Pacific Institute
for the Mathematical Sciences

PIMS Distinguished Chair Lectures

KLAUS SCHMIDT

Professor, Mathematics Institute, University of Vienna

and

Director, Erwin Schrödinger Institute
for Mathematical Physics

PIMS Distinguished Chair,
University of Victoria, November, 2002

Algebraic $\mathbb{Z}^d$-actions

ALGEBRAIC $\mathbb{Z}^d$-ACTIONS

A SERIES OF LECTURES BY
KLAUS SCHMIDT
ERWIN SCHRÖDINGER INSTITUTE FOR MATHEMATICAL PHYSICS
BOLTZMANNGASSE 9, A-1090 VIENNA, AUSTRIA

Abstract. This is a written account of five Pacific Institute for the Mathematical Sciences Distinguished Chair Lectures given at the Mathematics Department, University of Victoria, BC, in November 2002. The lectures were devoted to the ergodic theory of $\mathbb{Z}^d$-actions, i.e. of several commuting automorphisms of a probability space. After some introductory remarks on more general $\mathbb{Z}^d$-actions the lectures focused on 'algebraic' $\mathbb{Z}^d$-actions, their sometimes surprising properties, and their deep connections with algebra and arithmetic. Special emphasis was given to some of the very recent developments in this area, such as higher order mixing behaviour and rigidity phenomena.

Contents

I would like to thank the Pacific Institute for the Mathematical Sciences and the Department of Mathematics at the University of Victoria, BC, for the invitation to give these lectures and a very pleasant stay in Victoria while I was delivering them. Special thanks are due to Ian Putnam for his kind hospitality and to him and Dil Bains for assistance in all respects. My thanks are also due to the Mathematics Department, University of Washington, Seattle, for hospitality and support while writing up these notes, and to Manfred and Grete Einsiedler, Doug Lind, Selim Tuncel and Karin Bornfeldt for making my stay there very enjoyable.

This work was partially supported by the FWF Project P16004-MAT and the NSF grant DMS 0222452.

1. Introduction

Although $\mathbb{Z}^d$-actions have played an important role in physics (for example, in the lattice models of statistical mechanics), the mathematical theory of these actions has been hampered to some extent by the lack of classes of examples which one could analyze systematically. The two classical sources of examples are multi-dimensional shifts of finite type and commuting diffeomorphisms of smooth manifolds. Both these classes have serious limitations: the first leads very quickly to undecidability problems (mentioned briefly in Section 3), and the second by necessity to $\mathbb{Z}^d$-actions for which every $\mathbb{Z}^{d'}$-subaction with $d' > 1$ has zero entropy.

About 15 years ago a class of $\mathbb{Z}^d$-actions emerged which was rich enough to exhibit a variety of new and unexpected phenomena and yet simple enough to allow detailed investigation: the $\mathbb{Z}^d$-actions by commuting automorphisms of compact abelian groups, or *algebraic $\mathbb{Z}^d$-actions* for short. By using Pontryagin duality one can associate with each such $\mathbb{Z}^d$-action α a module M over the ring $R_d = \mathbb{Z}[u_1^{\pm 1}, \dots, u_d^{\pm 1}]$ of Laurent polynomials in d variables (or, equivalently, over the group ring of $\mathbb{Z}^d$), and by identifying certain algebraic properties of this module (which can largely be expressed in terms of its associated prime ideals) with dynamical properties of α. If one understands this translation of between algebra and dynamics well enough one can use it to construct explicit algebraic $\mathbb{Z}^d$-actions with prescribed dynamical behaviour (such as $\mathbb{Z}^d$-actions with completely positive entropy with or without expansiveness, or mixing zero-entropy $\mathbb{Z}^d$-actions which have $\mathbb{Z}^{d'}$-subactions with completely positive entropy for some d' with $1 \le d' < d$, or $\mathbb{Z}^d$-actions which are mixing of order r, but not of order $r+1$, for any $r \ge 2$).

Some of the correspondence between algebraic properties of the modules and dynamical properties of the $\mathbb{Z}^d$-actions is quite straightforward, such as ergodicity and mixing. Other dynamical properties express themselves more subtly in terms of algebra: expansiveness, entropy and the Bernoulli property may serve as examples (cf. Section 4). An intriguing connection between algebra and dynamics which has been clarified only recently is the link between the higher order mixing behaviour of algebraic $\mathbb{Z}^d$-actions and additive relations in fields: this will be discussed in the Sections 5–7 of these notes.

Perhaps the most puzzling problems in this area are the rigidity properties of algebraic $\mathbb{Z}^d$-actions with zero entropy, which express themselves in a number of different ways as scarcity of invariant probability measures, of Haar measure preserving Borel automorphisms commuting with the actions, or of measurable conjugacies between such actions. In spite of some recent progress many of the main questions are still virtually untouched. I describe these problems and some of the partial answers in the Sections 8–10.

These notes are, of course, a considerably expanded version of the original lectures. Some parts of these notes will appear in print as a separate article under the title *Algebraic $\mathbb{Z}^d$-actions on zero-dimensional compact abelian groups.*

2. Continuous $\mathbb{Z}^d$-actions

Let Y be a be a compact metrizable space, and let $d \geq 1$. A *continuous $\mathbb{Z}^d$-action* T on Y is a homomomorphism $\mathbf{n} \mapsto T^{\mathbf{n}}$ from $\mathbb{Z}^d$ into the group of homeomorphisms of Y. In classical ergodic theory d is usually equal to 1, i.e. T is determined by the powers of a single homeomorphism $T^1 = V$ of Y, but in these notes we concentrate on the case where $d > 1$ and on some of the phenomena specific to such higher-rank actions.

We fix a continuous $\mathbb{Z}^d$-action T on a compact metric space (Y, δ).

A point $y \in Y$ is *periodic* if its orbit $\{T^{\mathbf{n}} : \mathbf{n} \in \mathbb{Z}^d\}$ is finite.

The action T is *topologically transitive* if there exists a point $y \in Y$ with dense orbit.

The action T is *topologically mixing* if, for every pair of nonempty open sets $\mathcal{O}_1, \mathcal{O}_2$ in Y, $\mathcal{O}_1 \cap T^{-\mathbf{n}}\mathcal{O}_2 \neq \varnothing$ for all but finitely many $\mathbf{n} \in \mathbb{Z}^d$.

Finally, T is *expansive* if

$$\varepsilon_T = \inf_{\substack{y,y' \in Y \\ y \neq y'}} \sup_{\mathbf{m} \in \mathbb{Z}^d} \delta(T^{\mathbf{m}}y, T^{\mathbf{m}}y') > 0.$$

The number ε_T is called the *expansive constant* of T. Since Y is compact, expansiveness is independent of the particular choice of the metric δ, but the expansive constant obviously depends on δ.

If T and T' are continuous $\mathbb{Z}^d$-actions on compact metrizable spaces Y and Y', respectively, then T' is a *topological factor* of T (or, to be pedantic, (Y', T') is a *topological factor* of (Y, T)) if there exists a continuous surjective map $\phi \colon Y \longrightarrow Y'$ with

$$\phi \circ T^{\mathbf{m}} = T'^{\mathbf{m}} \circ \phi \tag{2.1}$$

for every $\mathbf{m} \in \mathbb{Z}^d$. If the map ϕ in (2.1) can be chosen to be a homeomorphism then T and T' (or (Y, T) and (Y', T')) are *topologically conjugate*. The map ϕ in (2.1) is called a (*topological*) *factor map* (or *conjugacy*). More generally, a not necessarily surjective map $\phi \colon X \longrightarrow Y$ is *equivariant* if it satisfies (2.1) for every $\mathbf{n} \in \mathbb{Z}^d$.

If μ (resp. μ') are Borel probability measures on Y(resp. Y') which are invariant under T (resp. T'), then (Y', T', μ') is a *measurable factor* of (Y, T, μ) if there exists a surjective Borel map $\phi \colon Y \longrightarrow Y'$ with $\mu\phi^{-1} = \mu'$ satisfying (2.1) μ-a.e. for every $\mathbf{m} \in \mathbb{Z}^d$. If this Borel map $\phi \colon Y \longrightarrow Y'$ can be chosen to be bijective then (Y,T,μ) and (Y',T',μ') are *measurably conjugate*. The definition of a measurable equivariant map $\phi\colon Y \longrightarrow Y'$ is analogous.

For the following discussion we assume that T is a continuous $\mathbb{Z}^d$-action on a compact metric space (Y,δ). If $\mathcal{U}$ is an open cover of Y we set $N(\mathcal{U})$ equal to the number of elements in the smallest subcover of $\mathcal{U}$. Then $\log N(\mathcal{U})$ is subadditive in the sense that $\log N(\mathcal{U}\vee\mathcal{V}) \le \log N(\mathcal{U}) + \log N(\mathcal{V})$ for all open covers $\mathcal{U},\mathcal{V}$ of Y, where $\mathcal{U}\vee\mathcal{V}$ is the open cover of Y consisting of all intersections $U\cap V$ with $U\in\mathcal{U}$ and $V\in\mathcal{V}$. For every rectangle $Q=\prod_{j=1}^d\{b_j,\dots,b_j+l_j-1\}\subset\mathbb{Z}^d$ we set $\langle Q\rangle = \min_{j=1,\dots,d} l_j$, and $|Q|$ is (as usual) the cardinality of Q. Put

$$h_{\mathrm{cover}}(T) = \sup_{\mathcal{U}} h(T,\mathcal{U}), \tag{2.2}$$

where $\mathcal{U}$ ranges over the collection of all open covers of Y, and

$$h(T,\mathcal{U}) = \lim_{\langle Q\rangle\to\infty} \frac{1}{|Q|}\log N\biggl(\bigvee_{\mathbf{m}\in Q} T^{-\mathbf{m}}(\mathcal{U})\biggr). \tag{2.3}$$

The limit in (2.3) exists by subadditivity and is less than or equal to $N(\mathcal{U})$.

If $Q\subset\mathbb{Z}^d$ is a rectangle then a set $E\subset Y$ is (Q,δ,ε)-*spanning* for T if there exists, for every $y\in Y$, a $y'\in E$ with $\delta(T^{\mathbf{m}}y,T^{\mathbf{m}}y')<\varepsilon$ for all $\mathbf{m}\in Q$, and E is (Q,δ,ε)-*separated* if there exists, for every pair $y\ne y'$ in E, an $\mathbf{m}\in Q$ with $\delta(T^{\mathbf{m}}y,T^{\mathbf{m}}y')\ge\varepsilon$. Let $r_Q(\delta,\varepsilon)$ be the smallest cardinality of a (Q,δ,ε)-spanning set, $s_Q(\delta,\varepsilon)$ the largest cardinality of a (Q,δ,ε)-separated set, and put

$$\begin{aligned} h_{\mathrm{span}}(T) &= \lim_{\varepsilon\to 0}\limsup_{\langle Q\rangle\to\infty}\frac{1}{|Q|}\log r_Q(\delta,\varepsilon),\\ h_{\mathrm{sep}}(T) &= \lim_{\varepsilon\to 0}\limsup_{\langle Q\rangle\to\infty}\frac{1}{|Q|}\log s_Q(\delta,\varepsilon). \end{aligned} \tag{2.4}$$

Definition 2.1. If T is a continuous $\mathbb{Z}^d$-action on a compact metric space (Y,δ), then

$$\begin{aligned} h_{\mathrm{cover}}(T) = h_{\mathrm{span}}(T) = h_{\mathrm{sep}}(T) &= \lim_{\varepsilon\to 0}\liminf_{\langle Q\rangle\to\infty}\frac{1}{|Q|}\log r_Q(\delta,\varepsilon)\\ &= \lim_{\varepsilon\to 0}\liminf_{\langle Q\rangle\to\infty}\frac{1}{|Q|}\log s_Q(\delta,\varepsilon), \end{aligned} \tag{2.5}$$

and this common value (which is independent of the metric δ) is the *topological entropy* $h_{\mathrm{top}}(T)$ of T.

Recall that a finite open cover $\mathcal{U}$ of Y is a *topological generator* for a continuous $\mathbb{Z}^d$-action T on Y if, for every map $\mathbf{n}\mapsto U_{\mathbf{n}}$ from $\mathbb{Z}^d$ to $\mathcal{U}$,

$$\biggl|\bigcap_{\mathbf{n}\in\mathbb{Z}^d} T^{-\mathbf{n}}(U_{\mathbf{n}})\biggr| \le 1,$$

where $|E|$ is the cardinality of a set E. If T is a continuous $\mathbb{Z}^d$-action on a compact space Y and $\mathcal{U}$ a topological generator for T, then it is easy to see that

$$h_{\mathrm{top}}(T) = h(T,\mathcal{U}) < \infty. \tag{2.6}$$

From (2.6) it is immediate that every continuous expansive $\mathbb{Z}^d$-action T on a compact space Y has finite entropy, since every open cover whose diameter[1] is less than the expansive constant is a topological generator for T.

3. Symbolic $\mathbb{Z}^d$-actions

Let A be a finite set (the *alphabet*), and let $A^{\mathbb{Z}^d}$ be the set of all maps $x\colon \mathbb{Z}^d \longrightarrow A$. For every nonempty subset $F \subset \mathbb{Z}^d$ we write

$$\pi_F\colon A^{\mathbb{Z}^d} \longrightarrow A^F$$

for the projection which restricts each $x \in A^{\mathbb{Z}^d}$ to F. For every $\mathbf{n} \in \mathbb{Z}^d$ we define a homeomorphism $\sigma^{\mathbf{n}}$ of the compact space $A^{\mathbb{Z}^d}$ by

$$(\sigma^{\mathbf{n}} x)_{\mathbf{m}} = x_{\mathbf{n}+\mathbf{m}} \tag{3.1}$$

for every $x = (x_{\mathbf{m}}) \in A^{\mathbb{Z}^d}$. The map $\sigma\colon \mathbf{n} \mapsto \sigma^{\mathbf{n}}$ is the *shift-action* of $\mathbb{Z}^d$ on $A^{\mathbb{Z}^d}$, and a subset $X \subset A^{\mathbb{Z}^d}$ is *shift-invariant* if $\sigma^{\mathbf{n}}(X) = X$ for all $\mathbf{n} \in \mathbb{Z}^d$. A closed nonempty shift-invariant subset $X \subset A^{\mathbb{Z}^d}$ is a *subshift*, and the restriction of σ to a subshift X is denoted by σ_X, and is obviously expansive.

A closed shift-invariant set $X \subset A^{\mathbb{Z}^d}$ is a *shift of finite type* (*SFT*) if there exist a finite set $F \subset \mathbb{Z}^d$ and a subset $P \subset A^F$ such that

$$X = X_{(F,P)} = \{x \in A^{\mathbb{Z}^d} : \pi_F \circ \sigma^{\mathbf{n}}(x) \in P \text{ for every } \mathbf{n} \in \mathbb{Z}^d\}. \tag{3.2}$$

Proposition 3.1. *Let A be a finite set, $d \geq 1$ and $X \subset A^{\mathbb{Z}^d}$ a closed shift-invariant subset. The following conditions are equivalent.*

1. *There exists a finite set $F \subset \mathbb{Z}^d$ such that*
$$X = \{x \in A^{\mathbb{Z}^d} : \pi_F \circ \sigma^{\mathbf{n}}(x) \in \pi_F(X) \text{ for every } \mathbf{n} \in \mathbb{Z}^d\}; \tag{3.3}$$
2. *For every nonincreasing sequence $X_1 \supset X_2 \supset X_3 \supset \cdots$ of subshifts of $A^{\mathbb{Z}^d}$ with $\bigcap_{n\geq 1} X_n = X$ there exists an $N \geq 1$ with $X_N = X$;*
3. *X is a* SFT.

If A and B are finite sets and $X \subset A^{\mathbb{Z}^d}$ and $Y \subset B^{\mathbb{Z}^d}$ are subshifts such that the shift-actions σ_X and σ_Y are topologically conjugate, then X is a SFT *if and only if Y is a* SFT.

[1] If δ is a metric on X, the *diameter* of an open cover $\mathcal{U}$ of X is $\sup_{U\in\mathcal{U}} \sup_{x,y\in U} \delta(x,y)$.

Proof. For the implication (1) $\Rightarrow$ (3) it suffices to choose F as in (3.2) and to set $P = \pi_F(X)$. Conversely, if X is a *SFT* with $X = X_{(F,P)}$, then the set F satisfies (3.3).

For every closed shift-invariant subset $X \subset A^{\mathbb{Z}^d}$, the sequence

$$X_n = \{x \in A^{\mathbb{Z}^d} : \pi_{Q(n)} \circ \sigma^{\mathbf{n}}(x) \in \pi_{Q(n)}(X) \text{ for every } \mathbf{n} \in \mathbb{Z}^d\},\ n \geq 1,$$

with $Q(n) = \{-n, \dots, n\}^d \subset \mathbb{Z}^d$ is nonincreasing and satisfies that $\bigcap_{n\geq 1} X_n = X$. If X satisfies (2), then $X = X_N$ for some $N \geq 1$, and hence X is a *SFT* by (1). Conversely, if X is a *SFT* we choose $F \subset \mathbb{Z}^d$ as in (3.3). For every nonincreasing sequence (X_n) of subshifts of $A^{\mathbb{Z}^d}$ decreasing to X there exists an N with $\pi_F(X_N) = \pi_F(X)$ and hence with $X_N = X$. This proves the equivalence of (1) and (3).

For the last statement we observe that any topological conjugacy $\phi\colon X \longrightarrow Y$ is a *block map*: there exist positive integers $N_1, N_2 \subset \mathbb{Z}^d$ such that $\phi(x)_{\mathbf{0}}$ is completely determined by $\pi_{Q(N_1)}(x)$ and $\phi^{-1}(y)_{\mathbf{0}}$ is completely determined by $\pi_{Q(N_2)}(y)$. Hence $\pi_{Q(n)}(\phi(x))$ is completely determined by $\pi_{Q(n+N_1)}(x)$ and $\pi_{Q(n)}(\phi^{-1}(y))$ is completely determined by $\pi_{Q(n+N_2)}(y)$ for every $n \geq 0$.

Suppose that X is a *SFT*. We set $\psi = \phi^{-1}$ and conclude that

$$\pi_{Q(n)}(\phi(\pi_{Q(n+N_1)}(\psi(\pi_{Q(n+N_1+N_2)}(y))))) = \pi_{Q(n)}(y) \tag{3.4}$$

for every $y \in Y$ and $n \geq 0$, where we are abusing notation atrociously. For every $n \geq 0$ we set

$$Y_n = \{y \in B^{\mathbb{Z}^d} : \pi_{Q(n)} \circ \sigma^{\mathbf{n}}(y) \in \pi_{Q(n)}(Y) \text{ for every } \mathbf{n} \in \mathbb{Z}^d\}.$$

The discussion above shows that ψ extends to a well-defined shift-equivariant map $\bar{\psi}\colon Y_{N_2} \longrightarrow A^{\mathbb{Z}^d}$ with $\bar{\psi}(Y_{N_2}) \supset X$. As X is a *SFT*, there exists an $N \geq N_2$ with $\bar{\psi}(Y_n) = X$ for every $n \geq N$. If $\bar{\psi}$ is injective on Y_n for some $n \geq N$, then $Y_n = Y$ und Y is a *SFT* by (1). Arguing by contradiction, we assume that $\bar{\psi}$ is noninjective on every Y_n, $n \geq N$. Then there exist, for every such n, points $y, y' \in Y_n$ with $y_{\mathbf{0}} \neq y'_{\mathbf{0}}$, but $\bar{\psi}(y) = \bar{\psi}(y')$. By choosing $n \geq N_1 + N_2$ we obtain a contradiction to (3.4). This completes the proof of the last assertion. □

If $X \subset A^{\mathbb{Z}^d}$ is a *SFT* we may change the alphabet A, if necessary, and assume that

$$F = F_0 = \{0,1\}^d. \tag{3.5}$$

In order to verify this we assume that $X = X_{(F,P)} \subset A^{\mathbb{Z}^d}$ with $P \subset A^F$ and $F \subset Q(m) = \{-m, \dots, m\}^d$ for some $m \geq 1$, and set $Q' = \{-m, \dots, m-1\}^d$, $A' = \pi_{Q'}(X) \subset A^{Q'}$ and define a continuous injective map $\phi\colon X \longrightarrow A'^{\mathbb{Z}^d}$ by

$$\phi(x)_{\mathbf{n}} = \pi_{Q'}(\sigma_X^{\mathbf{n}} x)$$

for every $x \in X$ and $\mathbf{n} \in \mathbb{Z}^d$. Clearly, $Y = \phi(X)$ satisfies (3.3) with $F = F_0$ and $\phi \circ \sigma_X = \sigma_Y \circ \phi$.

Unfortunately it is usually quite difficult (and, in general, undecidable) to determine even the most elementary properties of $X_{(F,P)}$ from the initial data (F, P). The most notorious of these difficulties is the following: there is no algorithm which determines, given a finite alphabet A, a nonempty finite set $F \subset \mathbb{Z}^d$ and a nonempty set $P \subset A^F$, whether the space $X_{(F,P)}$ in (3.2) is nonempty or not ([2], [36], [49]).

