MIXING AUTOMORPHISMS OF COMPACT GROUPS AND A THEOREM OF SCHLICKEWEI

KLAUS SCHMIDT AND TOM WARD

Abstract. We prove that every mixing $\mathbb{Z}^d$-action by automorphisms of a compact, connected, abelian group is mixing of all orders.

1. Introduction

If α is a mixing automorphism of a compact, abelian group X, then α is Bernoulli and hence mixing of all orders ([6], [8]). However, if $d > 1$, and if α is a mixing $\mathbb{Z}^d$-action by automorphismsms of a compact, abelian group X, then α need not be mixing of every order ([5]), and the intricate way in which higher order mixing can break down may be used to construct measurable isomorphism invariants for α ([3]). In [11] the question was raised whether higher order mixing can fail only if X is disconnected, and a partial result in this direction was obtained (the absence of *nonmixing shapes* for $\mathbb{Z}^d$-actions on connected groups). In this paper we answer this question by proving that every mixing $\mathbb{Z}^d$-action α by automorphisms of a compact, connected, abelian group is mixing of all orders. Even for commuting toral automorphisms this statement is far from obvious, and its proof depends on a highly nontrivial estimate by H.P. Schlickewei ([9]) of the maximal number of solutions $(v_1, \dots, v_r)$ of equations of the form $a_1 v_1 + \cdots + a_r v_r = 1$, subject to certain constraints, where the a_i and v_i lie in an algebraic number field $\mathbb{K}$.

2. Multiple mixing and prime ideals

Let $(X, \mathfrak{S}, \mu)$ be a standard (or Lebesgue) probability space, $d \geq 1$, and let $T : \mathbf{n} \to T_{\mathbf{n}}$ be a measure preserving $\mathbb{Z}^d$-action on $(X, \mathfrak{S}, \mu)$. The action T is *mixing of order* r (or r-*mixing*, or *mixing on* r *sets*) if,

---

1991 *Mathematics Subject Classification.* 22D40, 28C10, 11D61.

The second author gratefully acknowledges support from NSF grant DMS-91-03056 at the Ohio State University.

for all sets $B_1, \dots, B_r$ in $\mathfrak{S}$,

$$\lim_{\mathbf{n}_l \in \mathbb{Z}^d \text{ and } \mathbf{n}_l - \mathbf{n}_{l'} \to \infty \text{ for } 1 \le l' < l \le r} \mu\left(\bigcap_{l=1}^{r} T_{-\mathbf{n}_l}(B_l)\right) = \prod_{l=1}^{r} \mu(B_l). \tag{1}$$

In (1) we may obviously assume that $\mathbf{n}_1 = \mathbf{0}$. Now assume that X is a compact, abelian group (always assumed to be metrizable), $\mathfrak{S} = \mathfrak{B}_X$ is the Borel field of X, and that $\mu = \lambda_X$ is the normalized Haar measure of X. We write $\hat{X}$ for the dual group of X, denote by $\langle x, \chi \rangle = \chi(x)$ the value at $x \in X$ of a character $\chi \in \hat{X}$, and write $\hat{\eta}$ for the automorphism $\hat{\eta}(\chi) = \chi \cdot \eta$, $\chi \in \hat{X}$, of $\hat{X}$ dual to a continuous automorphism η of X. A homomorphism $\alpha : \mathbf{n} \to \alpha_{\mathbf{n}}$ from $\mathbb{Z}^d$ into the group $Aut(X)$ of continuous automorphisms of X is a $\mathbb{Z}^d$*-action by automorphisms of* X. From (2.1) it is clear that a $\mathbb{Z}^d$-action α by automorphisms of a compact, abelian group X is r-mixing if and only if, for all characters $\chi_1, \dots, \chi_r$ in $\hat{X}$ with $\chi_i \neq 1$ for some $i \in \{1, \dots, r\}$,

$$\lim_{\mathbf{n}_l \in \mathbb{Z}^d \text{ and } \mathbf{n}_l - \mathbf{n}_{l'} \to \infty \text{ for } 1 \le l' < l \le r} \int (\chi_1 \cdot \alpha_{\mathbf{n}_1}) \cdots (\chi_r \cdot \alpha_{\mathbf{n}_r}) \, d\lambda_X = 0. \tag{2}$$

Again we may assume that $\mathbf{n}_1 = \mathbf{0}$ in (2). The equivalence of (1) and (2) is seen by expanding the indicator functions of the sets B_i as Fourier series.

