda_b(D)|_p \right)^m &\rightarrow \infty \quad \text{when } p < \infty, \end{aligned} \quad (9)$$

such that if we define

$$v^{m,t} := D^m(u) + t \sum_{b \in \mathcal{J}} \lambda_b(D)^m c_b v_b,$$

where $t \in [0, t_m]$ when $p = \infty$, and $t \in p^{t_m} \mathbb{Z}_p$ when $p < \infty$, then $v^{m,t} \in \Omega$ and for every $\epsilon > 0$ and $m > m(\epsilon)$, the set $\pi^{-1}(\Upsilon - r)$ forms an ϵ -net for $\{v^{m,t}\}$.

5. Proof of the main theorem

As in the previous section, $\Upsilon = \{\pi(A^m B^n v): m, n \in \mathbb{N}\}$, and Υ' is the set of limit points of Υ . We first assume that Υ' contains a torsion point r fixed by Σ and apply Lemma 4.3. Let

$$\lambda := \max_{b \in \mathcal{J}} |\lambda_b(D)|_p \quad \text{and} \quad \mathcal{K} := \{b \in \mathcal{J}: |\lambda_b(D)|_p = \lambda\}.$$

We take a sequence $t'_m < t_m$ such that

$$t'_m \lambda^m \rightarrow \infty \quad \text{and} \quad t'_m \left(\max_{b \in \mathcal{J} \setminus \mathcal{K}} |\lambda_b(D)|_p \right)^m \rightarrow 0 \quad (10)$$

when $p = \infty$, and

$$p^{-t'_m} \lambda^m \rightarrow \infty \quad \text{and} \quad p^{-t'_m} \left(\max_{b \in \mathcal{J} \setminus \mathcal{K}} |\lambda_b(D)|_p \right)^m \rightarrow 0 \quad (11)$$

when $p < \infty$. Let

$$w^{m,t} = D^m(u) + t \sum_{b \in \mathcal{K}} \lambda_b(D)^m c_b v_b$$

where $t \in [0, t'_m]$ when $p = \infty$, and $t \in p^{t'_m} \mathbb{Z}_p$ when $p < \infty$. It follows from (10) and (11) that for every $\epsilon > 0$ and $m > m(\epsilon)$, $\{v^{m,t}\}$ forms an ϵ -net for $\{w^{m,t}\}$. This shows that we may assume that in Lemma 4.3 $|\lambda_b(D)|_p = \lambda$ for all $b \in \mathcal{J}$. We write $\lambda_b(D) = \lambda \omega_b$ where $|\omega_b|_p = 1$.

We claim that there exists $1 \leq m_0 \leq |\mathcal{J}|$ such that

$$c(m_0) := \sum_{b \in \mathcal{J}} \omega_b^{m_0} c_b \neq 0. \quad (12)$$

Indeed, suppose that $c(m) = 0$ for all $1 \leq m \leq |\mathcal{J}|$. This implies that the $(|\mathcal{J}| \times |\mathcal{J}|)$ -matrix

$$(\lambda_b(D)^m)_{b \in \mathcal{J}, 1 \leq m \leq |\mathcal{J}|}$$

is degenerate. However, it follows from Lemma 4.2(ii) that $\lambda_{b_1}(D) \neq \lambda_{b_2}(D)$ for $b_1 \neq b_2$, which is a contradiction. Hence, (12) holds.

We claim that there exists a subsequence $m_i \rightarrow \infty$ such that $\omega_b^{m_i} \rightarrow \omega_b^{m_0}$ for all $b \in \mathcal{J}$. To show this, we consider the rotation on the compact abelian group $\{|z|_p = 1\}^{\mathcal{J}}$ defined by the vector $(\omega_b)_{b \in \mathcal{J}}$. Since the orbit closure of the identity is minimal, it follows that $(\omega_b^{m_i})_{b \in \mathcal{J}} \rightarrow (1, \dots, 1)$ along a subsequence, and the claim follows.