This undecidability problem is closely related to the existence of nonempty shifts of finite type $X_{(F,P)}$ without periodic points. Suppose for simplicity that $d = 2$, $F = F_0 = \{0, 1\}^2 \subset \mathbb{Z}^2$ and $P \subset A^F$. If every nonempty shift of finite type contained a periodic point, we would have the following algorithm for deciding whether $X_{(F,P)}$ is nonempty: for every $n \geq 1$, consider the set of allowed configurations[2] $P_n \subset A^{Q(n)}$, where $Q(n) = \{-n, \dots, n\}^2 \subset \mathbb{Z}^2$. Then we can find an $n \geq 1$ for which exactly one of the following possibilities holds: either there exists an allowed configuration $y \in P_n$ which is periodic (in the sense that the restrictions of y to the left and right (resp. top and bottom) edges of $Q(n)$ match), or $P_n = \varnothing$. In the former case $X_{(F,P)} \neq \varnothing$, and in the latter case $X_{(F,P)} = \varnothing$.

For concrete examples of higher-dimensional shifts of finite type (e.g. for those arising in statistical mechanics) it is usually easy to check that the space is nonempty. However, the undecidability problem mentioned above is an indication of the difficulty of obtaining general mathematical statements about higher-dimensional Markov systems and shifts of finite type. We end this discussion with a few classical examples of *SFT*'s and some open problems attached to them.

Examples 3.2. (1) *The golden mean shift.* The d-dimensional golden mean (called the d-dimensional *hard core model* in [7]) is the subshift $X \subset \{0, 1\}^{\mathbb{Z}^d}$ consisting of all configurations in which the 1's are isolated. In other words, X is the set of points $x = (x_{\mathbf{n}}) \in \{0, 1\}^{\mathbb{Z}^d}$ with $x_{\mathbf{n} \pm \mathbf{e}^{(i)}} = 0$ for $i = 1, \dots, d$ whenever $x_{\mathbf{n}} = 1$, where $\mathbf{e}^{(i)}$ is the i-th unit vector in $\mathbb{Z}^d$. It is easy to see that σ_X is topologically mixing. Although the value of the topological entropy $h_{\mathrm{top}}(\sigma_X)$ of σ_X can be determined up to arbitrary precision, there is no explicit expression for it (cf. e.g. [29]–[30]).

There are many interesting variations of this example in the literature. Consider, for example, the subshift $X \subset \{-1, 0, 1\}^{\mathbb{Z}^d}$ consisting of all configurations in which no 1 is adjacent to a -1 (but without any other adjacency restrictions). According to [7], the shift-action σ_X has a unique measure of

[2] An element $y = (y_{k,l},\ -n \leq k, l \leq n) \in A^{Q(n)}$ is *allowed* if $(y_{k,l}, y_{k+1,l}, y_{k,l+1}, y_{k+1,l+1}) \in P$ for every $(k, l) \in \{-n, \dots, n-1\}^2$.

maximal entropy (i.e. a shift-invariant probability measure whose entropy is equal to the topological entropy of σ_X). However, if we replace the alphabet $A = \{-1, 0, 1\}$ by $A' = \{-N, \dots, -1, 0, 1, \dots, N\}$ and denote by $X' \subset A'^{\mathbb{Z}^2}$ the set of all configurations in which no positive symbol $1, \dots, N$ is adjacent to a negative symbol $-1, \dots, -N$, and if N is large enough, then $\sigma_{X'}$ is thought to have exactly two invariant probability measures of maximal entropy (cf. [7], where this property is verified for a very similar example).

(2) *Chess boards.* Let $n \geq 3$ and $d \geq 2$, and let $X^{(n,d)}$ be the set of all colourings of the lattice $\mathbb{Z}^d$ with n colours $\{0, \dots, n-1\}$ so that no two adjacent lattice points have the same colour. For $d = 2$, the space $X^{(n,2)}$ can be described as the set of all colourings of an infinite chessboard with n colours in which adjacent squares are coloured differently (cf. [1], [25]). Again one can prove without much difficulty that $\sigma_{X^{(n,d)}}$ is topologically mixing for every $n \geq 3$ and $d \geq 2$. The topological entropy of $\sigma_{X^{(3,2)}}$ was calculated by Lieb in [25]: $h(\sigma_{X^{(3,2)}}) = \frac{1}{2} \cdot \log \frac{64}{27}$. For $n \geq 4$ no explicit expression exists for $h_{\mathrm{top}}(\sigma_{X^{(n,2)}})$; the same is true for $h_{\mathrm{top}}(\sigma_{X^{(n,d)}})$ with $n, d \geq 3$.

(3) *Dimers on a lattice.* Let $A = \{0, 1, 2, 3\}$, and let $X = X_{(F,P)} \subset A^{\mathbb{Z}^2}$ be defined by

$$F = \left\{ \begin{smallmatrix} (0,1) & \\ (0,0) & (1,0) \end{smallmatrix} \right\} \subset \mathbb{Z}^2$$

$$P = \{ \{ \begin{smallmatrix} \text{not}\,3 & \\ 0 & 2 \end{smallmatrix} \}, \{ \begin{smallmatrix} 3 & \\ 1 & \text{not}\,2 \end{smallmatrix} \}, \{ \begin{smallmatrix} \text{not}\,3 & \\ 2 & \text{not}\,2 \end{smallmatrix} \}, \{ \begin{smallmatrix} \text{not}\,3 & \\ 3 & \text{not}\,2 \end{smallmatrix} \}, \}$$

where 'not j' has the obvious meaning that we can put any symbol $i \neq j$ in this location. The space $X = X_{(F,P)}$ is discussed in detail in [17] and [47]: it is isomorphic to the set of all coverings of $\mathbb{Z}^2$ by *dimers*, where each dimer covers exactly two horizontally or vertically adjacent lattice points; the isomorphism is given by interpreting 0 and 2 as the left and right endpoints of a horizontal dimer, and 1 and 3 as the bottom and top endpoints of a vertical dimer. Again it is not too difficult to see that the shift-action σ_X of $\mathbb{Z}^2$ on X is mixing. The topological entropy of σ_X is given by

$$\begin{aligned} h(\sigma_X) &= \frac{1}{4} \cdot \int_0^1 \int_0^1 \log \left(4 - e^{2\pi i s} - e^{-2\pi i s} - e^{2\pi i t} - e^{-2\pi i t}\right) ds\, dt \\ &= \lim_{k,l \to \infty} \frac{1}{kl} \cdot \log \left|\{x \in X : \sigma^{(k,0)} x = x \text{ and } \sigma^{(0,l)} x = x\}\right|, \end{aligned} \tag{3.6}$$

where the first identity in (3.6) was proved in [6] and the second in [17].

(4) *Zero entropy.* Here are two examples of *SFT*'s with zero entropy.

(a) Let $A = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$, $F \subset \mathbb{Z}^2$ a nonempty finite set, and let $P \subset A^F$ be the set of all configurations containing an even number of '1'-s. The shift space $X = X_{(F,P)} \subset (\mathbb{Z}/2\mathbb{Z})^{\mathbb{Z}^2}$ is, in fact, a subgroup, which makes life easier in many ways. For example, there is a distinguished shift-invariant probability measure on X (the normalized Haar measure λ_X), and many dynamical properties of σ_X can be determined via harmonic analysis. For details and generalizations of this example we refer to Section 4.

(b) Let A be a finite set, and let $Y = A^{\mathbb{Z}}$ be the full shift with alphabet A. For every continuous, surjective and shift-commuting map $\phi\colon Y \longrightarrow Y$ we consider the closed shift-invariant subset $X = \{(y^{(k)}) \in Y^{\mathbb{Z}} : y^{(k+1)} = \phi(y^{(k)})\}$ of $Y^{\mathbb{Z}}$ and view X as a closed shift-invariant subset of $A^{\mathbb{Z}^2}$ in the obvious manner. It is clear that X is a *SFT*; such examples are sometimes called *cellular automata* (cf. [15]). The entropy of the horizontal shift $\sigma^{(1,0)}$ is obviously equal to $\log |A|$, but determining the entropy and various other dynamical properties of $\sigma^{(0,1)}$ is an algorithmically undecidable problem (cf. [16], [33]). Note that Example (a) is a cellular automaton in this sense (but here one sees easily that $h(\sigma^{(0,1)}) = \log 2$).

Many further examples of *SFT*'s can be found in [6], [7], [29], [30], [40] and [43].

4. Algebraic $\mathbb{Z}^d$-actions

Whereas even apparently elementary questions about shifts of finite type quickly lead into very deep water, there is a class of $\mathbb{Z}^d$-actions with a variety of interesting properties which can be analyzed quite successfully with tools from algebra, harmonic analysis and, of course, from dynamical systems: the algebraic $\mathbb{Z}^d$-actions.

An *algebraic* $\mathbb{Z}^d$*-action* is an action $\alpha\colon \mathbf{n} \mapsto \alpha^{\mathbf{n}}$ of $\mathbb{Z}^d$, $d \geq 1$, by continuous automorphisms of a compact abelian group X with Borel field $\mathcal{B}_X$ and normalized Haar measure λ_X. Two algebraic $\mathbb{Z}^d$-actions α and β on compact abelian groups X and Y are *algebraically conjugate* if there exists a continuous group isomorphism $\phi\colon X \longrightarrow Y$ with

$$\phi \cdot \alpha^{\mathbf{n}} = \beta^{\mathbf{n}} \cdot \phi \tag{4.1}$$

for every $\mathbf{n} \in \mathbb{Z}^d$. *Measurable conjugacy, factor maps* and *equivariance* will always be understood with respect to Haar measure.

In [20] and [41], Pontryagin duality was shown to imply a one-to-one correspondence between algebraic $\mathbb{Z}^d$-actions (up to algebraic conjugacy) and modules over the ring of Laurent polynomials $R_d = \mathbb{Z}[u_1^{\pm 1}, \dots, u_d^{\pm 1}]$ with integral coefficients in the commuting variables $u_1, \dots, u_d$ (up to module isomorphism). In order to explain this correspondence we write a typical element $f \in R_d$ as

$$f = \sum_{\mathbf{m} \in \mathbb{Z}^d} f_{\mathbf{m}} u^{\mathbf{m}} \tag{4.2}$$

with $u^{\mathbf{m}} = u_1^{m_1} \cdots u_d^{m_d}$ and $f_{\mathbf{m}} \in \mathbb{Z}$ for every $\mathbf{m} = (m_1, \dots, m_d) \in \mathbb{Z}^d$, where $f_{\mathbf{m}} = 0$ for all but finitely many $\mathbf{m}$. If α is an algebraic $\mathbb{Z}^d$-action on a compact abelian group X, then the additively-written dual group $M = \widehat{X}$ is a module over the ring R_d with operation

$$f \cdot a = \sum_{\mathbf{m} \in \mathbb{Z}^d} f_{\mathbf{m}} \widehat{\alpha^{\mathbf{m}}}(a) \tag{4.3}$$

for $f \in R_d$ and $a \in M$, where $\widehat{\alpha^{\mathbf{m}}}$ is the automorphism of $M = \widehat{X}$ dual to $\alpha^{\mathbf{m}}$. In particular,

$$u^{\mathbf{m}} \cdot a = \widehat{\alpha^{\mathbf{m}}}(a) \tag{4.4}$$

for $\mathbf{m} \in \mathbb{Z}^d$ and $a \in M$. This module $M = \widehat{X}$ is called the *dual module* of α. Note that, for every $f \in R_d$, the group homomorphism

$$f(\alpha) = \sum_{\mathbf{n} \in \mathbb{Z}^d} f_{\mathbf{n}} \alpha^{\mathbf{n}} \colon X \longrightarrow X \tag{4.5}$$

is dual to multiplication by f on $M = \widehat{X}$ (or, equivalently, that $\widehat{f(\alpha)}a = f \cdot a$ in (4.3)). In particular, $f(\alpha)$ is surjective if and only if f does not lie in any prime ideal associated[3] with M.

Conversely, any R_d-module M determines an algebraic $\mathbb{Z}^d$-action α_M on the compact abelian group $X_M = \widehat{M}$ with $\alpha_M^{\mathbf{m}}$ dual to multiplication by $u^{\mathbf{m}}$ on M for every $\mathbf{m} \in \mathbb{Z}^d$ (cf. (4.4)). Note that X_M is metrizable if and only if the dual module M of α_M is countable.

Examples 4.1. (1) Let $M = R_d$. Since R_d is isomorphic to the direct sum $\sum_{\mathbb{Z}^d} \mathbb{Z}$ of copies of $\mathbb{Z}$, indexed by $\mathbb{Z}^d$, the dual group $X = \widehat{R_d}$ is isomorphic to the Cartesian product $\mathbb{T}^{\mathbb{Z}^d}$ of copies of $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. We write a typical element $x \in \mathbb{T}^{\mathbb{Z}^d}$ as $x = (x_{\mathbf{n}})$ with $x_{\mathbf{n}} \in \mathbb{T}$ for every $\mathbf{n} \in \mathbb{Z}^d$ and choose the following identification of $X_{R_d} = \widehat{R_d}$ and $\mathbb{T}^{\mathbb{Z}^d}$: for every $x \in \mathbb{T}^{\mathbb{Z}^d}$ and $f \in R_d$,

$$\langle x, f \rangle = e^{2\pi i \sum_{\mathbf{n} \in \mathbb{Z}^d} f_{\mathbf{n}} x_{\mathbf{n}}},$$

where f is given by (4.2). Under this identification the $\mathbb{Z}^d$-action α_{R_d} on $X_{R_d} = \mathbb{T}^{\mathbb{Z}^d}$ becomes the shift-action

$$(\alpha_{R_d}^{\mathbf{m}} x)_{\mathbf{n}} = x_{\mathbf{m}+\mathbf{n}}. \tag{4.6}$$

---

[3]A prime ideal $\mathfrak{p} \subset R_d$ is *associated with* an R_d-module M if

$$\mathfrak{p} = \operatorname{ann}(a) = \{f \in R_d : f \cdot a = 0_M\}$$

for some $a \in M$. The set of all prime ideals associated with M is denoted by $\operatorname{asc}(M)$ and satisfies that

$$\bigcup_{\mathfrak{p} \in \operatorname{asc}(M)} \mathfrak{p} = \bigcup_{0 \neq a \in M} \operatorname{ann}(a).$$

If M is Noetherian, then $\operatorname{asc}(M)$ is finite. For details see [23].

(2) Let $I \subset R_d$ be an ideal and $M = R_d/I$. Since M is a quotient of the additive group R_d by an $\widehat{\alpha_{R_d}}$-invariant subgroup (i.e. by a submodule), the dual group $X_M = \widehat{M}$ is the closed α_{R_d}-invariant subgroup

$$\begin{aligned} X_{R_d/I} &= \{x \in X_{R_d} = \mathbb{T}^{\mathbb{Z}^d} : \langle x, f\rangle = 1 \text{ for every } f \in I\} \\ &= \Bigl\{x \in \mathbb{T}^{\mathbb{Z}^d} : \sum_{\mathbf{n}\in\mathbb{Z}^d} f_{\mathbf{n}} x_{\mathbf{m}+\mathbf{n}} = 0 \pmod 1 \\ &\qquad\qquad \text{for every } f \in I \text{ and } \mathbf{m} \in \mathbb{Z}^d\Bigr\} \\ &= \bigcap_{f\in I} \ker f(\alpha_{R_d}) = \bigcap_{i=1}^{m} \ker f_i(\alpha_{R_d}), \end{aligned} \tag{4.7}$$

where $f_1, \dots, f_m$ is a set of generators of I, $f(\alpha_{R_d})$ is defined by (4.5) for every $f \in I$, and $\alpha_{R_d/I}$ is the restriction of the shift-action α_{R_d} in (4.6) to the shift-invariant subgroup $X_{R_d/I} \subset \mathbb{T}^{\mathbb{Z}^d}$.

Conversely, let $X \subset \mathbb{T}^{\mathbb{Z}^d} = \widehat{R_d}$ be a closed subgroup, and let

$$X^{\perp} = \{f \in R_d : \langle x, f\rangle = 1 \text{ for every } x \in X\}$$

be the annihilator of X in $\widehat{R_d}$. Then X is shift-invariant if and only if $X^{\perp}$ is an ideal in R_d.

Remark 4.2. Equation (4.7) shows that $X_{R_d/I} \subset \mathbb{T}^{\mathbb{Z}^d}$ is a shift of finite type of the form (3.2), albeit with uncountable alphabet $\mathbb{T}$. It is interesting to note that $X_{R_d/I}$ also satisfies the descending chain condition of Proposition 3.1 (2), and that this property is equivalent to the Noetherian property of the ring R_d. More generally, if α is an algebraic $\mathbb{Z}^d$-action on a compact abelian group X with dual module M, then M is Noetherian if and only if every nonincreasing sequence $X_1 \supset X_2 \supset X_3 \supset \cdots$ of closed α-invariant subgroups of X is eventually constant. For a more detailed discussion of these matters we refer to [42].

The correspondence between algebraic $\mathbb{Z}^d$-actions $\alpha = \alpha_M$ and R_d-modules M yields a correspondence (or 'dictionary') between dynamical properties of α_M and algebraic properties of the module M (cf. [42]). It turns out that some of the principal dynamical properties of α_M can be expressed entirely in terms of the prime ideals associated with the module M (cf. Footnote 3 on the preceding page).

Table 1 provides a small illustration of this correspondence; all the relevant results can be found in [42]. In the third column we assume that the R_d-module $M = \widehat{X}$ defining α is of the form $R_d/\mathfrak{p}$, where $\mathfrak{p} \subset R_d$ is a prime ideal, and describe the algebraic condition on $\mathfrak{p}$ equivalent to the dynamical condition on $\alpha = \alpha_{R_d/\mathfrak{p}}$ appearing in the second column. In the fourth column we consider a countable R_d-module M and state the algebraic property of M corresponding to the property of $\alpha = \alpha_M$ in the second column.

	Property of α	$\alpha = \alpha_{R_d/\mathfrak{p}}$	$\alpha = \alpha_M$
(1)	α is expansive	$V_{\mathbb{C}}(\mathfrak{p}) \cap \mathbb{S}^d = \varnothing$	M is Noetherian and $\alpha_{R_d/\mathfrak{p}}$ is expansive for every $\mathfrak{p} \in \operatorname{asc}(M)$
(2)	$\alpha^{\mathbf{n}}$ is ergodic for some $\mathbf{n} \in \mathbb{Z}^d$	$u^{k\mathbf{n}} - 1 \notin\subset \mathfrak{p}$ for every $k \geq 1$	$\alpha^{\mathbf{n}}_{R_d/\mathfrak{p}}$ is ergodic for every $\mathfrak{p} \in \operatorname{asc}(M)$
(3)	α is ergodic	$\{u^{k\mathbf{n}} - 1 : \mathbf{n} \in \mathbb{Z}^d\} \not\subset \mathfrak{p}$ for every $k \geq 1$	$\alpha_{R_d/\mathfrak{p}}$ is ergodic for every $\mathfrak{p} \in \operatorname{asc}(M)$
(4)	α is mixing	$u^{\mathbf{n}} - 1 \notin \mathfrak{p}$ for every non-zero $\mathbf{n} \in \mathbb{Z}^d$	$\alpha_{R_d/\mathfrak{p}}$ is mixing for every $\mathfrak{p} \in \operatorname{asc}(M)$
(5)	α is mixing of every order	Either $\mathfrak{p}$ is equal to pR_d for some rational prime p, or $\mathfrak{p} \cap \mathbb{Z} = \{0\}$ and $\alpha_{R_d/\mathfrak{p}}$ is mixing	For every $\mathfrak{p} \in \operatorname{asc}(M)$, $\alpha_{R_d/\mathfrak{p}}$ is mixing of every order
(6)	$h(\alpha) > 0$	$\mathfrak{p}$ is principal and $\alpha_{R_d/\mathfrak{p}}$ is mixing	$h(\alpha_{R_d/\mathfrak{p}}) > 0$ for at least one $\mathfrak{p} \in \operatorname{asc}(M)$
(7)	$h(\alpha) < \infty$	$\mathfrak{p} \neq \{0\}$	If M is Noetherian: $\mathfrak{p} \neq \{0\}$ for every $\mathfrak{p} \in \operatorname{asc}(M)$
(8)	α has completely positive entropy (or is Bernoulli)	$h(\alpha^{R_d/\mathfrak{p}}) > 0$	$h(\alpha_{R_d/\mathfrak{p}}) > 0$ for every $\mathfrak{p} \in \operatorname{asc}(M)$

TABLE 1. A Pocket Dictionary

The notation in Table 1 is as follows. In (1),

$$V_{\mathbb{C}}(\mathfrak{p}) = \{c \in (\mathbb{C} \smallsetminus \{0\})^d : f(c) = 0 \text{ for every } f \in \mathfrak{p}\}$$

is the *variety* of $\mathfrak{p}$, and $\mathbb{S} = \{c \in \mathbb{C} : |c| = 1\}$. From (2)–(4) it is clear that α is ergodic if and only if $\alpha^{\mathbf{n}}$ is ergodic for *some* $\mathbf{n} \in \mathbb{Z}^d$, and that α is mixing if and only if $\alpha^{\mathbf{n}}$ is ergodic for *every nonzero* $\mathbf{n} \in \mathbb{Z}^d$. In (5), α is mixing of order $r \geq 2$ if

$$\lim_{\substack{\mathbf{n}_1,\dots,\mathbf{n}_r \in \mathbb{Z}^d \\ \|\mathbf{n}_i - \mathbf{n}_j\| \to \infty \text{ for } 1 \leq i < j \leq d}} \lambda_X\Bigl(\bigcap_{i=1}^r \alpha^{-\mathbf{n}_i} B_i\Bigr) = \prod_{i=1}^r \lambda_X(B_i) \tag{4.8}$$

for all Borel sets $B_i \subset X$, $i = 1, \dots, r$. In (6)–(8), $h(\alpha) = h_{\mathrm{top}}(\alpha)$ stands for the topological entropy of α (which coincides with the metric entropy $h_{\lambda_X}(\alpha)$). In [27] and [42] there is an explicit entropy formula for algebraic $\mathbb{Z}^d$-actions: in the special case where $\alpha = \alpha_{R_d/\mathfrak{p}}$ for some prime ideal $\mathfrak{p} \subset R_d$ this formula reduces to

$$h(\alpha) = \begin{cases} |\log \mathsf{M}(f)| & \text{if } \mathfrak{p} = (f) = fR_d \text{ is principal,} \\ 0 & \text{otherwise,} \end{cases}$$

where

$$\mathsf{M}(f) = \begin{cases} \exp\bigl(\int_{\mathbb{S}^d} \log |f(\mathbf{s})| \, d\mathbf{s}\bigr) & \text{if } f \neq 0, \\ 0 & \text{if } f = 0, \end{cases}$$

is the *Mahler measure* of the polynomial f. Here $d\mathbf{s}$ denotes integration with respect to the normalized Haar measure on the multiplicative subgroup $\mathbb{S}^d \subset \mathbb{C}^d$. Furthermore, $h(\alpha) = h_{\lambda_X}(\alpha)$, and if α has completely positive entropy, then the Haar measure is the unique measure of maximal entropy on X.