Before we discuss the higher order mixing properties of $\mathbb{Z}^d$-actions by automorphisms of compact, abelian groups we recall the algebraic description of such actions in [2] and [10]. Let $\mathfrak{R}_d = \mathbb{Z}[u_1^{\pm 1}, \dots, u_d^{\pm 1}]$ be the ring of Laurent polynomials with integral coefficients in the commuting variables $u_1, \dots, u_d$. If α is a $\mathbb{Z}^d$-action by automorphisms of a compact, abelian group X, then the dual group $\mathfrak{M} = \hat{X}$ of X becomes an $\mathfrak{R}_d$-module under the $\mathfrak{R}_d$-action defined by

$$f \cdot a = \sum_{\mathbf{m} \in \mathbb{Z}^d} c_f(\mathbf{m}) \beta_{\mathbf{m}}(a) \tag{3}$$

for all $a \in \mathfrak{M}$ and $f = \sum_{\mathbf{m} \in \mathbb{Z}^d} c_f(\mathbf{m}) u^{\mathbf{m}} \in \mathfrak{R}_d$, where $u^{\mathbf{n}} = u_1^{n_1} \cdots u_d^{n_d}$ for every $\mathbf{n} = (n_1, \dots, n_d) \in \mathbb{Z}^d$, and where $\beta_{\mathbf{n}} = \widehat{\alpha_{\mathbf{n}}}$ is the automorphism of $\mathfrak{M} = \hat{X}$ dual to $\alpha_{\mathbf{n}}$. In particular,

$$\widehat{\alpha_{\mathbf{n}}}(a) = \beta_{\mathbf{n}}(a) = u^{\mathbf{n}} \cdot a \tag{4}$$

for all $\mathbf{n} \in \mathbb{Z}^d$ and $a \in \mathfrak{M}$. Conversely, if $\mathfrak{M}$ is an $\mathfrak{R}_d$-module, and if

$$\beta_{\mathbf{n}}^{\mathfrak{M}}(a) = u^{\mathbf{n}} \cdot a \tag{5}$$

for every $\mathbf{n} \in \mathbb{Z}^d$ and $a \in \mathfrak{M}$, then we obtain a $\mathbb{Z}^d$-action

$$\alpha^{\mathfrak{M}} : \mathbf{n} \to \alpha_{\mathbf{n}}^{\mathfrak{M}} = \widehat{\beta_{\mathbf{n}}^{\mathfrak{M}}} \tag{6}$$

on the compact, abelian group

$$X^{\mathfrak{M}} = \widehat{\mathfrak{M}} \tag{7}$$

dual to the $\mathbb{Z}^d$-action $\beta^{\mathfrak{M}} : \mathbf{n} \to \beta^{\mathfrak{M}}_{\mathbf{n}}$ on $\mathfrak{M}$. In this notation the r-mixing condition (2.2) is equivalent to the condition that, for all nonzero elements $(a_1, \dots, a_r) \in \mathfrak{M}^r$,

$$u^{\mathbf{m}_1} \cdot a_1 + \cdots + u^{\mathbf{m}_r} \cdot a_r \neq 0 \tag{8}$$

whenever $\mathbf{m}_l \in \mathbb{Z}^d$ and $\mathbf{m}_l - \mathbf{m}_{l'}$ lies outside some sufficiently large finite subset of $\mathbb{Z}^d$ for all $1 \leq l' < l \leq r$.

If $\mathfrak{M}$ is an $\mathfrak{R}_d$-module, then a prime ideal $\mathfrak{p} \subset \mathfrak{R}_d$ is *associated with* $\mathfrak{M}$ if $\mathfrak{p} = \{f \in \mathfrak{R}_d : f \cdot a = 0\}$ for some $a \in \mathfrak{M}$, and $\mathfrak{M}$ is *associated with a prime ideal* $\mathfrak{p} \subset \mathfrak{R}_d$ if $\mathfrak{p}$ is the only prime ideal in $\mathfrak{R}_d$ which is associated with $\mathfrak{M}$. A nonzero Laurent polynomial $f \in \mathfrak{R}_d$ is a *generalized cyclotomic polynomial* if there exist $\mathbf{m}, \mathbf{n} \in \mathbb{Z}^d$ and a cyclotomic polynomial c in a single variable such that $\mathbf{n} \neq \mathbf{0}$ and $f = u^{\mathbf{m}} c(u^{\mathbf{n}})$. The following theorem was proved in [10].

Theorem 2.1. *Let α be a $\mathbb{Z}^d$-action by automorphisms of a compact, abelian group X, and let $\mathfrak{M} = \hat{X}$ be the $\mathfrak{R}_d$-module arising from α via* (2.3)–(2.4). *The following conditions are equivalent.*

1. *α is mixing (i.e. 2-mixing);*
2. *$\alpha_{\mathbf{m}}$ is ergodic for every $\mathbf{0} \neq \mathbf{m} \in \mathbb{Z}^d$;*
3. *None of the prime ideals associated with $\mathfrak{M}$ contains a generalized cyclotomic polynomial.*

If the $\mathbb{Z}^d$-action α in Theorem 2.1 is mixing, then the higher order mixing behaviour of α is again determined by the prime ideals associated with $\mathfrak{M} = \hat{X}$.