We consider the cases $p = \infty$ and $p < \infty$ separately. Suppose that $p = \infty$. We observe that by (5),

$$\Pi(v^{m_i, t}) = z_m + \sum_{b \in \mathcal{J}} \{t\lambda^m \omega_b^m c_b\}_{\infty} = z_m + \{t\lambda^m c(m)\}_{\infty} \pmod{1},$$

where $z_m = \Pi(D^m(u))$. Since

$$t_{m_i} \lambda^{m_i} \rightarrow \infty \quad \text{and} \quad c(m_i) \rightarrow c(m_0) \neq 0,$$

we conclude that for all sufficiently large i ,

$$\Pi(\{v^{m_i, t}\}_{0 \leq t \leq t_{m_i}}) = \mathbb{R}/\mathbb{Z}.$$

On the other hand, for every $\epsilon > 0$ and $i > i(\epsilon)$, the set $\pi^{-1}(\mathcal{Y} - r)$ forms an ϵ -net for $\{v^{m_i, t}\}_{0 \leq t \leq t_{m_i}}$. Therefore, since Π is continuous, it follows that $\Pi(\mathcal{Y} - r)$ is dense in $\mathbb{R}/\mathbb{Z}$, which completes the proof of the theorem.

Now suppose that $p < \infty$. In this case, $\lambda = p^{-n}$, and

$$\Pi(v^{m_i, t}) = z_m + \sum_{b \in \mathcal{J}} \{tp^{-mn} \omega_b^m c_b\}_p = z_m + \{tp^{mn} c(m)\}_p \pmod{1}.$$

For all sufficiently large i , we have $|c(m_i)|_p = |c(m_0)|_p = p^l$. Thus,

$$\begin{aligned} \{\Pi(v^{m_i, t})\}_{t \in p^{t_{m_i}} \mathbb{Z}_p} &= z_{m_i} + \{p^{t_{m_i} - nm_i + l} \mathbb{Z}_p\}_p \\ &= z_{m_i} + \left\{ \sum_{j=t_{m_i} - nm_i + l}^{-1} c_j p^j : 0 \leq c_j \leq p-1 \right\} \pmod{1}, \end{aligned}$$

and this set is $p^{t_{m_i} - nm_i + l}$ -dense in $\mathbb{R}/\mathbb{Z}$. Since $p^{-t_{m_i} + nm_i} \rightarrow \infty$, for all $\epsilon > 0$ and $i > i(\epsilon)$ this set forms an ϵ -net for $\mathbb{R}/\mathbb{Z}$. On the other hand, for every $\epsilon > 0$ and sufficiently large i , the set $\pi^{-1}(\mathcal{Y} - r)$ forms an ϵ -net for $\{v^{m_i, t}\}_{t \in p^{t_{m_i}} \mathbb{Z}_p}$. Hence, we conclude that $\Pi(\mathcal{Y} - r)$ is dense in $\mathbb{R}/\mathbb{Z}$.

This completes the proof of the theorem under the assumption that $\mathcal{Y}'$ contains a torsion point r fixed by Σ . To prove the theorem in general, we observe that by Lemma 3.3 there exist $s \in \mathbb{N}$ and a torsion point $r \in \mathcal{Y}'$ such that $A^s(r) = B^s(r) = r$. Then there exist $0 \leq m_0, n_0 \leq s-1$ such that r is an accumulation point for $\{\pi(A^{ms+m_0} B^{ns+n_0} v) : m, n \in \mathbb{N}\}$. Applying the above argument to the semigroup $\Sigma' = \langle A^s, B^s \rangle$ and the vector $v' = A^{m_0} B^{n_0} v$, we establish the theorem in general.

Acknowledgments

The first author is supported by EPSRC, ERC and RCUK, and the second author is supported by EPSRC.

References

- [1] D. Berend, Minimal sets on tori, *Ergodic Theory Dynam. Systems* 4 (1984) 499–507.
- [2] D. Berend, Multi-invariant sets on compact abelian groups, *Trans. Amer. Math. Soc.* 286 (1984) 505–535.
- [3] D. Berend, Dense (mod 1) dilated semigroups of algebraic numbers, *J. Number Theory* 26 (1987) 246–256.
- [4] B. Kra, A generalization of Furstenberg's Diophantine theorem, *Proc. Amer. Math. Soc.* 127 (7) (1999) 1951–1956.
- [5] R. Urban, On density modulo 1 of some expressions containing algebraic integers, *Acta Arith.* 127 (3) (2007) 217–229.
- [6] R. Urban, Algebraic numbers and density modulo 1, *J. Number Theory* 128 (2008) 645–661.
- [7] R. Urban, Algebraic numbers and density modulo 1, II, *Unif. Distrib. Theory* 5 (2010) 111–132.