For background, details and proofs of these and further results we refer to [42] and the original articles cited there. Here we restrict ourselves to a single example.

Example 4.3. Let $d = 2$, and let $f = 4 - u_1 - u_2 - u_1^{-1} - u_2^{-1} \in R_2$. Since f is irreducible, the principal ideal $(f) = fR_2 \subset R_2$ is prime, and Table 1 on the page before implies that the $\mathbb{Z}^2$-action $\alpha = \alpha_{R_2/(f)}$ on $X = X_{R_2/(f)} = \widehat{R_2/(f)}$ in (4.7) is mixing, nonexpansive (since $(1,1) \in V_{\mathbb{C}}(f) \cap \mathbb{S}^2$) and has entropy

$$h(\alpha) = \int_0^1 \int_0^1 \log\left(4 - e^{2\pi is} - e^{-2\pi is} - e^{2\pi it} - e^{-2\pi it}\right) ds\, dt.$$

A glance at (3.6) shows that $h(\alpha) = 4h(\sigma_X)$, where σ_X is the dimer shift in Example 3.2 (3). We write $\bar{\sigma}_X \colon \mathbf{n} \mapsto \sigma_X^{2\mathbf{n}}$ for the *even* dimer shift and conclude that $h(\alpha) = h(\bar{\sigma}_X)$. As α and $\bar{\sigma}_X$ are Bernoulli by Table 1 and [6], respectively, these two $\mathbb{Z}^2$-actions are measurably conjugate by [35], but no explicit isomorphism between these actions is known (cf. also [46]).

5. Mixing properties of algebraic $\mathbb{Z}^d$-actions and additive relations in fields

In this section we describe the connection between higher order mixing properties of algebraic $\mathbb{Z}^d$-actions and certain diophantine results on additive relations in fields due to Mahler ([28]), Masser ([31], [21]) and Schlickewei, W. Schmidt and van der Poorten ([13], [48]).

In the discussion below we shall use the following elementary consequence of Pontryagin duality.

Lemma 5.1. *Let α be an algebraic $\mathbb{Z}^d$-action on a compact abelian group X with dual module $M = \widehat{X}$. Then X is connected if and only if* no *prime ideal $\mathfrak{p} \in \operatorname{asc}(M)$ contains a nonzero constant, and X is zero-dimensional if and only if* every *$\mathfrak{p} \in \operatorname{asc}(M)$ contains a nonzero constant.*

Proof. If M contains a nonzero element a of finite order $n \geq 2$, say, then $\langle a, x \rangle$ is an n-th root of unity for every $x \in X$, and the map $x \mapsto \langle a, x \rangle$ sends X to a finite set containing more than one element. Hence X is not connected.

Conversely, suppose that every nonzero element of M has infinite order, and that X is not connected. We fix a metric δ on X and choose two complementary open sets $\mathcal{O}_1, \mathcal{O}_2$ in X. By compactness there exists an $\varepsilon > 0$ such that $x + B_\delta(\varepsilon) \subset \mathcal{O}_i$ for every $x \in \mathcal{O}_i$, $i = 1, 2$, where $B_\delta(\varepsilon) = \{y \in X : \delta(y, 0) < \varepsilon\}$.

Choose an increasing sequence of finitely generated subgroups (A_n) in M with $\bigcup_{n \geq 1} A_n = M$. The annihilators $Y_n = A_n^\perp$ form a decreasing sequence of closed subgroups of X with $\bigcap_{n \geq 1} Y_n = \{0\}$, and hence with $Y_n \subset B_\delta(\varepsilon)$ for all $n \geq n_0$, say. Our choice of ε implies that $x + Y_{n_0} \subset \mathcal{O}_i$ for every $x \in \mathcal{O}_i$, $i = 1, 2$, and hence that the quotient group X/Y_{n_0} is not connected. As $\widehat{X/Y_{n_0}} = A_{n_0}$ is finitely generated and has no nonzero elements of finite order, $A_{n_0} \cong \mathbb{Z}^m$ and $\widehat{A_{n_0}} = X/Y_{n_0} \cong \mathbb{T}^m$ for some $m \geq 1$, which contradicts the diconnectedness of X/Y_{n_0}.

We have established the (well known) fact that X is disconnected if and only if $\widehat{X} = M$ contains an element $a \neq 0$ of finite order. If the latter condition holds we set $N = R_d \cdot a$ and choose a $b \in N$ whose annihilator $\operatorname{ann}(b) = \{f \in R_d : f \cdot b = 0\}$ is maximal (this is possible since the ring R_d is Noetherian). Then $\mathfrak{p} = \operatorname{ann}(b)$ is a prime ideal which is obviously associated with M and contains a nonzero constant by assumption.

Conversely, if some $\mathfrak{p} \in \operatorname{asc}(M)$ contains a nonzero constant, then M obviously contains elements of finite order.

Essentially the same argument as above shows that the following conditions are equivalent:

(i) X is zero-dimensional,
(ii) X contains no nontrivial connected subgroups,
(iii) Every element $a \in M$ has finite order,
(iv) Every prime ideal $\mathfrak{p} \in \operatorname{asc}(M)$ contains a nonzero constant.

This completes the proof of the lemma. □

Let $\mathfrak{p} \subset R_d$ be a prime ideal, and let $\alpha = \alpha_{R_d/\mathfrak{p}}$ be the algebraic $\mathbb{Z}^d$-action with dual module $M = R_d/\mathfrak{p} = \widehat{X}$. If α is not mixing (i.e. mixing of order 2 in the sense of (4.8)), then there exist Borel sets $B_1, B_2 \subset X$ and a sequence $(\mathbf{n}_k,\ k \geq 1)$ in $\mathbb{Z}^d$ with $\lim_{k\to\infty} \mathbf{n}_k = \infty$ and

$$\lim_{k\to\infty} \lambda_X(B_1 \cap \alpha^{-\mathbf{n}_k} B_2) = c$$

for some $c \neq \lambda_X(B_1)\lambda_X(B_2)$. Fourier expansion implies that the latter condition is equivalent to the existence of nonzero elements $a_1, a_2 \in M$ such that

$$a_1 + u^{\mathbf{n}_k} \cdot a_2 = 0$$

for infinitely many $k \geq 1$. In particular,

$$(u^{\mathbf{m}} - 1) \cdot a_2 = 0 \tag{5.1}$$

for some nonzero $\mathbf{m} \in \mathbb{Z}^d$ (cf. Table 1 (4)). A very similar argument shows that α is not mixing of order $r \geq 2$ if and only if there exist elements $a_1, \dots, a_r$ in M, not all equal to zero, and a sequence $((\mathbf{n}_k^{(1)}, \dots, \mathbf{n}_k^{(r)}),\ k \geq 1)$ in $(\mathbb{Z}^d)^r$ with $\lim_{k\to\infty} \|\mathbf{n}_k^{(i)} - \mathbf{n}_k^{(j)}\| = \infty$ for all i, j with $1 \leq i < j \leq r$, such that

$$u^{\mathbf{n}_k^{(1)}} \cdot a_1 + \dots + u^{\mathbf{n}_k^{(r)}} \cdot a_r = 0 \tag{5.2}$$

for every $k \geq 1$.

Below we shall see that higher order mixing of an algebraic $\mathbb{Z}^d$-action α on a compact abelian group X can break down in a particularly regular way (cf. Examples 7.1). We call a nonempty finite subset $S \subset \mathbb{Z}^d$ *mixing* for α if

$$\lim_{k\to\infty} \lambda_X\Bigl(\bigcap_{\mathbf{n}\in S} \alpha^{-k\mathbf{n}} B_{\mathbf{n}}\Bigr) = \prod_{\mathbf{n}\in S} \lambda_X(B_{\mathbf{n}}) \tag{5.3}$$

for all Borel sets $B_{\mathbf{n}} \subset X$, $\mathbf{n} \in S$, and *nonmixing* otherwise. A set $S \subset \mathbb{Z}^d$ is *minimal nonmixing* if it is nonmixing, but every nonempty subset $S' \subsetneq S$ is mixing.

As in (5.2) one sees that a nonempty finite set $S \subset \mathbb{Z}^d$ is nonmixing if and only if there exist elements $a_{\mathbf{n}} \in M$, $\mathbf{n} \in S$, not all equal to zero, such that

$$\sum_{\mathbf{n}\in S} u^{k\mathbf{n}} \cdot a_{\mathbf{n}} = 0 \quad \text{for infinitely many } k \geq 1. \tag{5.4}$$

The next theorem shows that the higher order mixing behaviour of an algebraic $\mathbb{Z}^d$-action α with dual module M is again completely determined by that of the actions $\alpha_{R_d/\mathfrak{p}}$ with $\mathfrak{p} \in \operatorname{asc}(M)$ (cf. Table 1 (4)–(5), [21] and [45]).

Theorem 5.2. *Let α be an algebraic $\mathbb{Z}^d$-action on a compact abelian group X with dual module $M = \widehat{X}$.*

1. *For every $r \geq 2$, the following conditions are equivalent:*
   - (a) *α is r-mixing (i.e. mixing of order r),*
   - (b) *$\alpha_{R_d/\mathfrak{p}}$ is r-mixing for every $\mathfrak{p} \in \operatorname{asc}(M)$.*
2. *For every nonempty finite set $S \subset \mathbb{Z}^d$, the following conditions are equivalent:*
   - (a) *S is α-mixing,*
   - (b) *S is $\alpha_{R_d/\mathfrak{p}}$-mixing for every $\mathfrak{p} \in \operatorname{asc}(M)$.*

For the proof of Theorem 5.2 we have to introduce a little bit of algebraic terminology. Let $\mathfrak{p} \subset R_d$ be a prime ideal. An R_d-module M is *associated with* $\mathfrak{p}$ if $\mathfrak{p}$ is the only prime ideal associated with M (cf. Footnote 3 on page 10). A submodule W of an R_d-module M is $\mathfrak{p}$-*primary* (or $\mathfrak{p}$ *belongs to* W) if M/W is associated with $\mathfrak{p}$. If the module M is Noetherian (which we assume throughout the remainder of this discussion), then the set $\operatorname{asc}(M) =$

$\{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$ of prime ideals associated with M is finite. By [23, Theorem VI.5.3] there exist $\mathfrak{p}_i$-primary submodules $W_i \subset M$, $i = 1, \dots, m$, with the following properties:

(1) The primes $\mathfrak{p}_i$ belonging to the submodules W_i are all distinct;
(2) $W_1 \cap \dots \cap W_m = \{0\}$;
(3) For every subset $S \subsetneq \{1, \dots, m\}$, $\bigcap_{i \in S} W_i \neq \{0\}$.

A family $\{W_1, \dots, W_m\}$ of primary submodules satisfying these conditions is called a *reduced primary decomposition* of M.

If $\mathfrak{q} \subset R_d$ is a prime ideal and W a Noetherian R_d-module associated with $\mathfrak{q}$, then [42, Proposition 6.1] states that there exist integers $1 \leq t \leq s$ and submodules $\{0\} = N_0 \subset \dots \subset N_s = W$ such that, for every $i = 1, \dots, s$, $N_i/N_{i-1} \cong R_d/\mathfrak{q}_i$ for some prime ideal $\mathfrak{q}_i$ containing $\mathfrak{q}$, $\mathfrak{q}_i = \mathfrak{q}$ for $i = 1, \dots, t$, and $\mathfrak{q}_i \supsetneq \mathfrak{q}$ for $i = t+1, \dots, s$.

Proof of Theorem 5.2. Suppose that α is r-mixing. If $\mathfrak{p} \subset R_d$ is a prime ideal associated with M, then $\mathfrak{p} = \operatorname{ann}(a) = \{f \in R_d : f \cdot a = 0\}$ for some $a \in M$, and we set $N = R_d \cdot a \subset M$. Then $N \cong R_d/\mathfrak{p}$ and $Y = \widehat{N} = X/N^{\perp}$. Since N is invariant under the $\mathbb{Z}^d$-action $\hat{\alpha}\colon \mathbf{n} \mapsto \hat{\alpha}^{\mathbf{n}}$ dual to α, $N^{\perp}$ 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 dual module of α_Y is equal to $\widehat{Y} = N \cong R_d/\mathfrak{p}$ we conclude that $\alpha_{R_d/\mathfrak{p}}$ must be r-mixing.

Conversely, if α is not r-mixing, then (5.2) shows that there exist a non-zero element $(a_1, \dots, a_r) \in M^r$ and a sequence $(\mathbf{n}_k = (\mathbf{n}_k^{(1)}, \dots, \mathbf{n}_k^{(r)}), k \geq 1)$ in $(\mathbb{Z}^d)^r$ such that $\mathbf{n}_k^{(1)} = \mathbf{0}$ for every $k \geq 1$, $\lim_{k \to \infty} \mathbf{n}_k^{(j)} - \mathbf{n}_k^{(i)} = \infty$ for $1 \leq i < j \leq r$, and $u^{\mathbf{n}_k^{(1)}} \cdot a_1 + \dots + u^{\mathbf{n}_k^{(r)}} \cdot a_r = 0$ for every $k \geq 1$. There exists a Noetherian submodule $N \subset M$ such that $\{a_1, \dots, a_r\} \subset N$, and (5.2) implies that the $\mathbb{Z}^d$-action α_N, which is a factor of α, is not r-mixing.

Since N is Noetherian, the set of prime ideals associated with N is finite and equal to $\{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$, say, and we choose a corresponding reduced primary decomposition $W_1, \dots, W_m$ of N. The map $a \mapsto (a + W_1, \dots, a + W_m)$ from N into $K = \bigoplus_{i=1}^m N/W_i$ is injective, and the dual homomorphism from $\bar{X} = \widehat{K}$ to $\widehat{N} = X_N$ is surjective. Hence α_N is a factor of α_K, so that α_K cannot be r-mixing. By applying (5.2) to the R_d-module K we see that there exists a $j \in \{1, \dots, m\}$ such that α_{N/W_j} is not r-mixing.

Put $V = N/W_j$, $\mathfrak{p} = \mathfrak{p}_j$, and choose integers $1 \leq t \leq s$ and submodules $V = N_s \supset \dots \supset N_0 = \{0\}$ such that, for every $k = 1, \dots, s$, $N_k/N_{k-1} \cong R_d/\mathfrak{q}_k$ for some prime ideal $\mathfrak{p} \subset \mathfrak{q}_k \subset R_d$, $\mathfrak{q}_k = \mathfrak{p}$ 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 α_V is not r-mixing, (5.2) implies the existence of a non-zero element $(a_1, \dots, a_r) \in V^r$ and a sequence

$(\mathbf{n}^{(k)} = (\mathbf{n}_k^{(1)}, \dots, \mathbf{n}_k^{(r)}),\ k \geq 1)$ in $(\mathbb{Z}^d)^r$ such that $\mathbf{n}_k^{(1)} = \mathbf{0}$ for every $k \geq 1$, $\lim_{k\to\infty} \mathbf{n}_k^{(j)} - \mathbf{n}_k^{(i)} = \infty$ for $1 \leq i < j \leq r$, and $u^{\mathbf{n}_k^{(1)}} \cdot a_1 + \cdots + u^{\mathbf{n}_k^{(r)}} \cdot a_r = 0$ for every $k \geq 1$. Put $b_i = g \cdot a_i$, and note that $0 \neq (b_1, \dots, b_r) \in (N_t)^r$, since $g \cdot a \neq 0$ for every non-zero element $a \in V$. There exists a unique integer $l \in \{1, \dots, t\}$ such that $(b_1, \dots, b_r) \in (N_l)^r \smallsetminus (N_{l-1})^r$, and by setting $b_i' = b_i + N_{l-1} \in N_l/N_{l-1} \cong R_d/\mathfrak{p}$ we obtain that $0 \neq (b_1', \dots, b_r') \in (N_l/N_{l-1})^r \cong (R_d/\mathfrak{p})^r$ and $u^{\mathbf{n}_k^{(1)}} \cdot b_1' + \cdots + u^{\mathbf{n}_k^{(r)}} \cdot b_r' = 0$ for every $k \geq 1$, so that $\alpha_{R_d/\mathfrak{p}}$ is not r-mixing by (5.2). Since the prime ideal $\mathfrak{p}$ is associated with the submodule $N \subset M$, $\mathfrak{p}$ is also associated with M, and (1) is proved. The proof of (2) is identical, except that we use (5.4) instead of (5.2). □

6. Mixing properties of $\mathbb{Z}^d$-actions on connected groups

In order to exhibit the connection between mixing properties and additive relations in fields we begin with a theorem by Mahler.

Theorem 6.1 ([28])**.** *Let K be a field of characteristic 0, $r \geq 2$, and let $x_1, \dots, x_r$ be nonzero elements of K. If we can find nonzero elements $c_1, \dots, c_r$ such that the equation*

$$\sum_{i=1}^{r} c_i x_i^k = 0$$

holds for infinitely many $k \geq 0$, then there exist integers $s \geq 1$ and i, j with $1 \leq i < j \leq r$ such that $x_i^s = x_j^s$.

Theorem 6.1 implies the following statement.

Corollary 6.2 ([39])**.** *Let α be a mixing algebraic $\mathbb{Z}^d$-action on a compact connected abelian group X. Then every nonempty finite subset $S \subset \mathbb{Z}^d$ is mixing.*

Proof of Corollary 6.2*, given Theorem* 6.1. Since X is connected, none of the prime ideals $\mathfrak{p} \in \operatorname{asc}(M)$ contains a nonzero constant by Lemma 5.1. Furthermore, if a nonempty finite $S \subset \mathbb{Z}^d$ is nonmixing for α, then it is also nonmixing for some $\alpha_{R_d/\mathfrak{p}}$, $\mathfrak{p} \in \operatorname{asc}(M)$, by Theorem 5.2. In order to prove Corollary 6.2 it will thus suffice to show that none of the $\mathbb{Z}^d$-actions $\alpha_{R_d/\mathfrak{p}}$, $\mathfrak{p} \in \operatorname{asc}(M)$, has a nonmixing set.

We fix $\mathfrak{p} \in \operatorname{asc}(M)$ and conclude from Table 1 (4) that $u^{\mathbf{n}} - 1 \notin \mathfrak{p}$ for every nonzero $\mathbf{n} \in \mathbb{Z}^d$. If we denote by $K = Q(R_d/\mathfrak{p}) \supset R_d/\mathfrak{p}$ the field of fractions of the integral domain $R_d/\mathfrak{p}$ and set $x_{\mathbf{n}} = u^{\mathbf{n}} + \mathfrak{p} \in K$ for every $\mathbf{n} \in \mathbb{Z}^d$, then our mixing hypothesis implies that the multiplicative group $\{x_{\mathbf{n}} : \mathbf{n} \in \mathbb{Z}^d\} \subset K^\times = K \smallsetminus \{0\}$ is isomorphic to $\mathbb{Z}^d$, i.e. that all the $x_{\mathbf{n}}$, $\mathbf{n} \in \mathbb{Z}^d$, are distinct.