Theorem 2.2. *Let α be a $\mathbb{Z}^d$-action by automorphisms of a compact, abelian group X, and let $\mathfrak{M} = \hat{X}$ be the $\mathfrak{R}_d$-module arising from α via* (2.3)–(2.4). *The following conditions are equivalent for every $r \geq 2$.*

1. *α is r-mixing;*
2. *For every prime ideal $\mathfrak{p} \subset \mathfrak{R}_d$ associated with $\mathfrak{M}$, the $\mathbb{Z}^d$-action $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ defined in* (2.5)–(2.7) *is r-mixing.*

Proof. Suppose that α is r-mixing. If $\mathfrak{p} \subset \mathfrak{R}_d$ is a prime ideal associated with $\mathfrak{M}$, then there exists an element $a \in \mathfrak{M}$ such that $\mathfrak{p} = \{f \in \mathfrak{R}_d : f \cdot a = 0\}$, and we set $\mathfrak{Y} = \mathfrak{R}_d \cdot a \subset \mathfrak{M}$. Then $\mathfrak{Y} \cong \mathfrak{R}_d/\mathfrak{p}$ and $Y = \widehat{\mathfrak{Y}} = X/\mathfrak{Y}^{\perp}$, where $\mathfrak{Y}^{\perp} = \{x \in X : \langle x, a \rangle = 1 \text{ for all } a \in \mathfrak{Y}\}$ is the annihilator of $\mathfrak{Y}$. Since $\mathfrak{Y}$ is invariant under the $\mathbb{Z}^d$-action $\beta : \mathbf{n} \to \beta_{\mathbf{n}} = \widehat{\alpha_{\mathbf{n}}}$ dual to α, $\mathfrak{Y}^{\perp}$ is a closed, α-invariant subgroup of X, and the $\mathbb{Z}^d$-action α^Y induced by α on Y is a factor of α and hence r-mixing.

Since the $\mathfrak{R}_d$-module arising from α^Y is equal to $\hat{Y} = \mathfrak{Y} \cong \mathfrak{R}_d/\mathfrak{p}$ we conclude that $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ must be r-mixing.

Conversely, if α is not r-mixing, then (2.8) shows that there exists a nonzero element $(a_1, \dots, a_r) \in \mathfrak{M}^r$ and a sequence $(\mathbf{n}^{(m)} = (\mathbf{n}_1^{(m)}, \dots, \mathbf{n}_r^{(m)}),\ m \geq 1)$ in $(\mathbb{Z}^d)^r$ such that $\lim_{m\to\infty} \mathbf{n}_l^{(m)} - \mathbf{n}_{l'}^{(m)} = \infty$ for $1 \leq l' < l \leq r$ and $u^{\mathbf{n}_1^{(m)}} \cdot a_1 + \dots + u^{\mathbf{n}_r^{(m)}} \cdot a_r = 0$ for every $m \geq 1$. There exists a Noetherian submodule $\mathfrak{N} \subset \mathfrak{M}$ such that $\{a_1, \dots, a_r\} \subset \mathfrak{N}$, and (2.8) implies that the $\mathbb{Z}^d$-action $\alpha^{\mathfrak{N}}$, which is a quotient of α, is not r-mixing.

Since $\mathfrak{N}$ is Noetherian, the set of (distinct) prime ideals associated with $\mathfrak{N}$ is finite and equal to $\{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$, say. By Theorem VI.5.3 in [4] there exist submodules $\mathfrak{W}_1, \dots, \mathfrak{W}_m$ of $\mathfrak{N}$ such that $\mathfrak{N}/\mathfrak{W}_i$ is associated with $\mathfrak{p}_i$ for $i = 1, \dots, m$, $\bigcap_{i=1}^m \mathfrak{W}_i = \{0\}$, and $\bigcap_{i\in S} \mathfrak{W}_i \neq \{0\}$ for every subset $S \subsetneq \{1, \dots, m\}$. In particular, the map $a \to (a + \mathfrak{W}_1, \dots, a + \mathfrak{W}_m)$ from $\mathfrak{N}$ into $\mathfrak{K} = \bigoplus_{i=1}^m \mathfrak{N}/\mathfrak{W}_i$ is injective, and the dual homomorphism from $\bar{X} = \widehat{\mathfrak{K}}$ to $\widehat{\mathfrak{N}} = X^{\mathfrak{N}}$ is surjective. Hence $\alpha^{\mathfrak{N}}$ is a factor of $\alpha^{\mathfrak{K}}$, so that $\alpha^{\mathfrak{K}}$ cannot be r-mixing. By applying (2.8) to the $\mathfrak{R}_d$-module $\mathfrak{K}$ we see that there exists a $j \in \{1, \dots, m\}$ such that $\alpha^{\mathfrak{N}/\mathfrak{W}_j}$ is not r-mixing.