Suppose that a nonempty finite set $S \subset \mathbb{Z}^d$ is $\alpha_{R_d/\mathfrak{p}}$-nonmixing. Equation (5.4) translates into the existence of elements $c_{\mathbf{n}} \in K$, $\mathbf{n} \in S$, not all equal to zero, such that

$$\sum_{\mathbf{n}\in S} c_{\mathbf{n}} x_{\mathbf{n}}^k = 0$$

for infinitely many $k \geq 0$. By Theorem 6.1 there exist distinct elements $\mathbf{m}, \mathbf{n} \in S$ and a positive integer s with $x_{\mathbf{m}}^s = x_{\mathbf{n}}^s$, and hence with $u^{s\mathbf{m}} - u^{s\mathbf{n}} = u^{s\mathbf{n}}(u^{s(\mathbf{m}-\mathbf{n})} - 1) \in \mathfrak{p}$. This violates our earlier assertion that $u^{\mathbf{k}} - 1 \notin \mathfrak{p}$ for every nonzero $\mathbf{k} \in \mathbb{Z}^d$, and the resulting contradiction proves that there are no nonmixing sets for $\alpha_{R_d/\mathfrak{p}}$ and hence for α. □

If an algebraic $\mathbb{Z}^d$-action α is not mixing of every order, then there exists a smallest integer $r \geq 2$ such that α is not r-mixing. As a consequence of Lemma 5.1 and (5.2) one obtains the equivalence of Theorem 6.3 and Corollary 6.4 below.

Theorem 6.3 ([13], [48])**.** *Let K be a field of characteristic* 0 *and G a finitely generated multiplicative subgroup of $K^\times = K \smallsetminus \{0\}$. If $r \geq 2$ and $(c_1, \dots, c_r) \in (K^\times)^r$, then the equation*

$$\sum_{i=1}^{r} c_i x_i = 1 \tag{6.1}$$

has only finitely many solutions $(x_1, \dots, x_r) \in G^r$ such that no sub-sum of (6.1) *vanishes.*

Corollary 6.4 ([45])**.** *Let α be a mixing algebraic $\mathbb{Z}^d$-action on a compact connected abelian group X. Then α is mixing of every order.*

Proof of Corollary 6.4*, given Theorem* 6.3*.* As in the proof of Corollary 6.2 we may assume without loss in generality that $\alpha = \alpha_{R_d/\mathfrak{p}}$ for some prime ideal $\mathfrak{p} \subset R_d$. Using the same notation as in that proof, we denote by $K = Q(R_d/\mathfrak{p})$ the field of fractions of $R_d/\mathfrak{p}$, set $x_{\mathbf{n}} = u^{\mathbf{n}} + \mathfrak{p} \in R_d/\mathfrak{p} \subset K$ for every $\mathbf{n} \in \mathbb{Z}^d$, and observe that the multiplicative subgroup $G = \{x_{\mathbf{n}} : \mathbf{n} \in \mathbb{Z}^d\} \subset K^\times$ is isomorphic to $\mathbb{Z}^d$.

Suppose that α is mixing of order $r \geq 2$, but not of order $r+1$. According to (5.2) there exist elements $a_1, \dots, a_r \in K$, not all equal to zero, and a sequence $((\mathbf{n}_k^{(1)}, \dots, \mathbf{n}_k^{(r)}), k \geq 1)$ in $(\mathbb{Z}^d)^r$ with $\lim_{k\to\infty} \|\mathbf{n}_k^{(i)} - \mathbf{n}_k^{(j)}\| = \infty$ for all i, j with $1 \leq i < j \leq r$, such that

$$\sum_{i=1}^{r} a_i x_{\mathbf{n}_k^{(i)}} = 1$$

for every $k \geq 1$. Our hypothesis that α is r-mixing has two consequences:

(i) each a_i is nonzero,

(ii) for every nonempty subset $F \subsetneq \{1,\dots,r\}$, the set of all $k \geq 1$ with

$$\sum_{i\in F} a_i x_{\mathbf{n}_k^{(i)}} = 0$$

is finite.

After removing finitely many terms from the sequence $((\mathbf{n}_k^{(1)},\dots,\mathbf{n}_k^{(r)}),\ k \geq 1)$, if necessary, we obtain infinitely many distinct solutions $(x_1,\dots,x_r) \in G^r$ of the equation (6.1) without vanishing sub-sums, which contradicts Theorem 6.3. This shows that α has to be mixing of every order. □

The 'absolute' version of the S-unit theorem in [13] contains a bound on the number of solutions of (6.1) without vanishing subsums which is expressed purely in terms of the integer r and the rank of the group G (in our setting: the rank of the group $\mathbb{Z}^d$). This bound implies uniform speed of r-fold mixing for all mixing algebraic $\mathbb{Z}^d$-actions on compact connected abelian groups which are of the form $\alpha = \alpha_{R_d/\mathfrak{p}}$ for some prime ideal $\mathfrak{p} \subset R_d$.

7. Mixing properties of $\mathbb{Z}^d$-actions on totally disconnected groups

For algebraic $\mathbb{Z}^d$-actions on disconnected groups the higher order mixing behaviour is complicated by the possible presence of nonmixing sets.

In the following discussion we assume that $p > 1$ is a rational prime, denote by $R_d^{(p)} = (\mathbb{Z}/p\mathbb{Z})[u_1^{\pm 1},\dots,u_d^{\pm 1}]$ the ring of Laurent polynomials in $u_1,\dots,u_d$ with coefficients in the prime field $F_p = \mathbb{Z}/p\mathbb{Z}$ and write every $f \in R_d^{(p)}$ as $f = \sum_{\mathbf{n}\in\mathbb{Z}^d} f_{\mathbf{n}} u^{\mathbf{n}}$ with $f_{\mathbf{n}} \in F_p$ for every $\mathbf{n} \in \mathbb{Z}^d$. For every $f = \sum_{\mathbf{n}\in\mathbb{Z}^d} f_{\mathbf{n}} u^{\mathbf{n}} \in R_d$ we denote by

$$f_{/p} = \sum_{\mathbf{n}\in\mathbb{Z}^d} (f_{\mathbf{n}} \,(\mathrm{mod}\, p)) u^{\mathbf{n}} \in R_d^{(p)} \tag{7.1}$$

the Laurent polynomial obtained by reducing each coefficient of f modulo p. For every ideal $I \subset R_d^{(p)}$, $\bar{I} = \{f \in R_d : f_{/p} \in I\}$ is an ideal in R_d, and $R_d^{(p)}/I \cong R_d/\bar{I}$. Furthermore, $\bar{I} \subset R_d$ is a prime ideal if and only if $I \subset R_d^{(p)}$ is a prime ideal.

The additive group $R_d^{(p)}$ can be identified with the dual group $\widehat{(\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}^d}}$ of $(\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}^d}$ by setting

$$\langle h, \omega\rangle = e^{2\pi i \left(\sum_{\mathbf{n}\in\mathbb{Z}^d} h_{\mathbf{n}}\omega_{\mathbf{n}}\right)/p}$$

for every $h \in R_d^{(p)}$ and $\omega \in (\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}^d}$. With this identification the shift $\sigma^{\mathbf{m}} \colon (\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}^d} \longrightarrow (\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}^d}$ is dual to multiplication by $u^{\mathbf{m}}$ on $R_d^{(p)}$, and $h(\sigma)$ is dual to multiplication by h on $R_d^{(p)}$ for every $h \in R_d^{(p)}$ (cf. (4.5)).

If $\mathfrak{q} \subset R_d^{(p)}$ is an ideal with generators $\{h^{(1)}, \dots, h^{(k)}\}$, then we can rewrite (4.7) as

$$\begin{aligned}\widehat{R_d^{(p)}/\mathfrak{q}} = X_{R_d^{(p)}/\mathfrak{q}} &= \{\omega \in (\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}^d} : \langle h, \omega\rangle = 1 \text{ for every } h \in \mathfrak{q}\} \\ &= \bigcap_{h\in\mathfrak{q}} \ker(h(\sigma)) = \bigcap_{i=1}^{k} \ker(h^{(i)}(\sigma)),\end{aligned} \tag{7.2}$$

and

$$\alpha_{R_d^{(p)}/\mathfrak{q}} = \sigma_{X_{R_d^{(p)}/\mathfrak{q}}} \tag{7.3}$$

is the restriction of the shift-action σ to $X_{R_d^{(p)}/\mathfrak{q}} \subset (\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}^d}$.

Examples 7.1. (1) This is a special case of Example 3.2 (4) (a) with $F = \{(0,0),(1,0),(0,1)\}$, presented in algebraic language, and called *Ledrappier's example* after its first appearance in [24]. Let $\mathfrak{p} = (2, 1+u_1+u_2) = 2R_2 + (1+u_1+u_2)R_2$, $M = R_2/\mathfrak{p}$, and let $\alpha = \alpha_M$ be the algebraic $\mathbb{Z}^2$-action on $X = X_M = \widehat{M}$ defined in Example 4.1 (2). Then α is mixing by Table 1 (4), but the set $S = \{(0,0),(1,0),(0,1)\} \subset \mathbb{Z}^2$ is nonmixing.

Indeed, $(1+u_1+u_2)^{2^n} \cdot a = 0$ for every $n \geq 0$ and $a \in M$. For $a = 1 + (2, 1+u_1+u_2) \in M$ our identification of M with $\widehat{X}$ in Example 4.1 (2) implies that $x_{(0,0)} + x_{(2^n,0)} + x_{(0,2^n)} = 0 \pmod 1$ for every $x \in X$ and $n \geq 0$. For $B = \{x \in X : x_{(0,0)} = 0\}$ it follows that

$$B \cap \alpha^{-(2^n,0)}(B) \cap \alpha^{-(0,2^n)}(B) = B \cap \alpha^{-(2^n,0)}(B),$$

and hence that

$$\lambda_X(B \cap \alpha^{-(2^n,0)}(B) \cap \alpha^{-(0,2^n)}(B)) = \lambda_X(B \cap \alpha^{-(2^n,0)}(B)) = 1/4$$

for every $n \geq 0$. If the set $S = \{(0,0),(1,0),(0,1)\} \subset \mathbb{Z}^2$ were α-mixing, we would have that

$$\lim_{n\to\infty} \lambda_X(B \cap \alpha^{-(2^n,0)}(B) \cap \alpha^{-(0,2^n)}(B)) = \lambda_X(B)^3 = 1/8.$$

By comparing this with (5.3) we see that S is indeed nonmixing.

(2) In order to generalize Example (1) we fix an ideal $I \subset R_d^{(p)}$ and observe as in Example (1) that the *support*

$$\mathcal{S}(h) = \{\mathbf{n} \in \mathbb{Z}^d : h_{\mathbf{n}} \neq 0\} \tag{7.4}$$

of every nonzero $h \in I$ is a nonmixing set for $\alpha_{R_d^{(p)}/I}$.

The two following examples show that nonmixing sets can also arise in a much less obvious manner.

(3) ([21]) Let $f = 1 + u_1 + u_2 + u_1^2 + u_1u_2 + u_2^2 \in R_2^{(2)}$, and let $\mathfrak{p} = (f) = fR_2^{(2)} \subset R_2^{(2)}$. Since f is irreducible, $\mathfrak{p}$ is a prime ideal. We set $\alpha = \alpha_{R_2^{(2)}/\mathfrak{p}}$ and $X = X_{R_2^{(2)}/\mathfrak{p}}$ (cf. (7.2)–(7.3)).

A direct calculation shows that

$$\begin{aligned}(u_1+u_2)+(1+u_2)u_1+(1+u_1)u_2=0,\\ (1+u_1)^3=(1+u_2)^3=(u_1+u_2)^3 \pmod{\mathfrak{p}}.\end{aligned} \tag{7.5}$$

By raising the first of these equations to the fourth power and substituting terms according to the second equation we obtain that

$$\begin{aligned}0&=(u_1+u_2)^4+(1+u_2)^4u_1^4+(1+u_1)^4u_2^4\\ &=(u_1+u_2)^4+(1+u_2)(u_1+u_2)^3u_1^4+(1+u_1)(u_1+u_2)^3u_2^4 \pmod{\mathfrak{p}}.\end{aligned}$$

It follows that

$$(u_1+u_2)+(1+u_2)u_1^4+(1+u_1)u_2^4\in\mathfrak{p},$$

and by repeating this argument we see that

$$(u_1+u_2)+(1+u_2)u_1^{4^k}+(1+u_1)u_2^{4^k}\in\mathfrak{p} \tag{7.6}$$

for every $k\geq 0$. A glance at (5.4) reveals that we have proved that the set $S=\{(0,0),(1,0),(0,1)\}$ is α-nonmixing, although it is not the support of any element of $\mathfrak{p}$.

Theorem 7.3 below will explain what is going on here: if we choose a primitive third root of unity in $\bar{F}_2$, the algebraic closure of the prime field F_2, and set $F_4=F_2[\omega]$, then the polynomial $f\in F_2[u_1^{\pm1},u_2^{\pm1}]$ is no longer irreducible in the ring $F_4[u_1^{\pm1},u_2^{\pm1}]$:

$$1+u_1+u_2+u_1^2+u_1u_2+u_2^2=(1+\omega u_1+\omega^2u_2)(1+\omega^2u_1+\omega u_2).$$

For every $h\in R_2^{(2)}$ we set $[h]=h+\mathfrak{p}\in R_2^{(2)}/\mathfrak{p}$. If $K=Q(R_2^{(2)}/\mathfrak{p})$ is the field of fractions of the integral domain $R_2^{(2)}/\mathfrak{p}$, then the second equation in (7.5) is equivalent to saying that $\omega=\frac{[1+u_2]}{[u_1+u_2]}$ is a primitive third root of unity in K and hence that $K\supset F_4$. Equation (7.6) translates as

$$1+\omega^{4^k}[u_1]^{4^k}+(\omega^2)^{4^k}[u_2]^{4^k}=1+\omega[u_1]^{4^k}+\omega^2[u_2]^{4^k}=0$$

for every $k\geq 0$.

(4) ([21]) Let $f=1+u_1+u_2+u_1^2+u_1u_2+u_2^2+u_1^3+u_1^2u_2+u_1u_2^2+u_2^3\in R_2^{(2)}$, $g=1+u_1+u_2\in R_2^{(2)}$, $\mathfrak{p}=(f)\subset R_2^{(2)}$, $\mathfrak{q}=(g)\subset R_2^{(2)}$, and let $\alpha=\alpha_{R_2^{(2)}/\mathfrak{p}}=\alpha_{R_2/\bar{\mathfrak{p}}}$ and $X=X_{R_2^{(2)}/(f)}=X_{R_2/\bar{\mathfrak{p}}}$ as in Example (3). We claim that the set $S=\{(0,0),(1,0),(0,1)\}$ is nonmixing for α.

In contrast to Example (3), the polynomial f is irreducible not only in $R_2^{(2)}$, but also in $\bar{F}_2[u_1^{\pm1},u_2^{\pm1}]$, i.e. f is *absolutely irreducible*. However,

$$f(u_1^3,u_2^3)=1+u_1^3+u_2^3+u_1^6+u_1^3u_2^3+u_2^6+u_1^9+u_1^6u_2^3+u_1^3u_2^6+u_2^9=gh$$

for some $h\in R_2^{(2)}$.

We denote by $K=Q(R_2^{(2)}/\mathfrak{p})$ and $L=Q(R_2^{(2)}/\mathfrak{q})$ the fields of fractions of the integral domains $R_2^{(2)}/\mathfrak{p}$ and $R_2^{(2)}/\mathfrak{q}$, respectively, and set $[h]=h+\mathfrak{q}\in$

$R_2^{(2)}/\mathfrak{q} \subset L$ for every $h \in R_2^{(2)}$. The ring homomorphism $\eta\colon R_2^{(2)} \longrightarrow L$, defined by setting $\eta(u_i) = [u_i^3] = [u_i]^3 \in R_2^{(2)}/\mathfrak{q} \subset L$ for $i = 1, 2$, satisfies that $\ker \eta = \mathfrak{p} = (f)$. Hence η induces an embedding $\eta'\colon K \longrightarrow L$ of K as a subfield $K' = \eta'(K) \subset L$.

By assumption, $1 + [u_1]^{2^k} + [u_2]^{2^k} = 0$ in L for every $k \geq 0$. As $2^{2k} = 1 \pmod 3$ for every $k \geq 0$, the sequence of integers $l_k = \frac{2^{2k}-1}{3}$, $k \geq 0$, satisfies that

$$1 + [u_1]^{2^{2k}} + [u_2]^{2^{2k}} = 1 + [u_1^3]^{l_k}[u_1] + [u_2^3]^{l_k}[u_2] = 0$$

for every $k \geq 0$. This shows that the nonzero vector $\mathbf{v} = (1, [u_1], [u_2])$ is orthogonal to all the vectors $\mathbf{w}_k = (1, [u_1^3]^{l_k}, [u_2^3]^{l_k})$, $k \geq 0$, in L^3. As $\mathbf{w}_k \in {K'}^3$ for every $k \geq 0$, there also exists a nonzero vector $\mathbf{v}' = (a, b, c) \in {K'}^3$ which is orthogonal to every $\mathbf{w}_k$. After identifying K' with K and multiplying out denominators we obtain a nonzero vector $(a', b', c') \in (R_2^{(2)}/\mathfrak{p})^3$ such that

$$a' + u_1^{l_k} \cdot b' + u_2^{l_k} \cdot c' = 0$$

in $R_2^{(2)}/\mathfrak{p}$ for every $k \geq 0$. According to (5.4) this shows that the set $S = \{(0,0), (1,0), (0,1)\}$ is indeed nonmixing for α.

In contrast to the connected case, all zero entropy algebraic $\mathbb{Z}^d$-actions on zero-dimensional compact abelian groups have nonmixing sets.

Theorem 7.2. *A mixing algebraic $\mathbb{Z}^d$-action α on a totally disconnected compact abelian group X has nonmixing sets* (*and is thus not mixing of every order*) *if and only if it is not Bernoulli.*

Proof. Theorem 5.2 shows that α has no nonmixing sets if and only if the same is true for each $\alpha_{R_d/\mathfrak{p}}$, $\mathfrak{p} \in \operatorname{asc}(M)$, where $M = \widehat{X}$ is the dual module of α.

As X is zero-dimensional, every $\mathfrak{p} \in \operatorname{asc}(M)$ contains a rational prime $p = p(\mathfrak{p}) > 0$ by Lemma 5.1. If some $\mathfrak{p} \in \operatorname{asc}(M)$ is principal, then it is of the form $\mathfrak{p} = p(\mathfrak{p})R_d$, $\alpha_{R_d/\mathfrak{p}}$ is the shift action of $\mathbb{Z}^d$ on the full shift space $X_{R_d/\mathfrak{p}} = (\mathbb{Z}/p(\mathfrak{p})\mathbb{Z})^{\mathbb{Z}}$, $h(\alpha_{R_d/\mathfrak{p}}) = \log p(\mathfrak{p}) > 0$, and $\alpha_{R_d/\mathfrak{p}}$ is mixing of every order.

If the ideal $\mathfrak{p} \in \operatorname{asc}(M)$ is nonprincipal, we set $\mathfrak{q} = \{f_{/p(\mathfrak{p})} : f \in \mathfrak{p}\} \subset R_d^{(p(\mathfrak{p}))}$ and observe that $\mathfrak{q} \neq \{0\}$ and $\alpha_{R_d/\mathfrak{p}} = \alpha_{R_d^{(p(\mathfrak{p}))}/\mathfrak{q}}$. Example 7.1 (2) shows that the support $\mathcal{S}(h)$ of every nonzero Laurent polynomial $h \in \mathfrak{q}$ is a nonmixing set for $\alpha_{R_d/\mathfrak{p}} = \alpha_{R_d^{(p(\mathfrak{p}))}/\mathfrak{q}}$ and hence, by Theorem 5.2, for α.

If α is Bernoulli, then Table 1 (8) implies that *every* $\mathfrak{p} \in \operatorname{asc}(M)$ is principal, and Theorem 5.2 and the discussion above show that α is mixing of every order. If α is not Bernoulli, at least one $\mathfrak{p} \in \operatorname{asc}(M)$ is nonprincipal, and α therefore has nonmixing sets. $\square$

The description of the nonmixing sets of an algebraic $\mathbb{Z}^d$-action α is facilitated by a Theorem of Masser ([21], [31]), which should be seen as an analogue of Theorem 6.1 in positive characteristic.