Put $\mathfrak{V} = \mathfrak{N}/\mathfrak{W}_j$, $\mathfrak{p} = \mathfrak{p}_j$, and use Lemma 3.4 in [3] to find integers $1 \leq t \leq s$ and submodules $\mathfrak{V} = \mathfrak{N}_s \supset \cdots \supset \mathfrak{N}_0 = \{0\}$ such that, for every $k = 1, \dots, s$, $\mathfrak{N}_k/\mathfrak{N}_{k-1} \cong \mathfrak{R}_d/\mathfrak{q}_k$ for some prime ideal $\mathfrak{p} \subset \mathfrak{q}_k \subset \mathfrak{R}_d$, $\mathfrak{q}_k = \mathfrak{p}$ for $k = 1, \dots, t$, and $\mathfrak{q}_k \supsetneq \mathfrak{p}$ for $i = t+1, \dots, s$. We choose Laurent polynomials $g_k \in \mathfrak{q}_k \smallsetminus \mathfrak{p}$, $k = t+1, \dots, s$, and set $g = g_{t+1} \cdots g_s$. Since $\alpha^{\mathfrak{V}}$ is not r-mixing, (2.8) implies the existence of a nonzero element $(a_1, \dots, a_r) \in \mathfrak{V}^r$ and a sequence $(\mathbf{n}^{(m)} = (\mathbf{n}_1^{(m)}, \dots, \mathbf{n}_r^{(m)}),\ m \geq 1)$ in $(\mathbb{Z}^d)^r$ such that $\lim_{m\to\infty} \mathbf{n}_l^{(m)} - \mathbf{n}_{l'}^{(m)} = \infty$ whenever $1 \leq l' < l \leq r$, and $u^{\mathbf{n}_1^{(m)}} \cdot a_1 + \dots + u^{\mathbf{n}_r^{(m)}} \cdot a_r = 0$ for every $m \geq 1$. Put $b_i = g \cdot a_i$, and note that $0 \neq (b_1, \dots, b_r) \in (\mathfrak{N}_t)^r$, since $g \cdot a \neq 0$ for every nonzero element $a \in \mathfrak{V}$. There exists a unique integer $p \in \{1, \dots, t\}$ such that $(b_1, \dots, b_r) \in (\mathfrak{N}_p)^r \smallsetminus (\mathfrak{N}_{p-1})^r$, and by setting $b_i' = b_i + \mathfrak{N}_{p-1} \in \mathfrak{N}_p/\mathfrak{N}_{p-1} \cong \mathfrak{R}_d/\mathfrak{p}$ we obtain that $0 \neq (b_1', \dots, b_r') \in (\mathfrak{N}_p/\mathfrak{N}_{p-1})^r \cong (\mathfrak{R}_d/\mathfrak{p})^r$ and $u^{\mathbf{n}_1^{(m)}} \cdot b_1' + \dots + u^{\mathbf{n}_r^{(m)}} \cdot b_r' = 0$ for every $m \geq 1$, so that $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ is not r-mixing by (2.8). Since the prime ideal $\mathfrak{p}$ is associated with the submodule $\mathfrak{N} \subset \mathfrak{M}$, $\mathfrak{p}$ is also associated with $\mathfrak{M}$, and the theorem is proved. □

3. Schlickewei's theorem and mixing

Theorem 2.2 shows that a $\mathbb{Z}^d$-action α by automorphisms of a compact, abelian group X is mixing of order $r \geq 2$ if and only if the

$\mathbb{Z}^d$-actions $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ are r-mixing for all prime ideals $\mathfrak{p} \subset \mathfrak{R}_d$ associated with the $\mathfrak{R}_d$-module $\mathfrak{M} = \hat{X}$ defined by α (cf. (2.3)–(2.8)). In order to be able to apply this result we shall characterize those prime ideals $\mathfrak{p} \subset \mathfrak{R}_d$ for which $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ is r-mixing for every $r \geq 2$.

We identify $\mathbb{Z}$ with the set of constant polynomials in $\mathfrak{R}_d$ and note that, for every prime ideal $\mathfrak{p} \subset \mathfrak{R}_d$, $\mathfrak{p} \cap \mathbb{Z}$ is either equal to $p\mathbb{Z}$ for some rational prime $p = p(\mathfrak{p})$, or to $\{0\}$, in which case we set $p(\mathfrak{p}) = 0$.

Theorem 3.1. *Let $d \geq 1$, and let $\mathfrak{p} \subset \mathfrak{R}_d$ be a prime ideal such that $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ is mixing (cf.* Theorem 2.1).

(1) *If $p(\mathfrak{p}) > 0$ then $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ is r-mixing for every $r \geq 2$ if and only if $\mathfrak{p} = (p(\mathfrak{p})) = p(\mathfrak{p})\mathfrak{R}_d$;*
(2) *If $p(\mathfrak{p}) = 0$ then $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ is r-mixing for every $r \geq 2$.*

Theorem 3.1 (1) follows from Theorem 3.3 (2) of [Sc2]. We postpone the proof of Theorem 3.1 (2) for the moment and look instead at some of the consequences of that theorem. If α is a $\mathbb{Z}^d$-action by automorphisms of a compact, abelian group X with completely positive entropy, then it is mixing of all orders by Theorem 6.5 and Corollary 6.7 in [7]. If the group X is zero-dimensional, the reverse implication is also true.

Corollary 3.2. *Let α be a $\mathbb{Z}^d$-action by automorphisms of a compact, abelian, zero-dimensional group X. The following conditions are equivalent.*

(1) *α has completely positive entropy;*
(2) *α is r-mixing for every $r \geq 2$.*

Proof. Since X is zero-dimensional, every prime ideal $\mathfrak{p}$ associated with the $\mathfrak{R}_d$-module $\mathfrak{M} = \hat{X}$ arising from α via (2.3)–(2.4) contains a nonzero constant, so that $p(\mathfrak{p}) > 0$. According to Theorem 6.5 in [7], this implies that α has completely positive entropy if and only if $\mathfrak{p} = p(\mathfrak{p}) \cdot \mathfrak{R}_d$ for every prime ideal $\mathfrak{p}$ associated with $\mathfrak{M}$, and the equivalence of (1) and (2) follows from Theorem 2.2 and Theorem 3.1 (1). $\square$

The next corollary shows that the higher order mixing behaviour of $\mathbb{Z}^d$-actions by automorphisms of compact, connected, abelian groups is quite different from the zero-dimensional case, and requires no assumptions concerning entropy.