Theorem 7.3. *Let K be an algebraically closed field of characteristic $p > 0$, $r \geq 2$, and let $(x_1, \dots, x_r) \in (K^\times)^r$. The following conditions are equivalent:*

(1) *There exists a a nonzero element $(c_1, \dots, c_r) \in K^r$ such that*

$$\sum_{i=1}^{r} c_i x_i^k = 0$$

for infinitely many $k \geq 0$;

(2) *There exists a rational number $s > 0$ such that the set $\{x_1^s, \dots, x_r^s\}$ is linearly dependent over the algebraic closure $\bar{F}_p \subset K$ of the prime field $F_p = \mathbb{Z}/p\mathbb{Z}$.*

Corollary 7.4. *Let $\mathfrak{p} \subset R_d$ be a prime ideal containing a rational prime $p > 1$, and let $\alpha = \alpha_{R_d/\mathfrak{p}}$ be the algebraic $\mathbb{Z}^d$-action on $X = X_{R_d/\mathfrak{p}}$ defined in Example* 4.1 (2)*. We denote by $K = Q(R_d/\mathfrak{p}) \supset R_d/\mathfrak{p}$ the field of fractions of the integral domain $R_d/\mathfrak{p}$, write $\bar{K}$ for its algebraic closure, and set $x_{\mathbf{n}} = u^{\mathbf{n}} + \mathfrak{p} \in R_d/\mathfrak{p} \subset K \subset \bar{K}$ for every $\mathbf{n} \in \mathbb{Z}^d$. If $S \subset \mathbb{Z}^d$ is a nonempty finite set, then the following conditions are equivalent:*

(1) *S is not α-mixing;*

(2) *There exists a rational number $s > 0$ such that the set $\{x_{\mathbf{n}}^s : \mathbf{n} \in S\} \subset \bar{K}$ is linearly dependent over $\bar{F}_p \subset \bar{K}$.*

Proof of Corollary 7.4*, given Theorem* 7.3. If a nonempty finite subset $S \subset \mathbb{Z}^d$ is not mixing for α, then (5.4) implies that there exist elements $\{a_{\mathbf{n}} : \mathbf{n} \in S\}$ in $R_d/\mathfrak{p}$, not all equal to zero, and infinitely many $k \geq 1$ such that

$$\sum_{\mathbf{n} \in S} u^{k\mathbf{n}} \cdot a_{\mathbf{n}} = 0.$$

If we set $x_{\mathbf{n}} = u^{\mathbf{n}} + \mathfrak{p} \in R_d/\mathfrak{p} \subset K$ for every $\mathbf{n} \in S$, we obtain Condition (1) in Theorem 7.3 and hence Condition (2) in our corollary.

Conversely, if $\{x_{\mathbf{n}}^s : \mathbf{n} \in S\}$ is linearly dependent over $\bar{F}_p$ for some rational number $s > 0$, then we obtain a nontrivial equation of the form

$$\sum_{\mathbf{n} \in S} \omega_{\mathbf{n}} x_{\mathbf{n}}^s = 0$$

with $\omega_{\mathbf{n}} \in \bar{F}_p$ for every $\mathbf{n} \in S$. By Theorem 7.3 there exists a nonzero element $(c_{\mathbf{n}}, \mathbf{n} \in S) \in \bar{K}^S$ with

$$\sum_{\mathbf{n} \in S} c_{\mathbf{n}} x_{\mathbf{n}}^k = 0$$

for infinitely many $k \geq 0$. Hence there exists a nonzero element $(c'_{\mathbf{n}}, \mathbf{n} \in S) \in K^S$ with

$$\sum_{\mathbf{n}\in S} c'_{\mathbf{n}} x^k_{\mathbf{n}} = 0$$

for infinitely many $k \geq 0$, and after clearing denominators we obtain a nonzero element $(a_{\mathbf{n}}, \mathbf{n} \in S) \in (R_d/\mathfrak{p})^S$ with

$$\sum_{\mathbf{n}\in S} u^{k\mathbf{n}} \cdot a_{\mathbf{n}} = 0$$

for infinitely many $k \geq 0$. This shows that the set S is α-nonmixing. □

In order to understand the dynamical implications of Corollary 7.4 we return to the Examples 7.1 on page 20.

Examples 7.5. (1) In Example 7.1 (2) we used the fact that $f = 1 + u_1 + u_2 + u_1^2 + u_1 u_2 + u_2^2 \in R_2^{(2)}$ is irreducible over F_2, but not over $\bar{F}_2$. We define $\mathfrak{p} = (f) \subset R_2^{(2)}$ as in that example, set $R_2^{(4)} = F_4[u_1^{\pm1}, u_2^{\pm1}]$ and put $\mathfrak{q} = (1 + \omega u_1 + \omega^2 u_2) \subset R_2^{(4)}$. If $\iota\colon R_2^{(2)} \longrightarrow R_2^{(4)}$ is the inclusion map and $\pi\colon R_2^{(4)} \mapsto R_2^{(4)}/\mathfrak{q}$ the quotient map, then $\ker(\pi \circ \iota) = \mathfrak{p}$, and the map $\pi \circ \iota$ induces an embedding of the field of fractions $K = Q(R_2^{(2)}/\mathfrak{p})$ in the field of fractions $L = Q(R_2^{(4)}/\mathfrak{p})$. As we saw in Example 7.1 (2),

$$1 + \omega u_1^{2^{2k}} + \omega^2 u_2^{2^{2k}} = 0$$

in L for every $k \geq 0$, i.e the vector $(1, \omega, \omega^2) \in L^3$ is orthogonal to $(1, u_1^{2^{2k}}, u_2^{2^{2k}}) \in K \subset L$ for every $k \geq 0$. Hence there exists an nonzero $\mathbf{v} \in K^3$ which is orthogonal to every $(1, u_1^{2^{2k}}, u_2^{2^{2k}})$, and $\mathbf{v} = (u_1 + u_2, 1 + u_2, 1 + u_1)$ amounts to an explicit choice of such a vector.

The injection $\hat{\eta}\colon R_2^{(2)}/\mathfrak{p} \longrightarrow R_2^{(4)}/\mathfrak{p}$ induced by the map $\pi \circ \iota\colon R_2^{(2)} \longrightarrow R_2^{(4)}/\mathfrak{q}$ above embeds the R_2-module $M = R_2^{(2)}/\mathfrak{p}$ as a submodule of index 2 in the R_2-module $N = R_2^{(4)}/\mathfrak{q}$. The corresponding dual factor map $\eta\colon X_N \longrightarrow X_M$ sends $\alpha = \alpha_M$ to $\beta = \alpha_N$ and is two-to-one. We shall return to these two algebraic $\mathbb{Z}^2$-actions in Example 8.21 on page 45.

(2) In the notation of Example 7.1 (4) we set $\mathfrak{p} = (f) \subset R_2^{(2)}$, $\mathfrak{q} = (g) \subset R_2^{(2)}$, $\alpha = \alpha_{R_2^{(2)}/\mathfrak{p}}$, $X = X_{R_2^{(2)}/\mathfrak{p}} = \widehat{R_2^{(2)}/\mathfrak{p}}$, $\beta = \alpha_{R_2^{(2)}/\mathfrak{q}}$ and $Y = X_{R_2^{(2)}/\mathfrak{q}} = \widehat{R_2^{(2)}/\mathfrak{q}}$. We put $\Gamma = 3\mathbb{Z}^3$ and write $\pi_\Gamma\colon Y \longrightarrow (\mathbb{Z}/2\mathbb{Z})^\Gamma$ for the projection onto the coordinates in Γ. By identifying Γ with $\mathbb{Z}^2$ we view $\pi_\Gamma(Y)$ as a closed shift-invariant subgroup of $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{Z}^2}$, and a little calculation shows that $\pi_\Gamma(Y) = X$ and that $\pi_\Gamma\colon Y \longrightarrow X$ is two-to-one.

The set $S = \{(0,0), (1,0), (0,1)\} \subset \mathbb{Z}^2$ is obviously β-nonmixing. We write $\beta_\Gamma\colon \mathbf{n} \mapsto \beta^{3\mathbf{n}}$ for the Γ-action obtained from β by restriction and observe that the two-to-one factor map $\pi_\Gamma\colon Y \longrightarrow X$ sends β_Γ to α. Furthermore, the set S is also β_Γ-nonmixing, and this property of S survives under the factor map $\pi_\Gamma\colon Y \longrightarrow X$ (this is the essence of the calculation in Example 7.1 (4)).

If an algebraic $\mathbb{Z}^d$-action α is r-mixing, then every set $S \subset \mathbb{Z}^d$ with cardinality $|S| \le r$ is obviously mixing. The converse is far from obvious: if α is not mixing of order $r \ge 2$, and if r is the smallest integer with this property, does there exist a nonmixing set $S \subset \mathbb{Z}^d$ of size r? Remarkably, this turns out to be the case, as a consequence of a second theorem by Masser.

Theorem 7.6 ([32])**.** *Let α be an algebraic $\mathbb{Z}^d$-action on a compact abelian group X, and let $r \ge 2$. If every subset $S \subset \mathbb{Z}^d$ of cardinality r is mixing, then α is r-mixing.*

In order to explain the connection between Theorem 7.6 and an appropriate analogue of Theorem 6.3 we need a definition.

Definition 7.7. Let G be a multiplicative abelian group and n a positive integer. An infinite subset $\Xi \subset G^n$ is *broad* if it satisfies the following conditions.

(1) If $g \in G$ and $1 \le i \le n$, then there are at most finitely many $(\xi_1, \dots, \xi_n) \in \Xi$ with $\xi_i = g$;
(2) If $n \ge 2$, $g \in G$ and $1 \le i < j \le n$, then there are at most finitely many $(\xi_1, \dots, \xi_n) \in \Xi$ with $\xi_i/\xi_j = g$.

Theorem 7.8 ([32])**.** *Let K be a field of characteristic $p > 1$ and $G \subset K^\times$ a finitely generated subgroup. Suppose that $n \ge 1$, and that the equation*

$$a_1x_1 + \cdots + a_nx_n = 1 \tag{7.7}$$

has a broad set of solutions $(x_1, \dots, x_n) \in G^n$ for some $(a_1, \dots, a_n) \in (K^\times)^n$. Then there exist a positive integer $m \le n$ and elements $(b_1, \dots, b_m) \in (K^\times)^m$, $(g_1, \dots, g_m) \in G^m$, with the following properties.

(1) *$g_i \ne 1$ for $i = 1, \dots, m$;*
(2) *$g_i/g_j \ne 1$ for $1 \le i < j \le m$;*
(3) *There exist infinitely many $k \ge 1$ with*

$$b_1g_1^k + \cdots + b_mg_m^k = 1. \tag{7.8}$$

Proof of Theorem 7.6*, given Theorem* 7.8*.* The translation of Theorem 7.6 into Theorem 7.8 works exactly as in Corollary 7.4. If α is an algebraic $\mathbb{Z}^d$-action on a compact abelian group X which is not mixing of order $r \ge 2$, and if r is the smallest integer with this property, then Theorem 5.2 guarantees the existence of a prime ideal $\mathfrak{p}$ associated with the dual module $M = \widehat{X}$ of α such that $\alpha_{R_d/\mathfrak{p}}$ is not r-mixing.

If $r = 2$, Table 1 (4) implies that $u^{\mathbf{n}} - 1 \in \mathfrak{p}$ for some nonzero $\mathbf{n} \in \mathbb{Z}^d$. Hence $u^{k\mathbf{n}} - 1 \in \mathfrak{p}$ and $a - u^{k\mathbf{n}} \cdot a = 0$ for every $k \geq 0$ and $a \in R_d/\mathfrak{p}$, and (5.4) shows that the set $S = \{\mathbf{0}, \mathbf{n}\} \subset \mathbb{Z}^d$ is nonmixing for $\alpha_{R_d/\mathfrak{p}}$ and hence, by Theorem 5.2, for α.

If $r > 2$ we denote by K the field of fractions of the integral domain $R_d/\mathfrak{p}$, embed $R_d/\mathfrak{p}$ in K in the obvious manner, and write $G \subset K^{\times}$ for the multiplicative group generated by $\{x_{\mathbf{n}} = u^{\mathbf{n}} + \mathfrak{p} : \mathbf{n} \in \mathbb{Z}^d\}$. Since $\alpha_{R_d/\mathfrak{p}}$ is mixing, $G \cong \mathbb{Z}^d$ by Table 1 (4). Equation (5.2) shows that there exist elements $a_1, \dots, a_r \in R_d/\mathfrak{p}$, not all equal to zero, and a sequence $((\mathbf{n}_k^{(1)}, \dots, \mathbf{n}_k^{(r)}),\ k \geq 1)$ in $(\mathbb{Z}^d)^r$ such that $\lim_{k\to\infty} \|\mathbf{n}_k^{(i)} - \mathbf{n}_k^{(j)}\| = \infty$ for all i, j with $1 \leq i < j \leq r$, and

$$u^{\mathbf{n}_k^{(1)}} \cdot a_1 + \cdots + u^{\mathbf{n}_k^{(r)}} \cdot a_r = 0$$

for every $k \geq 1$. The minimality of r implies that the a_i are all nonzero, and we may obviously assume in addition that $\mathbf{n}_k^{(r)} = \mathbf{0}$ for every $k \geq 1$.

We set $\xi_k = (\xi_k^{(1)}, \dots, \xi_k^{(r-1)}) = (u^{\mathbf{n}_k^{(1)}} + \mathfrak{p}, \dots, u^{\mathbf{n}_k^{(r-1)}} + \mathfrak{p}) \in G^{r-1}$ for every $k \geq 1$. Then $\Xi = \{\xi_k : k \geq 1\}$ is a broad set of solutions of the equation

$$\frac{a_1}{a_r} x_1 + \cdots + \frac{a_{r-1}}{a_r} x_{r-1} = 1.$$

Theorem 7.8 yields a positive integer $m \leq r - 1$ and elements $(b_1, \dots, b_m) \in (K^{\times})^m$, $(g_1, \dots, g_m) \in G^m$, with the properties listed there, such that

$$b_1 g_1^k + \cdots + b_m g_m^k = 1$$

for infinitely many $k \geq 1$. Since each $g_i = u^{\mathbf{t}_i} + \mathfrak{p}$ for some unique nonzero $\mathbf{t}_i \in \mathbb{Z}^d$ we obtain after clearing denominators that

$$u^{k\mathbf{t}_1} \cdot b'_1 + \cdots + u^{k\mathbf{t}_m} \cdot b'_m = b'_{m+1}$$

for some nonzero elements $b'_i \in R_d/\mathfrak{p}$ and infinitely many $k \geq 1$. An application of (5.4) shows that the set $S = \{\mathbf{0}, \mathbf{t}_1, \dots, \mathbf{t}_m\}$ is nonmixing for $\alpha_{R_d/\mathfrak{p}}$ and hence, by Theorem 5.2, for α. The minimality of r implies that $|S| = m + 1 = r$. This completes the proof of the theorem. □

In order to appreciate the difficulty in proving Theorem 7.6 one should once again consider Ledrappier's Example 7.1 (1). As we saw there, the set $S = \{(0,0), (1,0), (0,1)\}$ is nonmixing (and obviously minimal) for the $\mathbb{Z}^2$-action $\alpha = \alpha_{R_2^{(2)}/(f)}$ defined in that example. However, for every $k_0, k_1, k_2, k_3 \geq 0$ with $2^{k_0} > 2^{k_1} + 2^{k_2} + 2^{k_3}$, say, the set

$$S_{k_0,k_1,k_2,k_3} = \{(2^{k_1}, 0), (0, 2^{k_1}), (2^{k_0} - 2^{k_2}, 0), (2^{k_0} - 2^{k_2}, 2^{k_2}), (0, 2^{k_0} - 2^{k_3}), (2^{k_3}, 2^{k_0} - 2^{k_3})\}$$

is also minimal nonmixing: it is the support of the polynomial

$$g_{k_0,k_1,k_2,k_3} = (1+u_1+u_2)^{2^{k_0}} + (1+u_1+u_2)^{2^{k_1}} + u_1^{2^{k_0}-2^{k_2}}(1+u_1+u_2)^{2^{k_2}} + u_2^{2^{k_0}-2^{k_3}}(1+u_1+u_2)^{2^{k_3}} \in \mathfrak{p}.$$

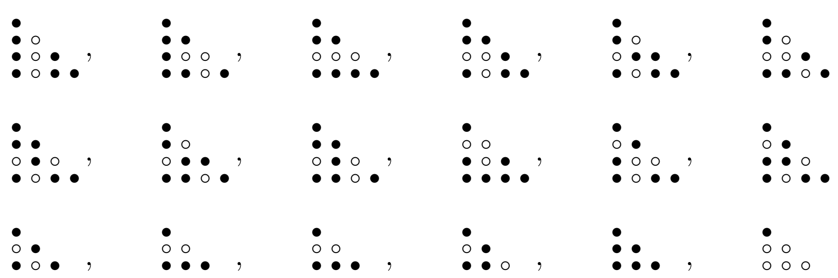
By choosing appropriate increasing sequences $k_i^{(n)}$, $n \geq 1$, $i = 0, \dots, 3$, we obtain minimal nonmixing sets $S_n = S_{k_0^{(n)},k_1^{(n)},k_2^{(n)},k_3^{(n)}}$, $n \geq 1$, of varying shapes without any resemblance to linear multiples of a single nonmixing set $S' \subset \mathbb{Z}^2$. Nevertheless one can extract sufficient information from any such sequence to obtain a nonmixing set for α; for details we refer to [32].

Theorem 7.6 reduces the problem of determining the order of mixing to finding nonmixing sets of smallest cardinality. However, even with Corollary 7.4 at hand, the latter problem remains nontrivial: I am not aware of any good general algorithm for determining polynomials with minimal support in a given ideal. The following list, taken from [42], illustrates a much easier problem which can be solved effectively with Corollary 7.4: it shows all irreducible polynomials $f \in R_2^{(2)}$ of degree ≤ 4 in each of the variables u_1, u_2, such that the set $S = \{(0,0),(1,0),(0,1)\}$ is nonmixing for $\alpha_{R_2^{(2)}/(f)}$. For convenience we adopt a (hopefully self-explanatory) graphical representation of the supports of these polynomials as subsets of $\mathbb{Z}^2$. We start with the polynomials of degree ≤ 2.

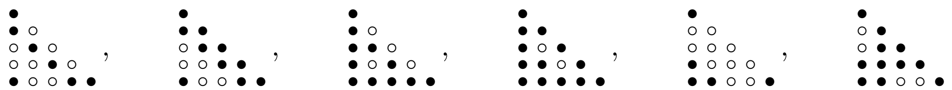
 (corresponding to the polynomial $1+u_1+u_2$),

(corresponding to the polynomials $1+u_1+u_1^2+u_1u_2+u_2^2$, $1+u_1^2+u_2+u_1u_2+u_2^2$, $1+u_1+u_1^2+u_2+u_2^2$ and $1+u_1+u_1^2+u_2+u_1u_2+u_2^2$).

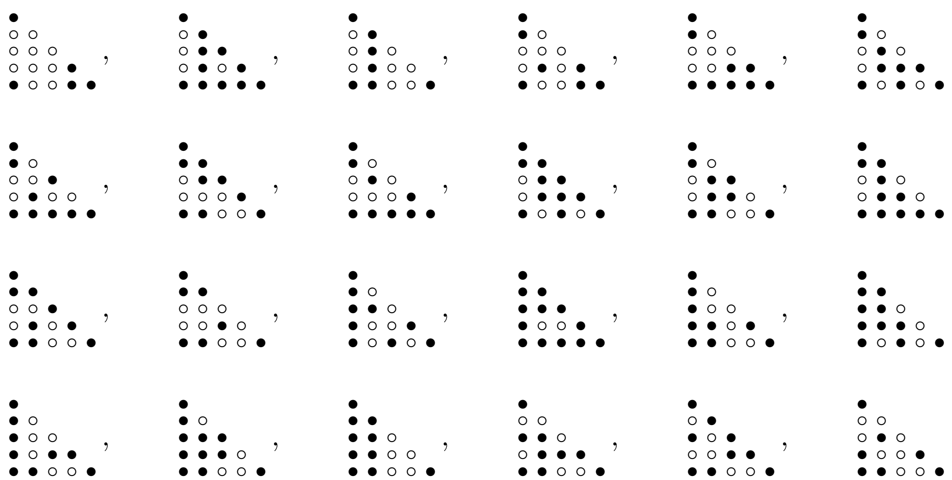
There are 18 irreducible polynomials $f \in R_2^{(2)}$ of degree 3 such that S is non-mixing for $\alpha_{R_2^{(2)}/(f)}$. The supports of these polynomials are as follows.



Similarly one can describe the supports of all 54 irreducible polynomials $f \in R_2^{(2)}$ of degree 4 such that S is non-mixing for $\alpha_{R_2^{(2)}/(f)}$. We begin by listing the supports of those polynomials which are symmetric in u_1 and u_2. These supports are unaffected if the coordinates are interchanged.