Corollary 3.3. *Let $d \geq 1$, and let α be a mixing $\mathbb{Z}^d$-action on a compact, connected, abelian group X. Then α is r-mixing for every $r \geq 2$.*

Proof. The group X is connected if and only if the dual group $\hat{X}$ is torsion-free, i.e. if and only if $na \neq 0$ whenever $0 \neq a \in \hat{X}$ and $0 \neq n \in \mathbb{Z}$. We write $\mathfrak{M} = \hat{X}$ for the $\mathfrak{R}_d$-module defined by α via (2.3)–(2.4), note that the connectedness of X implies that $p(\mathfrak{p}) = 0$ for every prime ideal $\mathfrak{p} \subset \mathfrak{R}_d$ associated with $\mathfrak{M}$, and apply Theorems 2.2 and 3.1 (2). □

Corollary 3.4. *Let $A_1, \dots, A_d$ be commuting automorphism of the n-torus $\mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n$ with the property that the $\mathbb{Z}^d$-action $\alpha : (m_1, \dots, m_d) \to \alpha_{(m_1,\dots,m_d)} = A_1^{m_1} \cdots A_d^{m_d}$ is mixing. Then α is r-mixing for every $r \geq 2$.*

The proof of Theorem 3.1 (2) depends on a result by Schlickewei [9]. Let $\mathbb{K}$ be an algebraic number field of degree D, and let $P(\mathbb{K})$ be the set of places and $P_\infty(\mathbb{K})$ the set of infinite (or archimedean) places of $\mathbb{K}$. For every $v \in P(\mathbb{K})$, $|\cdot|_v$ denotes the associated absolute value, normalized so that $|a|_v$ is equal to the standard absolute value $|a|$ if $v \in P_\infty(\mathbb{K})$ and $a \in \mathbb{Q}$, and $|p|_v = p^{-1}$ if v lies above the rational prime p. Let S, $P_\infty(\mathbb{K}) \subset S \subset P(\mathbb{K})$, be a finite set of cardinality s. An element $a \in \mathbb{K}$ is an *S-unit* if $|a|_v = 1$ for every $v \in P(\mathbb{K}) \smallsetminus S$.

Theorem 3.5. (Schlickewei) *Let $a_1, \dots, a_n$ be nonzero elements of $\mathbb{K}$. Then the equation*

$$a_1 v_1 + \dots + a_n v_n = 1 \tag{9}$$

has not more than

$$(4sD!)^{2^{36nD!}s^6}$$

solutions $(v_1, \dots, v_n)$ in S-units such that no proper subsum $a_{i_1}v_{i_1} + \dots + a_{i_k}v_{i_k}$ vanishes.

Proof. Proof of Theorem 3.1 (2) For every field $\mathbb{F}$ we set $\mathbb{F}^\times = \mathbb{F} \smallsetminus \{0\}$. Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the algebraic closure of $\mathbb{Q}$, and let $V(\mathfrak{p}) = \{\mathbf{c} = (c_1, \dots, c_d) \in (\overline{\mathbb{Q}}^\times)^d : f(\mathbf{c}) = 0 \text{ for every } f \in \mathfrak{p}\}$ and $V_\mathbb{C}(\mathfrak{p}) = \{\mathbf{c} = (c_1, \dots, c_d) \in (\mathbb{C}^\times)^d : f(\mathbf{c}) = 0 \text{ for every } f \in \mathfrak{p}\}$.

Suppose that $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ is not r-mixing for some $r \geq 3$, and that r is the smallest integer with this property. According to (2.8) there exists a nonzero element $(a_1, \dots, a_r) \in (\mathfrak{R}_d/\mathfrak{p})^r$ and a sequence $(\mathbf{n}^{(m)} = (\mathbf{n}_1^{(m)}, \dots, \mathbf{n}_r^{(m)}), m \geq 1)$ in $(\mathbb{Z}^d)^r$ such that $\lim_{m\to\infty} \mathbf{n}_l^{(m)} - \mathbf{n}_{l'}^{(m)} = \infty$ whenever $1 \leq l' < l \leq r$, and $u^{\mathbf{n}_1^{(m)}} \cdot a_1 + \dots + u^{\mathbf{n}_r^{(m)}} \cdot a_r = 0$ for every $m \geq 1$. For simplicity we assume that $\mathbf{n}^{(m)} \neq \mathbf{n}^{(n)}$ whenever $1 \leq m < n$, and that $\mathbf{n}_1^{(m)} = \mathbf{0}$ for all $m \geq 1$. The minimality of r is easily seen to imply that $a_i \neq 0$ for $i = 1, \dots, r$. Choose $f_i \in \mathfrak{R}_d$ such that $a_i = f_i + \mathfrak{p}$, $i = 1, \dots, r$, set, for every $\mathbf{c} \in V_\mathbb{C}(\mathfrak{p})$ and

$\mathbf{m} = (m_1, \dots, m_d) \in \mathbb{Z}^d$, $\mathbf{c}^{\mathbf{m}} = c_1^{m_1} \cdots c_d^{m_d}$, and note that

$$f_1(\mathbf{c}) + f_2(\mathbf{c})\mathbf{c}^{\mathbf{n}_2^{(m)}} + \cdots + f_r(\mathbf{c})\mathbf{c}^{\mathbf{n}_r^{(m)}} = 0 \tag{10}$$

for all $\mathbf{c} \in V_{\mathbb{C}}(\mathfrak{p})$ and $m \geq 1$.