For each of the remaining polynomials $f \in R_2^{(2)}$, the polynomial $\tilde{f}$ (not shown here) obtained by interchanging the coordinates u_1, u_2 again has S as an $\alpha_{R_2^{(2)}/(\tilde{f})}$-nonmixing set.



8. Isomorphism rigidity of algebraic $\mathbb{Z}^d$-actions: the irreducible case

In this section we turn to a problem of a quite different nature from that of the last sections. Every algebraic $\mathbb{Z}^d$-action α with completely positive entropy is measurably conjugate to a Bernoulli shift (cf. Table 1 (8) on page 12). Since entropy is a complete invariant for measurable conjugacy of Bernoulli shifts by [35], α is measurably conjugate to the $\mathbb{Z}^d$-action

$$\alpha^A\colon \mathbf{n} \mapsto \alpha^{A\mathbf{n}}$$

for every $A \in \mathrm{GL}(d, \mathbb{Z})$, since the entropies of all these actions coincide. In general, however, α and α^A are not topologically conjugate.

Every algebraic $\mathbb{Z}^d$-action α with positive entropy has Bernoulli factors by [27] and [38], and two such actions may again be measurably conjugate without being topologically conjugate. For zero entropy actions, however, there is some evidence for a very strong form of isomorphism rigidity. In order to formulate this property we introduce a definition.

Definition 8.1. Let α and β be algebraic $\mathbb{Z}^d$-actions on compact abelian groups X and Y, respectively. Then (Y,β) is an *algebraic factor* of (X,α) if there exists a continuous surjective group homomorphism $\psi\colon X \longrightarrow Y$ with

$$\psi \circ \alpha^{\mathbf{n}} = \beta^{\mathbf{n}} \circ \psi \tag{8.1}$$

for every $\mathbf{n} \in \mathbb{Z}^d$. The map ψ in (8.1) is an *algebraic factor map*. The actions α and β (or the pairs (X,α) and (Y,β)) are *algebraically conjugate* if the map ψ in (8.1) can be chosen to be a group isomorphism. Finally, α and β (or (X,α) and (Y,β)) are *finitely* (*algebraically*) *equivalent* if each of them is an algebraic factor of the other one with a finite-to-one factor map.

A map $\phi\colon X \longrightarrow Y$ is *affine* if it is of the form $\phi(x) = \psi(x) + y$ for every $x \in X$, where $\psi\colon X \longrightarrow Y$ is a continuous surjective group homomorphism and $y \in Y$. If there exists an affine map $\phi\colon X \longrightarrow Y$ satisfying (8.1) (with ϕ replacing ψ), then β is obviously an algebraic factor of α.

We say that *isomorphism rigidity* holds for a class of algebraic $\mathbb{Z}^d$-actions if any measurable conjugacy between two actions in this class coincides *a.e.* with an affine map. Let us begin with the class of irreducible $\mathbb{Z}^d$-actions to illustrate a much more general phenomenon.

Definition 8.2. An algebraic $\mathbb{Z}^d$-action α on a compact abelian group X is *irreducible* if every closed α-invariant subgroup $Y \subsetneq X$ is finite.

Irreducible $\mathbb{Z}^d$-actions were called *almost minimal* in [42].

Proposition 8.3. *Let α be an irreducible and ergodic algebraic $\mathbb{Z}^d$-action on a compact abelian group X, and let β be an algebraic $\mathbb{Z}^d$-action on a compact abelian group $Y \neq \{0\}$ such that (Y,β) is an algebraic factor of (X,α). Then the factor map is finite-to-one, and β is irreducible, ergodic and finitely equivalent to α. Furthermore there exists a unique prime ideal $\mathfrak{p} \subset R_d$ with the following properties.*

1. *$\alpha_{R_d/\mathfrak{p}}$ is ergodic (and hence $R_d/\mathfrak{p}$ is infinite — cf.* Table 1 (3)*);*
2. *For every ideal $I \supsetneq \mathfrak{p}$ in R_d, R_d/I is finite;*
3. *α is finitely equivalent to $\alpha_{R_d/\mathfrak{p}}$.*

Conversely, if $\mathfrak{p} \subset R_d$ is a prime ideal satisfying Condition (2) *above, then the $\mathbb{Z}^d$-action $\alpha = \alpha_{R_d/\mathfrak{p}}$ on the group $X_{R_d/\mathfrak{p}}$ is irreducible.*

Proof. Let $\phi\colon X \longrightarrow Y$ be an algebraic factor map from (X,α) to (Y,β). The kernel $K = \ker\phi$ is an α-invariant closed subgroup of X. As $Y \neq \{0\}$ by assumption, K is a proper α-invariant subgroup and thus finite by irreducibility.

Let Z be a proper closed β-invariant subgroup of Y. The subgroup $\phi^{-1}(Z) \subset X$ is finite by irreducibility. This shows that $Z = \phi(\phi^{-1}(Z))$ is finite. The (obviously ergodic) action β is therefore irreducible.

The ergodicity of α also implies that every nonzero submodule $N \subset M$ of the dual module $M = \widehat{X}$ of α is infinite: otherwise $Z = \widehat{N} = X/N^{\perp}$ would be a finite quotient of X by an α-invariant subgroup, contrary to ergodicity. As the inclusion $N \subset M$ is dual to a factor map ψ from (X, α) to (X_N, α_N), the beginning of this proof shows that α_N is irreducible and $|M/N| = |\ker \psi|$ is finite. In particular, if $\mathfrak{p}$ is a prime ideal associated with M, and if $a \in M$ satisfies that $\operatorname{ann}(a) = \mathfrak{p}$ and hence $N = R_d \cdot a \cong R_d/\mathfrak{p}$, then N is infinite, M/N is finite and $\alpha_N = \alpha_{R_d/\mathfrak{p}}$ is ergodic and irreducible.

If $I \supsetneq \mathfrak{p}$ is an ideal, then $N' = I \cdot a \cong I/\mathfrak{p}$ is a submodule of N and hence — again by irreducibility — of finite index in N. It follows that R_d/I is finite, as claimed in (2).

If $\mathfrak{q} \neq \mathfrak{p}$ is a second prime ideal associated with M then $\mathfrak{q} = \operatorname{ann}(b)$ for some $b \in M \smallsetminus N$. Every nonzero $b' \in N' = R_d \cdot b$ has $\mathfrak{q}$ as its annihilator. However, since $R_d/\mathfrak{q} \cong N'$ is infinite by ergodicity and $N'/N = N'/(N \cap N')$ is finite, there exists an $h \in R_d \smallsetminus \mathfrak{q}$ with $h \cdot b \in N$ and hence $\operatorname{ann}(h \cdot b) = \mathfrak{p}$. This contradiction implies that $\mathfrak{p}$ is the only prime ideal associated with M.

In order to complete the proof that α and $\alpha_N = \alpha_{R_d/\mathfrak{p}}$ are finitely equivalent we have to find a (necessarily finite-to-one) algebraic factor map $\phi' \colon (X_N, \alpha_N) \longrightarrow (X, \alpha)$. As in the preceding paragraph we note that there exists, for every $b \in M \smallsetminus N$, an element $h_b \in R_d \smallsetminus \mathfrak{p}$ with $h_b \cdot b \in N$. The polynomial

$$h = \prod_{b \in M \smallsetminus N} h_b \in R_d \smallsetminus \mathfrak{p}$$

satisfies that $h \cdot M \subset N$. The map $m_h \colon M \longrightarrow N$ consisting of multiplication by h is injective by Footnote 3 on page 10, and the surjective homomorphism $\phi' \colon X_N \longrightarrow X$ dual to m_h is an algebraic factor map from (X_N, α_N) to (X, α). This proves (3).

We return to the first assertion of this proposition. We have proved that β is irreducible and hence finitely equivalent to $\alpha_{R_d/\mathfrak{p}}$ for some prime ideal $\mathfrak{p} \subset R_d$ satisfying the conditions (1) and (2). The factor map $\phi \colon (X, \alpha) \longrightarrow (Y, \beta)$ is dual to an embedding $\hat{\phi} \colon \widehat{Y} \longrightarrow M$. Since $\mathfrak{p}$ is the only prime ideal associated with M, $\mathfrak{p}$ is also associated with $\widehat{Y}$, and β is finitely equivalent to $\alpha_{R_d/\mathfrak{p}}$ and hence to α.

The final assertion has already been verified in the course of this proof. $\square$

Irreducibility is an extremely strong hypothesis: if α is mixing it implies that $\alpha^{\mathbf{n}}$ is Bernoulli with finite entropy for every nonzero $\mathbf{n} \in \mathbb{Z}^d$, and hence, if $d > 1$, that α has zero entropy. If β is a second irreducible and mixing algebraic $\mathbb{Z}^d$-action on a compact abelian group Y such that $h(\alpha^{\mathbf{n}}) = h(\beta^{\mathbf{n}})$ for every $\mathbf{n} \in \mathbb{Z}^d$, then $\alpha^{\mathbf{n}}$ is measurably conjugate to $\beta^{\mathbf{n}}$ for every $\mathbf{n} \in \mathbb{Z}^d$.

However, if $d > 1$, then the actions α and β are generally not measurably conjugate, as the following theorem and the examples below show.

Theorem 8.4 (Isomorphism rigidity for irreducible $\mathbb{Z}^d$-actions)**.** *Let $d > 1$, and let α_1 and α_2 be irreducible and mixing algebraic $\mathbb{Z}^d$-actions on compact abelian groups X_1 and X_2, respectively. If $\phi\colon X_1 \longrightarrow X_2$ is a measurable conjugacy of α_1 and α_2, then ϕ is λ_{X_1}-a.e. equal to an affine map. In particular, measurable conjugacy implies algebraic conjugacy.*

Theorem 8.4 is a combination of two theorems in [18] and [22], respectively, and follows from a result on invariant measures of algebraic $\mathbb{Z}^d$-actions with $d \geq 2$ whose scope is still something of a mystery. We state a very special case which will be sufficient for proving Theorem 8.4; possible ramifications of Theorem 8.5 will be discussed in Section 9.

Theorem 8.5. *Let $d \geq 2$, and let α_1 and α_2 be irreducible and mixing algebraic $\mathbb{Z}^d$-actions on compact abelian groups X_1 and X_2 with normalized Haar measures λ_{X_1} and λ_{X_2}, respectively. We write $\alpha = \alpha_1 \times \alpha_2$ for the product-$\mathbb{Z}^d$-action on $X = X_1 \times X_2$ and assume that μ is an α-invariant probability measure on X with the following property: if $\pi_i\colon X \longrightarrow X_i$ denotes the i-th coordinate projection, then $\mu\pi_i^{-1} = \lambda_{X_i}$, and π_i is a measurable conjugacy of the $\mathbb{Z}^d$-actions (X, μ, α) and $(X_i, \lambda_{X_i}, \alpha_i)$.*

Then there exists a closed α-invariant subgroup $Y \subset X$ such that μ is a translate of the Haar measure λ_Y.

Proof. Since the $\mathbb{Z}^d$-actions α_i are irreducible, Proposition 8.3 shows that the groups X_i have to be either zero-dimensional or connected (depending on whether or not the prime ideal $\mathfrak{p} \subset R_d$ appearing there contains a nonzero constant). If X_1 and X_2 are finite-dimensional tori, Theorem 8.5 follows from Corollary 5.2′ in [19, Corrections] (cf. [18, Theorem 5.1]), and this result can be extended to irreducible $\mathbb{Z}^d$-actions on compact connected abelian groups without much difficulty, using the structure theorems about irreducible $\mathbb{Z}^d$-actions in Subsection 8.1. If X_1 and X_2 are zero-dimensional, Theorem 8.5 follows from the main result in [22].

The case where one of the groups is connected and the other is zero-dimensional is impossible: if X_1 is connected and X_2 zero-dimensional, then Corollary 6.2 implies that α_1 has no nonmixing sets, whereas α_2 has nonmixing sets by Theorem 7.2, since it has entropy zero. Since the hypotheses of Theorem 8.5 imply that α_1 and α_2 are measurably conjugate we obtain a contradiction. $\square$

Proof of Theorem 8.4*, given Theorem* 8.5. Suppose that $\phi\colon X_1 \longrightarrow X_2$ is a measurable conjugacy of α_1 and α_2. We set $X = X_1 \times X_2$, consider the product $\mathbb{Z}^d$-action $\alpha = \alpha_1 \times \alpha_2$ on $X = X_1 \times X_2$, and denote by μ the unique

α-invariant probability measure on the graph $\Gamma(\phi) = \{(x, \phi(x)) : x \in X_1\} \subset X$ which satisfies that $\mu\pi_i^{-1} = \lambda_{X_i}$ for $i = 1, 2$, where $\pi_i \colon X \longrightarrow X_i$ are the coordinate projections. Since all the hypotheses of Theorem 8.4 are satisfied we conclude that μ is a translate of the Haar measure of a closed subgroup of X and hence that ϕ is *a.e.* equal to an affine map. □

In order to present examples of the subtle isomorphism behaviour of irreducible algebraic $\mathbb{Z}^d$-actions we start with a description of such actions on connected groups, taken from [12].

8.1. **Irreducible $\mathbb{Z}^d$-actions on compact connected abelian groups.** There is an intimate connection between irreducible $\mathbb{Z}^d$-actions on compact connected abelian groups and ideal classes of algebraic number fields (cf. e.g. [12], [18], [41], [42]). Since this connection plays a central role in the construction of examples it will be useful to describe it in some detail; further information can be found in [12], [42, Section 7] and [50].

Let K be an algebraic number field, i.e. a finite extension of $\mathbb{Q}$. A *valuation* of K is a map $\phi \colon K \longrightarrow \mathbb{R}_+$ with the property that $\phi(a) = 0$ if and only if $a = 0$, $\phi(ab) = \phi(a)\phi(b)$, and $\phi(a + b) \leq c \cdot \max\{\phi(a), \phi(b)\}$ for some $c \geq 1$ in $\mathbb{R}$ and all $a, b \in K$. The valuation ϕ is *non-trivial* if $\phi(K) \supsetneq \{0, 1\}$. A non-trivial valuation ϕ is *non-archimedean* if $\phi(a + b) \leq \max\{\phi(a), \phi(b)\}$ for all $a, b \in K$, and *archimedean* otherwise. Two valuations ϕ, ψ of K are *equivalent* if there exists an $s > 0$ with $\phi(a) = \psi(a)^s$ for all $a \in K$. An equivalence class v of non-trivial valuations of K is called a *place* of K; such a place v is *finite* if it consists of non-archimedean valuations, and *infinite* otherwise.

If v is a place of K, then a sequence $(a_n, n \geq 1)$ in K is v-*Cauchy* if $\lim_{k,l\to\infty} \phi(a_k - a_l) = 0$ for some (and hence for every) valuation $\phi \in v$. With this notion of a Cauchy sequence one can define the *completion* K_v of K at the place v.

Ostrowski's Theorem ([8, Theorem 2.2.1]) states that every non-trivial valuation ϕ of $\mathbb{Q}$ is either equivalent to the absolute value $\frac{m}{n} \mapsto |\frac{m}{n}| = |\frac{m}{n}|_\infty$, or to the p-adic valuation $|\frac{m}{n}|_p = p^{(n'-m')}$ for some rational prime p, where $m = p^{m'}m''$, $n = p^{n'}n''$, and neither m'' nor n'' are divisible by p. The completions $\mathbb{Q}_\infty$ and $\mathbb{Q}_p$ of $\mathbb{Q}$ are equal to $\mathbb{R}$ and the field of p-adic rationals, respectively.

For every valuation ϕ of K, the restriction of ϕ to $\mathbb{Q} \subset K$ is a valuation of $\mathbb{Q}$ and is thus equivalent either to $|\cdot|_\infty$ or to $|\cdot|_p$ for some rational prime p. In the first case the place $v \ni \phi$ is infinite (or *lies above* ∞), and in the second case v *lies above* p (or p *lies below* v).

We denote by w the place of $\mathbb{Q}$ below v and observe that the field K_v is a finite-dimensional vector space over the locally compact, metrizable field

$\mathbb{Q}_w$ and hence locally compact and metrizable. Choose a Haar measure λ_v on K_v (with respect to addition) and denote by $\mathrm{mod}_{K_v}\colon K_v \longrightarrow \mathbb{R}$ the map satisfying

$$\lambda_v(aB) = \mathrm{mod}_{K_v}(a)\lambda_v(B) \tag{8.2}$$

for every $a \in K_v$ and every Borel set $B \subset K_v$. The restriction of mod_{K_v} to K is a valuation in v, denoted by $|\cdot|_v$.

Above every place v of $\mathbb{Q}$ there are at least one and at most finitely many places of K. We write $P^{(K)}$, $P_f^{(K)}$, and $P_\infty^{(K)}$, for the sets of places, finite places and infinite places of K. An infinite place v of K is either *real* (if $K_v = \mathbb{R}$) or *complex* (if $K_v = \mathbb{C}$). The field K is *totally real* if $K_v = \mathbb{R}$ for every $v \in P_\infty^{(K)}$, and *totally complex* if $K_v = \mathbb{C}$ for every $v \in P_\infty^{(K)}$.

For every $v \in P^{(K)}$, the sets

$$\mathcal{R}_v = \{a \in K_v : |a|_v \le 1\}, \qquad \mathcal{R}_v^\times = \{a \in K_v : |a|_v = 1\} \tag{8.3}$$

are compact. If $v \in P_f^{(K)}$, then $\mathcal{R}_v$ is the unique maximal compact subring of K_v and is also open, and the ideal

$$\mathcal{P}_v = \{a \in K_v : |a|_v < 1\} \subset \mathcal{R}_v \tag{8.4}$$

is open, closed and maximal. The set

$$\mathfrak{o}_K = \bigcap_{v \in P_f^{(K)}} \{a \in K : |a|_v \le 1\} \tag{8.5}$$

is the ring of integral elements in K.

Now suppose that $d \ge 1$ and $\mathbf{c} = (c_1, \dots, c_d) \in (\bar{\mathbb{Q}}^\times)^d$, where $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ and $\bar{\mathbb{Q}}^\times = \bar{\mathbb{Q}} \smallsetminus \{0\}$. We set $K = K_{\mathbf{c}} = \mathbb{Q}(c_1, \dots, c_d) = \mathbb{Q}[c_1^{\pm 1}, \dots, c_d^{\pm 1}]$ and

$$S_{\mathbf{c}} = P_\infty^{(K)} \cup \{v \in P_f^{(K)} : |c_i|_v \ne 1 \text{ for some } i = 1, \dots, d\}. \tag{8.6}$$

The set $S_{\mathbf{c}}$ is finite by [50, Theorem III.3]. We denote by

$$\iota_{\mathbf{c}}\colon K \longrightarrow V_{\mathbf{c}} = \prod_{v \in S_{\mathbf{c}}} K_v \tag{8.7}$$

the diagonal embedding $a \mapsto (a, \dots, a)$, $a \in K$, and write

$$\mathcal{R}_{\mathbf{c}} = \{a \in K : |a|_v \le 1 \text{ for every } v \in P^{(K)} \smallsetminus S_{\mathbf{c}}\} \supset \mathfrak{o}_K \tag{8.8}$$

for the ring of $S_{\mathbf{c}}$-*integers* in K. The set $V_{\mathbf{c}}$ is a locally compact algebra over K with respect to coordinate-wise addition, multiplication and scalar multiplication, and $\iota_{\mathbf{c}}(\mathcal{R}_{\mathbf{c}})$ is a discrete, co-compact, additive subgroup of $V_{\mathbf{c}}$. Put

$$Y_{\mathbf{c}} = V_{\mathbf{c}} \,/\, \iota_{\mathbf{c}}(\mathcal{R}_{\mathbf{c}}) \tag{8.9}$$

and write

$$\pi_{\mathbf{c}}\colon V_{\mathbf{c}} \longrightarrow Y_{\mathbf{c}} \tag{8.10}$$

for the quotient map. According to [43, (7.6)] we may identify $Y_{\mathbf{c}}$ with the dual group of $\mathcal{R}_{\mathbf{c}}$, i.e.

$$Y_{\mathbf{c}} = \widehat{\mathcal{R}_{\mathbf{c}}}. \tag{8.11}$$

If every c_i, $i = 1, \dots, d$, is a unit in $\mathfrak{o}_K$ then $S_{\mathbf{c}} = P_\infty^{(K)}$ and

$$V_{\mathbf{c}} \cong \mathbb{R}^{r(K)}, \qquad Y_{\mathbf{c}} \cong \mathbb{T}^{r(K)}, \tag{8.12}$$

where

$$r(K) = [K : \mathbb{Q}] = |\{v \in P_\infty^{(K)} : K_v = \mathbb{R}\}| + 2|\{v \in P_\infty^{(K)} : K_v = \mathbb{C}\}|. \tag{8.13}$$

In general,

$$c_i \in \mathcal{R}_{\mathbf{c}}^\times = \{a \in \mathcal{R}_{\mathbf{c}} : a^{-1} \in \mathcal{R}_{\mathbf{c}}\} \tag{8.14}$$

is a unit in $\mathcal{R}_{\mathbf{c}}$ for every $1 \le i \le d$. We put, for every $\mathbf{n} = (n_1, \dots, n_d) \in \mathbb{Z}^d$,

$$\mathbf{c}^{\mathbf{n}} = c_1^{n_1} \cdots c_d^{n_d}, \tag{8.15}$$

write every $a \in V_{\mathbf{c}}$ as $a = (a_v) = (a_v,\, v \in S)$ with $a_v \in K_v$ for every $v \in S$, and define a $\mathbb{Z}^d$-action $\bar{\beta}_{\mathbf{c}}$ on $V_{\mathbf{c}}$ by setting

$$\bar{\beta}_{\mathbf{c}}^{\mathbf{n}} a = \iota_{\mathbf{c}}(\mathbf{c}^{\mathbf{n}}) a = (\mathbf{c}^{\mathbf{n}} a_v) \tag{8.16}$$

for every $a = (a_v) \in V_{\mathbf{c}}$ and $\mathbf{n} \in \mathbb{Z}^d$. As $\bar{\beta}_{\mathbf{c}}^{\mathbf{n}}(\iota_{\mathbf{c}}(\mathcal{R}_{\mathbf{c}})) = \iota_{\mathbf{c}}(\mathcal{R}_{\mathbf{c}})$ for every $\mathbf{n} \in \mathbb{Z}^d$, $\bar{\beta}_{\mathbf{c}}$ induces an algebraic $\mathbb{Z}^d$-action $\beta_{\mathbf{c}}$ on the compact abelian group $Y_{\mathbf{c}}$ in (8.9) by

$$\beta_{\mathbf{c}}^{\mathbf{n}}(a + \iota_{\mathbf{c}}(\mathcal{R}_{\mathbf{c}})) = \bar{\beta}_{\mathbf{c}}^{\mathbf{n}} a + \iota_{\mathbf{c}}(\mathcal{R}_{\mathbf{c}}) \tag{8.17}$$

for every $\mathbf{n} \in \mathbb{Z}^d$ and $a \in V_{\mathbf{c}}$, whose dual action $\hat{\beta}_{\mathbf{c}} \colon \mathbf{n} \mapsto \hat{\beta}_{\mathbf{c}}^{\mathbf{n}}$ is given by

$$\hat{\beta}_{\mathbf{c}}^{\mathbf{n}} b = \mathbf{c}^{\mathbf{n}} b \tag{8.18}$$

for every $\mathbf{n} \in \mathbb{Z}^d$ and $b \in \mathcal{R}_{\mathbf{c}} = \widehat{Y_{\mathbf{c}}}$ (cf. (8.11)).

We denote by $\eta_{\mathbf{c}} \colon f \mapsto f(\mathbf{c})$ the evaluation map and define the ideal $P_{\mathbf{c}} = \ker \eta_{\mathbf{c}}$. Then

$$R_d / P_{\mathbf{c}} \cong \eta_{\mathbf{c}}(R_d) = \mathbb{Z}[\mathbf{c}^{\pm 1}] = \mathbb{Z}[c_1^{\pm 1}, \dots, c_d^{\pm 1}] \subset \mathcal{R}_{\mathbf{c}}, \tag{8.19}$$

and $\mathcal{R}_{\mathbf{c}}$ is a module over the integral domain $\mathbb{Z}[\mathbf{c}^{\pm 1}]$.

Lemma 8.6. *The $\mathbb{Z}[\mathbf{c}^{\pm 1}]$-module $\mathcal{R}_{\mathbf{c}}$ is equal to $\mathfrak{o}_K[\mathbf{c}^{\pm 1}]$ and is thus finitely generated.*

Proof. The inclusion $\mathfrak{o}_K[\mathbf{c}^{\pm 1}] \subset \mathcal{R}_{\mathbf{c}}$ is obvious. For the reverse inclusion let $x \in \mathcal{R}_{\mathbf{c}}$ and put

$$E_x = \{v \in S_{\mathbf{c}} \cap P_f^{(K)} : |x|_v > 1\}.$$

If $E_x = \varnothing$ then $x \in \mathfrak{o}_K$ and we are done. Now assume that $k \ge 1$ and that $y \in \mathfrak{o}_K[\mathbf{c}^{\pm 1}]$ for every $y \in \mathcal{R}_{\mathbf{c}}$ with $|E_y| < k$. If $|E_x| = k$ and $v \in E_x$, then we can find an $\mathbf{n} \in \mathbb{Z}^d$ with $|\mathbf{c}^{\mathbf{n}}|_v > |x|_v$. By the Chinese remainder theorem there exists $a \in \mathfrak{o}_K$ such that

$$|a|_v = 1 \ \text{ and } \ |a\mathbf{c}^{\mathbf{n}}|_w < 1 \ \text{ for every } \ w \in S_{\mathbf{c}} \smallsetminus \{v\}.$$

Then $x(a\mathbf{c}^{\mathbf{n}})^{-1} \in \mathcal{R}_v$ and, since $\mathfrak{o}_K$ is dense in $\mathcal{R}_v$, we can find $b \in \mathfrak{o}_K$ and $d \in \mathcal{R}_v$ such that

$$x(a\mathbf{c}^{\mathbf{n}})^{-1} = b + d \ \text{ with } \ |d|_v \leq |\mathbf{c}^{\mathbf{n}}|_v^{-1}.$$

This shows that

$$\begin{aligned} &|x - ab\mathbf{c}^{\mathbf{n}}|_v = |ad\mathbf{c}^{\mathbf{n}}|_v \leq 1, \\ &|x - ab\mathbf{c}^{\mathbf{n}}|_w = |x|_w && \text{for } w \in E_x \smallsetminus \{v\}, \\ &|x - ab\mathbf{c}^{\mathbf{n}}|_w \leq 1 && \text{for } w \in P_f^{(K)} \smallsetminus E_x. \end{aligned}$$

Our induction hypothesis implies that $x - ab\mathbf{c}^{\mathbf{n}} \in \mathfrak{o}_K[\mathbf{c}^{\pm 1}]$ and hence that $x \in \mathfrak{o}_K[\mathbf{c}^{\pm 1}]$. By induction, $\mathcal{R}_{\mathbf{c}} \subset \mathfrak{o}_K[\mathbf{c}^{\pm 1}]$, as promised.

Since $\mathfrak{o}_K$ is a finitely generated $\mathbb{Z}$-module, $\mathcal{R}_{\mathbf{c}}$ is finitely generated over $\mathbb{Z}[\mathbf{c}^{\pm 1}]$. □

Let $\mathcal{L} \subset K$ be a finitely generated $\mathbb{Z}[\mathbf{c}^{\pm 1}]$-submodule. We denote by $\hat{\alpha}_{(\mathbf{c},\mathcal{L})}$ the $\mathbb{Z}^d$-action on $\mathcal{L}$ defined by

$$\hat{\alpha}^{\mathbf{n}}_{(\mathbf{c},\mathcal{L})} a = \mathbf{c}^{\mathbf{n}} a \tag{8.20}$$

for every $\mathbf{n} \in \mathbb{Z}^d$ and $a \in \mathcal{L}$ and write $\alpha_{(\mathbf{c},\mathcal{L})}$ for the dual algebraic $\mathbb{Z}^d$-action on

$$X_{\mathcal{L}} = \widehat{\mathcal{L}}. \tag{8.21}$$

Since $K = \mathbb{Q}[\mathbf{c}]$ we can write every $a \in K$ as $a = b/n$ for some $b \in \mathcal{R}_{\mathbf{c}}$ and $n \in \mathbb{Z}$. As $\mathcal{L}$ is assumed to be finitely generated, we can find a common integer $N > 0$ such that $N\mathcal{L} \subset \mathcal{R}_{\mathbf{c}}$. If

$$\hat{\theta}_{\mathcal{L}} \colon \widehat{X_{\mathcal{L}}} = \mathcal{L} \longrightarrow \mathcal{R}_{\mathbf{c}} = \widehat{Y_{\mathbf{c}}} \tag{8.22}$$

is the injective map defined by multiplication with N, then we obtain a dual algebraic factor map

$$\theta_{\mathcal{L}} \colon Y_{\mathbf{c}} \longrightarrow X_{\mathcal{L}} \tag{8.23}$$

between the algebraic $\mathbb{Z}^d$-actions $\beta_{\mathbf{c}}$ and $\alpha_{(\mathbf{c},\mathcal{L})}$.

For the particular choices $\mathcal{L} = \mathcal{R}_{\mathbf{c}}$ and $\mathcal{L} = \mathbb{Z}[\mathbf{c}^{\pm 1}]$ we obtain the actions

$$\begin{aligned} \beta_{\mathbf{c}} &= \alpha_{(\mathbf{c},\mathcal{R}_{\mathbf{c}})} && \text{on } \ Y_{\mathbf{c}} = \widehat{\mathcal{R}_{\mathbf{c}}}, \\ \alpha_{\mathbf{c}} &= \alpha_{(\mathbf{c},\mathbb{Z}[\mathbf{c}^{\pm 1}])} && \text{on } \ X_{\mathbf{c}} = \widehat{\mathbb{Z}[\mathbf{c}^{\pm 1}]}, \end{aligned} \tag{8.24}$$

which will be referred to as the *maximal* and *minimal* irreducible actions associated with the point $\mathbf{c}$. The motivation for this terminology is provided by Proposition 8.15 on page 41 and the fact that every $\mathbb{Z}[\mathbf{c}^{\pm 1}]$-submodule $\mathcal{L} \subset \mathcal{R}_{\mathbf{c}}$ must contain an isomorphic copy of $\mathbb{Z}[\mathbf{c}^{\pm 1}]$.

Proposition 8.7. *For any two nonzero finitely generated $\mathbb{Z}[\mathbf{c}^{\pm 1}]$-modules $\mathcal{L} \subset \mathcal{L}' \subset K$ the module $\mathcal{L}'/\mathcal{L}$ is finite.*

Furthermore the $\mathbb{Z}^d$-action $\beta_{\mathbf{c}}$ on $Y_{\mathbf{c}}$ is irreducible, the factor map $\theta_{\mathfrak{L}}\colon Y_{\mathbf{c}} \longrightarrow X_{\mathfrak{L}}$ in (8.22)–(8.23) *is finite-to-one, and the action $\alpha_{(\mathbf{c},\mathfrak{L})}$ on $X_{\mathfrak{L}}$ is irreducible and finitely equivalent to $\beta_{\mathbf{c}}$.*

For the proof of Proposition 8.7 we need another lemma.

Lemma 8.8. *Let $\mathfrak{o} \subset K$ be a finitely generated subring with identity of the algebraic number field K. Then every nonzero ideal $\mathfrak{J} \subset \mathfrak{o}$ has finite index.*

Proof. Assume that we have already shown that some finitely generated subring $\mathfrak{o} \subset K$ containing 1 has the property that $|\mathfrak{o}/\mathfrak{J}| < \infty$ for every nonzero ideal $\mathfrak{J} \subset \mathfrak{o}$. By assumption $\mathbb{Z} \subset \mathfrak{o}$.

Let $a \in K$ be an algebraic number with primitive minimal polynomial $f(x) \in \mathbb{Z}[x]$, and let $\mathfrak{J} \subset \mathfrak{o}[a]$ be a nonzero ideal. We set $S = \mathfrak{o} \smallsetminus \{0\}$ and consider the number fields $S^{-1}\mathfrak{o} = L$ and $S^{-1}\mathfrak{o}[a] = L[a] = L'$. As $\{0\} \subsetneq S^{-1}\mathfrak{J} \subset L'$, it follows that $S^{-1}\mathfrak{J} = L'$ and $\mathfrak{J} \cap S \neq \{0\}$

By our hypothesis on $\mathfrak{o}$, the nonzero ideal $\mathfrak{J} \cap \mathfrak{o}$ has finite index in $\mathfrak{o}$. We claim that

$$\text{there exists a monic polynomial } h \in \mathbb{Z}[x] \text{ with } h(a) \in \mathfrak{J}. \tag{8.25}$$

Indeed, since $\mathbb{Z} \subset \mathfrak{o}$ and $\mathfrak{J} \cap \mathfrak{o}$ has finite index in $\mathfrak{o}$, there exists a positive integer $n \in \mathfrak{J}$. We denote by $\mathfrak{I} = \langle n, f \rangle \subset \mathbb{Z}[x]$ the ideal generated by the elements $n, f \in \mathbb{Z}[x]$ and assert that

$$\mathfrak{I} \text{ contains a monic polynomial } h. \tag{8.26}$$

By evaluating the generators of $\mathfrak{I}$ at a we conclude that $h(a) \in \mathfrak{J}$, which shows that (8.25) is a consequence of (8.26).

In order to prove (8.26) we first assume that $n = p^e$ is a prime power. We write f as a sum $f = f_1 - pf_2$ with $f_1, f_2 \in \mathbb{Z}[x]$, where the leading coefficient of f_1 is co-prime to p. Multiplication with $a = f_1^{e-1} + f_1^{e-2}pf_2 + \cdots + (pf_2)^{e-1} \in \mathbb{Z}[x]$ gives that $f_1^e - p^e f_2^e \in \mathfrak{I}$. We have thus found polynomials $a, b \in \mathbb{Z}[x]$ such that $h_p' = f_1^e = af + bp^e \in \mathfrak{I}$ has a leading coefficient which is co-prime to p and hence to $n = p^e$. If m is the degree of h_p' we can apply Euclid's algorithm to find integers k, k' such that the leading coefficient of

$$h_p = kh_p' + k'nx^m \in \mathfrak{I} \tag{8.27}$$

is one.

If n contains a product of at least two distinct primes we write $n = p_1^{e_1} \cdots p_k^{e_k}$ for the prime power decomposition of n and use the isomorphism $\mathbb{Z}/n\mathbb{Z} \cong \prod_{j=1}^k \mathbb{Z}/p_j^{e_j}\mathbb{Z}$ to obtain an isomorphism

$$\theta\colon (\mathbb{Z}/n\mathbb{Z})[x] \longrightarrow \prod_{j=1}^{k} (\mathbb{Z}/p_j^{e_j}\mathbb{Z})[x]$$

of the polynomial rings. Denote by $\bar{f} \in R = (\mathbb{Z}/n\mathbb{Z})[x]$ the polynomial obtained by reducing each coefficient of f modulo n and put $\theta(\bar{f}) = (\bar{f}_1, \dots, \bar{f}_k)$ with $\bar{f}_j \in R_j = (\mathbb{Z}/p_j^{e_j}\mathbb{Z})[x]$ for every $j = 1, \dots, k$. The preceding paragraph shows that the principal ideal generated by $\bar{f}_j$ in R_j contains a polynomial $\bar{h}_j$ with leading coefficient 1, i.e. that there exists a $\bar{g}_j \in R_j$ with $\bar{h}_j = \bar{f}_j\bar{g}_j$. The polynomial $g \in R$ with $\theta(g) = (\bar{g}_1, \dots, \bar{g}_k)$ satisfies that $\bar{f}\bar{g} \in R$ has leading coefficient 1. This shows that there exists a $g' \in \mathbb{Z}[x]$ such that the polynomial $h = fg + ng' \in \mathfrak{I}$ has leading coefficient 1 and proves (8.26) and hence (8.25).

If m is the degree of the polynomial h found in (8.25), then

$$\left|\mathfrak{o}[a]/\mathfrak{J}\right| = \left|\mathfrak{o} + a\mathfrak{o} + \dots + a^{m-1}\mathfrak{o}/\mathfrak{J}\right| \leq \left|\mathfrak{o}/\mathfrak{o} \cap \mathfrak{J}\right|^m < \infty.$$

This shows that the ring $\mathfrak{o}[a]$ again has the property that $|\mathfrak{o}[a]/\mathfrak{J}| < \infty$ for every nonzero ideal $\mathfrak{J} \subset \mathfrak{o}[a]$.

The proof of the lemma is completed by induction on the number of generators of the subring $\mathfrak{o}$. □

Proof of Proposition 8.7. This is a slight extension of [42, Theorem 7.1] (cf. [12]).

Let $\mathfrak{L} \subset \mathfrak{L}' \subset K$ be two nonzero finitely generated $\mathbb{Z}[\mathbf{c}^{\pm 1}]$-submodules. Since $\mathfrak{L} \subset K$ is nonzero, $\mathbb{Z}[\mathbf{c}^{\pm 1}]a \subset \mathfrak{L}$ for some nonzero $a \in \mathfrak{L}$. Since $\mathfrak{L}'$ is finitely generated as a $\mathbb{Z}[\mathbf{c}^{\pm 1}]$-module and $\mathfrak{L}' \subset K = \mathbb{Q}[\mathbf{c}]$, we can find $M \in \mathbb{Z}$ such that

$$\mathbb{Z}[\mathbf{c}^{\pm 1}]a \subset \mathfrak{L} \subset \mathfrak{L}' \subset \frac{1}{M}\mathbb{Z}[\mathbf{c}^{\pm 1}].$$

Lemma 8.8 shows that $\mathbb{Z}[\mathbf{c}^{\pm 1}]a$ has finite index in $\frac{1}{M}\mathbb{Z}[\mathbf{c}^{\pm 1}]$, which completes the proof of the first statement of the proposition.

For the second statement we consider the action $\beta_{\mathbf{c}}$ on $Y_{\mathbf{c}}$. If $Z \subset Y_{\mathbf{c}}$ is a proper invariant closed subgroup, then the annihilator $\mathfrak{L} = Z^{\perp} \subset \mathfrak{R}_{\mathbf{c}}$ is a nonzero $\mathbb{Z}[\mathbf{c}^{\pm 1}]$-submodule. Therefore has $\mathfrak{L}$ finite index in $\mathfrak{R}_{\mathbf{c}}$ and Z is finite. This shows that $\beta_{\mathbf{c}}$ is irreducible. Proposition 8.3 implies the remaining statements. □

Our next theorem shows that every irreducible algebraic $\mathbb{Z}^d$-action α on a compact abelian connected group is of the form $\alpha_{(\mathbf{c},\mathfrak{L})}$ described in (8.20)–(8.21).

Theorem 8.9. *Suppose that $d \geq 1$, and that α is an algebraic $\mathbb{Z}^d$-action on an infinite compact connected abelian group X. Then α is irreducible if and only if it is finitely equivalent to each of the irreducible algebraic $\mathbb{Z}^d$-actions $\alpha_{\mathbf{c}}$ on $X_{\mathbf{c}}$ and $\beta_{\mathbf{c}}$ on $Y_{\mathbf{c}}$ for some $\mathbf{c} = (c_1, \dots, c_d) \in (\bar{\mathbb{Q}}^{\times})^d$. Furthermore there exists a finitely generated $\mathbb{Z}[\mathbf{c}^{\pm 1}]$-submodule $\mathfrak{L} \subset K$ such that α is algebraically conjugate to the $\mathbb{Z}^d$-action $\alpha_{(\mathbf{c},\mathfrak{L})}$ on $X_{\mathfrak{L}}$ defined in*

(8.20)–(8.21). *Without loss of generality one may assume in addition that* $\mathcal{L} \subset \mathcal{R}_{\mathbf{c}}$.

Proof. Let α be an irreducible algebraic action on the compact connected abelian group X with dual module $M = \widehat{X}$ and let $\mathfrak{p}$ be an associated prime ideal for M. There exists $a \in M$ such that

$$\{f \in R_d : f \cdot a = 0\} = \mathfrak{p}.$$

This shows that the map $f + \mathfrak{p} \mapsto \hat{\theta}(f) = fa$ from $R_d/\mathfrak{p}$ to M is an injective module homomorphism. By duality, $\theta\colon X \longrightarrow X_{R_d/\mathfrak{p}}$ a factor map. From Proposition 8.3 we see that θ is finite-to-one and the action $\alpha_{R_d/\mathfrak{p}}$ on $X_{R_d/\mathfrak{p}}$ is irreducible.

As X is connected, the dual module is torsion-free as an abelian group and $\mathfrak{p}$ does not contain a constant. Hilbert's Nullstellensatz shows that there exists a point

$$\mathbf{c} \in V(\mathfrak{p}) = \{\mathbf{c}' \in \overline{\mathbb{Q}}^{\times} : f(\mathbf{c}') = 0 \text{ for every } f \in \mathfrak{p}\}.$$

Let $\pi\colon R_d/\mathfrak{p} \longrightarrow R_d/\mathfrak{p}_{\mathbf{c}}$ be the canonical projection map, where

$$\mathfrak{p}_{\mathbf{c}} = \{f \in R_d : f(\mathbf{c} = 0)\}. \tag{8.28}$$

Then $\hat{\pi}\colon X_{\mathbf{c}} \longrightarrow X$ is injective. As $\alpha_{R_d/\mathfrak{p}}$ is irreducible by the previous paragraph, every non-trivial closed α-invariant subgroup must be finite and $\widehat{\pi}$ must be surjective. By duality, π is injective and $\mathfrak{p} = \mathfrak{p}_{\mathbf{c}}$.