If $V(\mathfrak{p})$ is finite, then $V(\mathfrak{p}) = V_{\mathbb{C}}(\mathfrak{p})$ consists of the orbit of a single point $\mathbf{c} = (c_1, \dots, c_d)$ under the Galois group $Gal[\overline{\mathbb{Q}} : \mathbb{Q}]$, and the assumption that $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ is mixing is equivalent to saying that $\mathbf{c}^{\mathbf{m}} \neq 1$ whenever $\mathbf{0} \neq \mathbf{m} \in \mathbb{Z}^d$. The evaluation map $f \to f(\mathbf{c})$, $f \in \mathfrak{R}_d$, has kernel $\mathfrak{p}$, and may thus be regarded as an injective homomorphism from $\mathfrak{R}_d/\mathfrak{p}$ into $\mathbb{C}$; in particular, $f_1(\mathbf{c}) \cdots f_r(\mathbf{c}) \neq 0$. We denote by $\mathbb{K}$ the algebraic number field $\mathbb{Q}(\mathbf{c}) = \mathbb{Q}(c_1, \dots, c_d)$ and set $S = P_\infty(\mathbb{K}) \cup \{v \in P(\mathbb{K}) : |c_i|_v \neq 1 \text{ for some } i \in \{1, \dots, d\}\}$. Then S is finite, and Schlickewei's Theorem 3.5 implies that the equation

$$-\frac{f_2(\mathbf{c})}{f_1(\mathbf{c})} v_2 - \cdots - \frac{f_r(\mathbf{c})}{f_1(\mathbf{c})} v_r = 1$$

has only finitely many solutions $(v_2, \dots, v_r)$ in S-units such that $f_{i_1}(\mathbf{c})v_{i_1} + \cdots + f_{i_k}(\mathbf{c})v_{i_k} \neq 0$ whenever $1 < i_1 < \cdots < i_k \leq r$. However, the properties of $\mathbf{c}$ and S imply that the vectors $(\mathbf{c}^{\mathbf{n}_2^{(m)}}, \dots, \mathbf{c}^{\mathbf{n}_r^{(m)}})$, $m \geq 1$, are all distinct, and that $\mathbf{c}^{\mathbf{n}_i^{(m)}}$ is an S-unit for every $i = 2, \dots, r$ and $m \geq 1$. From (10) we conclude that, for all but finitely many $m \geq 1$, one of the subsums $f_{i_1}(\mathbf{c})\mathbf{c}^{\mathbf{n}_{i_1}^{(m)}} + \cdots + f_{i_k}(\mathbf{c})\mathbf{c}^{\mathbf{n}_{i_k}^{(m)}}$ vanishes. For some choice of $1 < i_1 < \cdots < i_k \leq r$ we obtain an infinite set M of positive integers such that $f_{i_1}(\mathbf{c})\mathbf{c}^{\mathbf{n}_{i_1}^{(m)}} + \cdots + f_{i_k}(\mathbf{c})\mathbf{c}^{\mathbf{n}_{i_k}^{(m)}} = 0$ for every $m \in M$, and this is easily seen to imply that $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ fails to be k-mixing, where $k < r$, contrary to the minimality of r.

A moment's reflection shows that we have now proved enough to obtain Corollary 3.4. For Theorem 3.1 (2) and Corollary 3.3, however, we have to deal with the case where $V(\mathfrak{p})$ is infinite. Since $p(\mathfrak{p}) = 0$, the natural homomorphism $\iota : \mathfrak{N} = \mathfrak{R}_d/\mathfrak{p} \longmapsto \mathcal{N} = \mathbb{Q} \otimes_{\mathbb{Z}} \mathfrak{N}$, defined by $a \to 1 \otimes a$ for every $a \in \mathfrak{N}$, is injective, and we put $z_i = \iota(u_i + \mathfrak{p})$ and $z_{d+i} = \iota(u_i^{-1} + \mathfrak{p})$ for $i = 1, \dots, d$. Noether's normalization lemma ([1]), applied to the $\mathbb{Q}$-algebra $\mathcal{N}$, allows us to find an integer $t \in \{1, \dots, 2d\}$ and $\mathbb{Q}$-linear functions $w_1, \dots, w_t$ of the elements $z_1, \dots, z_{2d}$ such that $\{w_1, \dots, w_t\}$ is algebraically independent over $\mathbb{Q}$ and each $z_1, \dots, z_{2d}$ is integral over $\mathbb{Q}[w_1, \dots, w_t]$. We choose and fix monic polynomials $Q_i \in \mathbb{Q}[w_1, \dots, w_t][y] = \mathbb{Q}[w_1, \dots, w_t, y]$ such that $Q_i(w_1, \dots, w_t, z_i) = 0$ for $i = 1, \dots, 2d$ and regard each Q_i either as a polynomial in y with coefficients in $\mathbb{Q}[w_1, \dots, w_t]$, or as an element of $\mathbb{Q}[w_1, \dots, w_t, y]$.

Put $W_{\mathbb{C}}(\mathfrak{p}) = \{(c_1, \dots, c_d, c_1^{-1}, \dots, c_d^{-1}) : (c_1, \dots, c_d) \in V_{\mathbb{C}}(\mathfrak{p})\} \subset \mathbb{C}^{2d}$, define a surjective map $\omega : W_{\mathbb{C}}(\mathfrak{p}) \longmapsto \mathbb{C}^t$ by $\omega(\mathbf{c}) = (w_1(\mathbf{c}), \dots, w_t(\mathbf{c}))$

for every $\mathbf{c} \in W_{\mathbb{C}}(\mathfrak{p})$, and note that $V_{\mathbb{C}}(\mathfrak{p}) = \pi(W_{\mathbb{C}}(\mathfrak{p})) \subset (\mathbb{C}^\times)^d \subset \mathbb{C}^d$, where $\pi : \mathbb{C}^{2d} \longmapsto \mathbb{C}^d$ is the projection onto the first d coordinates. We write $R \subset \mathbb{Q}$ for the set of rational numbers which occur as one of the coefficients of one of the linear maps w_i (regarded as a rational linear map in $2d$ variables), or of one of the polynomials Q_i (regarded as a polynomial in $t+1$ variables with rational coefficients), and let $\mathcal{P}$ denote a nonempty, finite set of rational primes which contains every prime divisor appearing in any element of R (either in the numerator or the denominator). Put $\mathbb{K} = \{a + b\sqrt{-1} : a, b \in \mathbb{Q}\}$ and denote by $S' \subset P(\mathbb{K})$ the (finite) set of all places of $\mathbb{K}$ which are either infinite, or which lie above one of the primes in $\mathcal{P}$. There exists an integer $D \geq 1$ such that, for every $\boldsymbol{\beta} = (\beta_1, \dots, \beta_t) \in \mathbb{K}^t$ and $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_{2d}) \in \omega^{-1}(\boldsymbol{\beta})$, the algebraic number field $\mathbb{K}(\boldsymbol{\gamma})$ generated by $\mathbb{K}$ and $(\gamma_1, \dots, \gamma_{2d})$ has degree $(\mathbb{K}(\boldsymbol{\gamma}) : \mathbb{K}) \leq D$. Then $\mathbb{K}(\boldsymbol{\gamma})$ has at most D distinct places above every place of $\mathbb{K}$, and it follows that the cardinality $|S(\boldsymbol{\gamma})|$ of the set $S(\boldsymbol{\gamma})$ of places of $\mathbb{K}(\boldsymbol{\gamma})$ which lie above one of the elements of S' is bounded by $D \cdot |S'|$, where $|S'|$ is the cardinality of S'.

Let $\Sigma \subset \mathbb{K}$ be the set of S'-units, and let $\boldsymbol{\beta} = (\beta_1, \dots, \beta_t) \in \Sigma^t \subset \mathbb{K}^t$. We claim that every coordinate of every $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_{2d}) \in \omega^{-1}(\boldsymbol{\beta})$ is an $S(\boldsymbol{\gamma})$-unit. Indeed, if $v' \in P(\mathbb{K}) \smallsetminus S'$, and if $v \in P(\mathbb{K}(\boldsymbol{\gamma}))$ lies above v', then γ_i is a root of the monic polynomial $Q_i(\boldsymbol{\beta}, y) \in \mathbb{K}[y]$, and each coefficient ζ of Q_i satisfies that $|\zeta|_{v'} \leq 1$. It follows that $|\gamma_i|_v \leq 1$ for $i = 1, \dots 2d$. In particular, since $\gamma_i^{-1} = \gamma_{i+d}$ for $i \in \{1, \dots, d\}$, we obtain that $|\gamma_i^{-1}|_v = (|\gamma_i|_v)^{-1} \leq 1$, so that $|\gamma_i|_v = |\gamma_{i+d}|_v = 1$, as claimed.

Since Σ is dense in $\mathbb{C}$, the set $\Omega = \pi(\omega^{-1}(\Sigma^t)) \subset V(\mathfrak{p})$ is dense in $V_{\mathbb{C}}(\mathfrak{p})$, and for every $\mathbf{c} = (c_1, \dots, c_d) \in \Omega$ we either have that $f_1(\mathbf{c}) = 0$ and $f_2(\mathbf{c})\mathbf{c}^{\mathbf{n}_2^{(m)}} + \dots + f_r(\mathbf{c})c^{\mathbf{n}_r^{(m)}} = 0$ for every $m \geq 1$, or that $f_1(\mathbf{c}) \neq 0$, in which case case Schlickewei's theorem implies that the equation

$$-\frac{f_2(\mathbf{c})}{f_1(\mathbf{c})}v_2 - \dots - \frac{f_r(\mathbf{c})}{f_1(\mathbf{c})}v_r = 1$$

has at most $C = (4D|S'|D!)^{2^{36(r-1)D!(D|S'|)^6}}$ distinct solutions $(v_2, \dots, v_r)$ in S-units for which no subsum $f_{i_1}(\mathbf{c})v_{i_1} + \dots + f_{i_k}(\mathbf{c})v_{i_k}$ vanishes. For all $1 \leq m < n$, $k < r$, and $\{i_1, \dots, i_k\} \subsetneq \{1, \dots, r\}$ with $1 \leq i_1 < \dots < i_k \leq r$, we set $\Phi^{(m,n)} = \{\mathbf{c} \in V_{\mathbb{C}}(\mathfrak{p}) : \mathbf{c}^{\mathbf{n}_i^{(m)}} = \mathbf{c}^{\mathbf{n}_i^{(n)}} \text{ for } i = 2, \dots, r\}$ and $\Psi(i_1, \dots, i_k)^{(m)} = \{\mathbf{c} \in V_{\mathbb{C}}(\mathfrak{p}) : f_{i_1}(\mathbf{c})\mathbf{c}^{\mathbf{n}_{i_1}^{(m)}} + \dots + f_{i_k}(\mathbf{c})\mathbf{c}^{\mathbf{n}_{i_k}^{(m)}} = 0\}$. As we have just seen,

$$\Omega \subset \bigcup_{s \leq m < n \leq C+s+2} \ \bigcup_{\{i_1, \dots, i_k\} \subsetneq \{1, \dots, r\}} \Psi(i_1, \dots, i_k)^{(m)} \cup \Phi^{(m,n)} \tag{11}$$

for every $s \geq 1$. Since the sets appearing in the right hand side of (11) are all closed subsets of the perfect set $V_{\mathbb{C}}(\mathfrak{p})$, we obtain that

$$V_{\mathbb{C}}(\mathfrak{p}) = \bigcup_{s \leq m < n \leq C+s+2} \quad \bigcup_{\{i_1,\dots,i_k\} \subsetneq \{1,\dots,r\}} \Psi(i_1,\dots,i_k)^{(m)} \cup \Phi^{(m,n)}$$

for every $s \geq 1$. As the ideal $\mathfrak{p} \subset \mathfrak{R}_d$ is prime, the variety $V_{\mathbb{C}}(\mathfrak{p})$ must, for every $s \geq 1$, be contained in one of the sets $\Psi(i_1,\dots,i_k)^{(m)}$ or $\Phi^{(m,n)}$ with $s \leq m < n \leq C+s+2$ and $\{i_1,\dots,i_k\} \subsetneq \{1,\dots,r\}$. The second possibility is excluded by our assumption that $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ is mixing, and we conclude that there exists, for infinitely many $m \geq 1$, a subset $\{i_1,\dots,i_k\} \subsetneq \{1,\dots,r\}$ (depending on m) such that $V_{\mathbb{C}}(\mathfrak{p}) \subset \Psi(i_1,\dots,i_k)^{(m)}$. Since there are only finitely many such subsets we obtain that $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ fails to be k-mixing for some $k < r$, contrary to the minimality of r, exactly as in the case where $V(\mathfrak{p})$ is finite. This contradiction implies that $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ is r-mixing for every $r \geq 2$. □

References

[1] M. Atiyah and I. G. MacDonald: *Introduction to Commutative Algebra*, Addison–Wesley, Reading, Mass. (1969).

[2] B. Kitchens and K. Schmidt: *Automorphisms of compact groups*, Ergod. Th. & Dynam. Sys. **9** (1989), 691–735.

[3] B. Kitchens and K. Schmidt: *Mixing Sets and Relative Entropies for Higher Dimensional Markov Shifts*, Preprint (1991).

[4] S. Lang: *Algebra* (2nd Ed.), Addison–Wesley, Reading, Mass. (1984).

[5] F. Ledrappier: *Un champ markovien peut être d'entropie nulle et mélangeant*, C. R. Acad. Sci. Paris Ser. A. **2**87 (1978), 561–562.

[6] D. Lind: *The structure of skew products with ergodic group automorphisms*, Israel J. Math. **2**8 (1977), 205–248.

[7] D. Lind, K. Schmidt, and T. Ward: *Mahler measure and entropy for commuting automorphisms of compact groups*, Invent. math. **1**01 (1990), 593–629.

[8] G. Miles and R.K. Thomas: *The breakdown of automorphisms of compact topological groups.* In: Studies in Probability and Ergodic Theory, Advances in Mathematics Supplementary Studies Vol. 2, Academic Press: New York–London, 1987, pp. 207–218.

[9] H.P. Schlickewei: *S-unit equations over number fields*, Invent. math. **1**02 (1990), 95–107.

[10] K. Schmidt: *Automorphisms of compact abelian groups and affine varieties*, Proc. London Math. Soc. **6**1 (1990), 480–496.

[11] K. Schmidt: *Mixing automorphisms of compact groups and a theorem by Kurt Mahler*, Pacific J. Math. **1**37 (1989), 371–384.

Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK

Department of Mathematics, Ohio State University, Columbus OH 43210, USA