Proposition 8.3 also shows that the actions $\alpha_{R_d/\mathfrak{p}_{\mathbf{c}}}$ and α are finitely equivalent. Let $\phi : X_{\mathbf{c}} \longrightarrow X$ be a factor map. The dual homomorphism $\hat{\phi}\colon M \longrightarrow R_d/\mathfrak{p}_{\mathbf{c}} \cong \mathbb{Z}[\mathbf{c}^{\pm 1}]$ of ϕ is injective. Hence $\mathcal{L} = \hat{\phi}(M) \subset \mathbb{Z}[\mathbf{c}^{\pm 1}] \subset K$ is a nonzero finitely generated $\mathbb{Z}[\mathbf{c}^{\pm 1}]$-submodule and the $\mathbb{Z}^d$-actions α and $\alpha_{(\mathbf{c},\mathcal{L})}$ are algebraically conjugate. □

So far we have concentrated on the dual modules of irreducible algebraic $\mathbb{Z}^d$-actions. By using the locally compact group $V_{\mathbf{c}}$ in (8.7) we can describe explicitly the actual actions and the groups carrying them.

Corollary 8.10. *Let $d \geq 1$, and let α be an irreducible $\mathbb{Z}^d$-action on an infinite compact connected abelian group X. We denote by $\mathbf{c} \in (\bar{\mathbb{Q}}^{\times})^d$ the point described in Theorem* 8.9 *and define the ring $\mathcal{R}_{\mathbf{c}} \subset K$, the set $S_{\mathbf{c}} \subset P^{(K)}$, the algebra $V_{\mathbf{c}} = \prod_{v \in S} K_v$ and the embedding $\iota_{\mathbf{c}}\colon K \longrightarrow V_{\mathbf{c}}$ as in* (8.6)–(8.7). *Then there exists a finitely generated $\mathbb{Z}[\mathbf{c}^{\pm 1}]$-submodule $\mathcal{K} \subset K$ such that α is algebraically conjugate to the $\mathbb{Z}^d$-action $\alpha'_{(\mathbf{c},\mathcal{K})}$ on the compact abelian group*

$$X'_{\mathcal{K}} = V_{\mathbf{c}}/\iota_S(\mathcal{K}), \tag{8.29}$$

defined as in (8.17) *by*

$$\alpha'^{\mathbf{n}}_{(\mathbf{c},\mathcal{K})}(a + \iota_S(\mathcal{K})) = \bar{\beta}^{\mathbf{n}}_{(\mathbf{c},S)} a + \iota_S(\mathcal{K}) \tag{8.30}$$

for every $\mathbf{n} \in \mathbb{Z}^d$ *and* $a \in V_{\mathbf{c}}$*. Furthermore one can always assume that* $\mathcal{K} \subset \mathcal{R}_{\mathbf{c}}$*.*

Conversely, if $\mathcal{K} \subset K$ *is a nonzero finitely generated* $\mathbb{Z}[\mathbf{c}^{\pm 1}]$*-submodule, then the* $\mathbb{Z}^d$*-action* $\alpha'_{(\mathbf{c},\mathcal{K})}$ *on the compact group* $X'_{\mathcal{K}}$ *in* (8.29)–(8.30) *is irreducible and finitely equivalent to* $\alpha_{\mathbf{c}}$ *and* $\beta_{\mathbf{c}}$*.*

Proof. According to Theorem 8.9 there exists a finite-to-one factor map $\phi\colon Y_{\mathbf{c}} \longrightarrow X$. The map ϕ induces a continuous surjective group homomorphism $\psi\colon V_{\mathbf{c}} \longrightarrow X$ with $\psi \circ \bar{\beta}_{\mathbf{c}}^{\mathbf{n}} = \alpha^{\mathbf{n}} \circ \psi$ for every $\mathbf{n} \in \mathbb{Z}^d$, whose kernel $\mathcal{K}' = \ker \psi$ is invariant under the $\mathbb{Z}^d$-action $\bar{\beta}_{\mathbf{c}}$ in (8.16) and contains $\iota_S(\mathcal{R}_{\mathbf{c}})$ as a subgroup of finite index.

Choose an integer $N \geq 1$ with $\mathcal{K}'' = N\mathcal{K}' \subset \iota_S(\mathcal{R}_{\mathbf{c}})$ and denote by $\mathcal{K} \subset \mathcal{R}_{\mathbf{c}}$ the $\eta_{\mathbf{c}}(R_d)$-submodule satisfying $\iota_S(\mathcal{K}) = \mathcal{K}''$. If $m_N\colon V_{\mathbf{c}} \longrightarrow V_{\mathbf{c}}$ denotes multiplication by N, then

$$X \cong V_{\mathbf{c}}/\mathcal{K}' \cong m_N(V_{\mathbf{c}})/m_N(\mathcal{K}'') \cong V_{\mathbf{c}}/\mathcal{K}'' \cong V_{\mathbf{c}}/\iota_S(\mathcal{K}) = X'_{\mathcal{K}},$$

and the isomorphism of X and $X'_{\mathcal{K}}$ carries the $\mathbb{Z}^d$-action α to $\alpha'_{(\mathbf{c},\mathcal{K})}$.

The other statements are clear from Proposition 8.7, since $\mathcal{K}$ has finite index in $\mathcal{R}_{\mathbf{c}}$. □

Theorem 8.9 and Corollary 8.10 give a variety of representations of irreducible algebraic $\mathbb{Z}^d$-action on infinite compact connected abelian groups. For a fixed $\mathbf{c}$ all these representations are finitely equivalent. Theorem 8.13 will show that these representations are sometimes, but not always, algebraically conjugate.

We can give an easy characterization of those actions which are algebraically conjugate to the minimal actions $\alpha_{\mathbf{c}}$ (cf. (8.24)).

Definition 8.11. Let α be an algebraic $\mathbb{Z}^d$-action on a compact abelian group X. The dual group $\widehat{X}$ of X is *cyclic* under the dual action $\hat{\alpha}$ of α (or α has *cyclic dual*) if there exists a character $a \in \widehat{X}$ such that $\widehat{X}$ is generated by the set $\{\hat{\alpha}^{\mathbf{n}} a : \mathbf{n} \in \mathbb{Z}\}$.

Proposition 8.12. *Let* $d \geq 1$*, and let* α *be an irreducible algebraic* $\mathbb{Z}^d$*-action on an infinite compact connected abelian group* X*. If* $\mathbf{c} \in \bar{\mathbb{Q}}^{\times}$ *is the point appearing in Theorem* 8.9*, then* α *is algebraically conjugate to* $\alpha_{\mathbf{c}}$ *if and only if* α *has cyclic dual.*

Proof. The action $\alpha_{\mathbf{c}}$ has cyclic dual, since the element $1 \in \mathbb{Z}[\mathbf{c}^{\pm 1}] = \widehat{X_{\mathbf{c}}}$ is cyclic under $\hat{\alpha}_{\mathbf{c}}$.

If α and $\alpha_{\mathbf{c}}$ are algebraically conjugate, there exists a continuous group isomorphism $\phi\colon X \longrightarrow X_{R_d/\mathfrak{p}_c}$ with $\phi \circ \alpha^{\mathbf{n}} = \alpha_{\mathbf{c}}^{\mathbf{n}} \circ \phi$ for every $\mathbf{n} \in \mathbb{Z}^d$, and the dual isomorphism $\hat{\phi}\colon R_d/\mathfrak{p}_c \longrightarrow \widehat{X}$ sends $1 \in \mathbb{Z}[\mathbf{c}^{\pm 1}]$ to a cyclic element $a \in \widehat{X}$ for $\hat{\alpha}$.

Conversely, if $a \in \widehat{X}$ is a cyclic element of $\hat{\alpha}$, then the map

$$h(\mathbf{c}) \mapsto h(\hat{\alpha})(a) = \sum_{\mathbf{n} \in \mathbb{Z}^d} h_{\mathbf{n}} \widehat{\alpha^{\mathbf{n}}} a$$

for $h = \sum_{\mathbf{n} \in \mathbb{Z}^d} h_{\mathbf{n}} u^{\mathbf{n}} \in R_d$ induces a module-isomorphism $\hat{\psi}\colon \mathbb{Z}[\mathbf{c}^{\pm 1}] \longrightarrow \widehat{X}$ whose dual $\psi\colon X \longrightarrow X_{R_d/P} = \widehat{X_{R_d/P}}$ is an algebraic conjugacy of α and $\alpha_{\mathbf{c}}$. □

We continue by describing the connection between algebraic conjugacy classes of irreducible algebraic $\mathbb{Z}^d$-actions and ideal classes in algebraic number fields. This will give us a collection of nonconjugate but finitely equivalent algebraic actions.

Every nonzero ideal $\mathfrak{I} \subset \mathcal{R}_S$ is called an *S-integral ideal* of K and has finite index in $\mathcal{R}_S$ by Lemma 8.8. Two S-integral ideals $\mathfrak{I}, \mathfrak{J}$ of K lie in the same *ideal class* if there exists an element $a \in K$ with $a\mathfrak{I} = \mathfrak{J}$.

Theorem 8.13. *Suppose that K is an algebraic number field, $\mathbf{c} \in (K^\times)^d$ a vector of nonzero algebraic numbers with $K = \mathbb{Q}(\mathbf{c})$, and let $S_{\mathbf{c}} \subset P^{(K)}$ be the set of places defined by (8.6). Then the $\mathbb{Z}^d$-action $\alpha_{(\mathbf{c},\mathfrak{I})}$ on $X_{\mathfrak{I}} = \hat{\mathfrak{I}}$ is irreducible for every nonzero ideal $\mathfrak{I} \subset \mathcal{R}_{\mathbf{c}}$. Furthermore, if $\mathfrak{I}, \mathfrak{J}$ are nonzero ideals in $\mathcal{R}_{\mathbf{c}}$, then $\alpha_{(\mathbf{c},\mathfrak{I})}$ and $\alpha_{(\mathbf{c},\mathfrak{J})}$ are finitely equivalent, and $\alpha_{(\mathbf{c},\mathfrak{I})}$ and $\alpha_{(\mathbf{c},\mathfrak{J})}$ are algebraically conjugate if and only if $\mathfrak{I}$ and $\mathfrak{J}$ lie in the same ideal class.*

Proof. Theorem 8.9 shows that the action $\alpha_{(\mathbf{c},\mathfrak{I})}$ is irreducible.

If $\mathfrak{I}, \mathfrak{J}$ are nonzero ideals in $\mathcal{R}_{\mathbf{c}}$, then $\alpha_{(\mathbf{c},\mathfrak{I})}$ and $\alpha_{(\mathbf{c},\mathfrak{J})}$ are obviously algebraically conjugate whenever $\mathfrak{I}$ and $\mathfrak{J}$ lie in the same ideal class.

Conversely, if $\phi\colon X_{\mathfrak{I}} \longrightarrow X_{\mathfrak{J}}$ is an algebraic conjugacy of $\alpha_{(\mathbf{c},\mathfrak{I})}$ and $\alpha_{(\mathbf{c},\mathfrak{J})}$, then the dual map $\hat{\phi}\colon \mathfrak{J} \longrightarrow \mathfrak{I}$ is an $\eta_{\mathbf{c}}(R_d)$-module isomorphism (cf. (8.19)), i.e. $\hat{\phi}(f(c)a) = f(c)\hat{\phi}(a)$ for every $f \in R_d$ and $a \in \mathfrak{J}$. Since K is the field of fractions of $\mathbb{Z}[\mathbf{c}^{\pm 1}]$ we can extend $\hat{\phi}$ to a K-linear map $\hat{\psi}\colon K \longrightarrow K$ by fixing a nonzero element $a \in \mathfrak{J}$ and setting $\hat{\psi}\big(\frac{f(c)}{g(c)}a\big) = \frac{f(c)}{g(c)}\hat{\phi}(a)$ for every $f, g \in R_d$ with $g(c) \neq 0$. An elementary calculation shows that $\hat{\psi}\big(\frac{f(c)}{g(c)}\big) = \hat{\phi}\big(\frac{f(c)}{g(c)}\big)$ whenever $\frac{f(c)}{g(c)} \in \mathfrak{J}$. If $b = \hat{\psi}(1)$, then the K-linearity of $\hat{\psi}$ guarantees that $\hat{\psi}(a) = ba$ for every $a \in K$, and hence that $\mathfrak{J} = \hat{\phi}(\mathfrak{I}) = \hat{\psi}(\mathfrak{I}) = b\mathfrak{I}$. This shows that $\mathfrak{I}$ and $\mathfrak{J}$ lie in the same ideal class. □

We end this discussion of irreducible actions with a few words about centralizers of such actions.

Definition 8.14. Let α be an algebraic $\mathbb{Z}^d$-action on a compact abelian group X. The *algebraic centralizer* $\mathcal{C}_0(\alpha)$ is the group of all continuous group automorphisms of X which commute with α.

The *affine centralizer* $\mathcal{C}_{\mathrm{aff}}(\alpha)$ is the group of all affine bijections of X which commute with α, and is of the form $\mathcal{C}_{\mathrm{aff}}(\alpha) = \mathcal{C}_0(\alpha) \times \mathrm{Fix}(\alpha)$, where $\mathrm{Fix}(\alpha)$ is the group of fixed points of α.

The *measurable centralizer* $\mathcal{C}_{\lambda_X}(\alpha)$ is the group of all Haar measure preserving bijective Borel maps $\phi\colon X \longrightarrow X$ which commute with α modulo λ_X.

If α is an irreducible and mixing algebraic $\mathbb{Z}^d$-action with $d \geq 2$, then Theorem 8.4 implies that $C_{\lambda_X}(\alpha) = \mathcal{C}_{\mathrm{aff}}(\alpha) = \mathcal{C}_0(\alpha) \times \mathrm{Fix}(\alpha)$. Hence both the set of fixed points and the algebraic centralizer of α are invariant under measurable conjugacy, which is a good reason for being interested in these objects.

Proposition 8.15. *Let α be an irreducible algebraic $\mathbb{Z}^d$-action on a compact connected abelian group X, and let $\mathbf{c} = (c_1, \dots, c_d) \in (\bar{\mathbb{Q}}^\times)^d$ be the point described in Theorem 8.9. If $\mathcal{R}_{\mathbf{c}} \subset K = \mathbb{Q}(\mathbf{c})$ is the ring of $S_{\mathbf{c}}$-integers in $K = \mathbb{Q}(\mathbf{c})$, then*

$$\mathcal{C}_0(\alpha) \subset \mathcal{C}_0(\beta_{\mathbf{c}}) \cong \mathcal{R}_{\mathbf{c}}^\times \cong F \times \mathbb{Z}^{|S_{\mathbf{c}}|-1},$$

where $\mathcal{R}_{\mathbf{c}}$ is the ring of units in $\mathcal{R}_{\mathbf{c}}$, F is the finite cyclic group consisting of all roots of unity on K and $\beta_{\mathbf{c}}$ is the $\mathbb{Z}^d$-action on $Y_{\mathbf{c}} = \widehat{\mathcal{R}_{\mathbf{c}}}$ defined in (8.24).

Proof. Multiplication by any $a \in \mathcal{R}_{\mathbf{c}}^\times$ is an automorphism of $\mathcal{R}_{\mathbf{c}}$ and induces a dual automorphism of $Y_{\mathbf{c}}$ which commutes with the $\mathbb{Z}^d$-action $\beta_{\mathbf{c}}$. In order to see that every automorphism γ of $Y_{\mathbf{c}}$ commuting with $\beta_{\mathbf{c}}$ arises in this manner we consider the dual automorphism $\hat{\gamma}$ of $\mathcal{R}_{\mathbf{c}}$ and set $a = \hat{\gamma}(1)$. Since $\hat{\gamma}$ commutes with multiplication by $\mathbf{c}^{\mathbf{n}}$ for every $\mathbf{n} \in \mathbb{Z}^d$ and hence with multiplication by any element in $\mathbb{Z}[\mathbf{c}^{\pm 1}]$, $\hat{\gamma}$ coincides with multiplication by a on $\mathbb{Z}[\mathbf{c}^{\pm 1}] \subset \mathcal{R}_{\mathbf{c}}$. We use Lemma 8.6 and Proposition 8.7 to find an integer $M \geq 1$ with $M\mathcal{R}_{\mathbf{c}} \subset \mathbb{Z}[\mathbf{c}^{\pm 1}]$ and conclude that $\hat{\gamma}$ coincides with multiplication by a on $\mathcal{R}_{\mathbf{c}}$. As $\hat{\gamma}$ is invertible we find that $a \in \mathcal{R}_{\mathbf{c}}^\times$ and hence that $\mathcal{C}_0(\beta_{\mathbf{c}}) \cong \mathcal{R}_{\mathbf{c}}^\times \cong F \times \mathbb{Z}^{|S_{\mathbf{c}}|-1}$, where the second isomorphism is proved in [34, Theorem 3.5].

If an algebraic $\mathbb{Z}^d$-action α on a compact abelian group X is finitely equivalent to $\beta_{\mathbf{c}}$, then Theorem 8.9 shows that $\alpha = \alpha_{(\mathbf{c},\mathcal{L})}$ and $X = X_{\mathcal{L}} = \widehat{\mathcal{L}}$ for some $\mathbb{Z}[\mathbf{c}^{\pm 1}]$-submodule $\mathcal{L} \subset \mathcal{R}_{\mathbf{c}}$. Suppose that γ is an automorphism of X which commutes with α. Then the same proof as above shows that there exists an element $a \in K^\times$ such that $\hat{\gamma}$ coincides with multiplication by a on $\mathcal{L} = \widehat{X}$. If $a \notin \mathcal{R}_{\mathbf{c}}$ we obtain a contradiction to the finiteness of $\mathcal{R}_{\mathbf{c}}/\mathcal{L}$ proved in Proposition 8.7. This shows that $\mathcal{C}_0(\alpha) \subset \mathcal{C}_0(\beta_{\mathbf{c}}) \cong \mathcal{R}_{\mathbf{c}}$, as claimed. □

We end the discussion in this subsection with a list of examples, taken from [18].

Example 8.16. Let K be a totally real cubic field given by the irreducible polynomial $f(x) = x^3 + 3x^2 - 6x + 1$, i.e. $K = \mathbb{Q}(\gamma)$ where γ is one of its roots. The algebraic integers $\gamma_1 = \gamma$ and $\gamma_2 = 2 - 4\gamma - \gamma^2$ are units with $f(\gamma_1) = f(\gamma_2) = 0$. The smallest subring in K containing γ_1 and γ_2 is $\mathbb{Z}[\gamma_1, \gamma_2] = \mathbb{Z}[\gamma]$. A basis in fundamental units is $\epsilon = \frac{\gamma^2+5\gamma+1}{3}$ and $\epsilon - 1$, hence the ring of units $\mathcal{U}_K$ is not contained in $\mathbb{Z}[\gamma]$.

With respect to the basis $\{1, \gamma, \gamma^2\}$ in $\mathbb{Z}[\gamma]$, multiplication by γ_1 and γ_2 is given by the matrices

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 6 & -3 \end{pmatrix}, \qquad B = \begin{pmatrix} 2 & -4 & -1 \\ 1 & -4 & -1 \\ 1 & -5 & -1 \end{pmatrix},$$

respectively (if acting from the right on row–vectors).

With respect to the basis $\{-\frac{2}{3} + \frac{5}{3}\gamma + \frac{1}{3}\gamma^2, -\frac{1}{3} + \frac{7}{3}\gamma + \frac{2}{3}\gamma^2\}$ in $\mathfrak{o}_K$, multiplications by γ_1 and γ_2 are given by the matrices

$$A' = \begin{pmatrix} 1 & 2 & -1 \\ -1 & -2 & 2 \\ 2 & 5 & -2 \end{pmatrix}, \qquad B' = \begin{pmatrix} 1 & -1 & -1 \\ -1 & -2 & -1 \\ -1 & -4 & -2 \end{pmatrix}.$$

We have $A' = VAV^{-1}$, $B' = VBV^{-1}$ for $V = \begin{pmatrix} 2 & -2 & -1 \\ 0 & -3 & 0 \\ 1 & -4 & -2 \end{pmatrix}$. Since A is a companion matrix of f, the $\mathbb{Z}^2$-action α generated by A and B has a cyclic element in $\mathbb{Z}^3$. If A' also had a cyclic element $\mathbf{m} = (m_1, m_2, m_3) \in \mathbb{Z}^3$, then the vectors

$$\mathbf{m} = (m_1, m_2, m_3), \quad \mathbf{m}A' = (m_1 - m_2 + 2m_3, 2m_1 - 2m_2 + 5m_3, -m_1 + 2m_2 - 2m_3)$$
$$\mathbf{m}(A')^2 = (-3m_1 + 5m_2 - 7m_3, -7m_1 + 12m_2 - 16m_3, 5m_1 - 7m_2 + 12m_3),$$

would have to generate $\mathbb{Z}^3$ or, equivalently

$$\begin{aligned} \det &\begin{pmatrix} m_1 & m_2 & m_3 \\ m_1 - m_2 + 2m_3 & 2m_1 - 2m_2 + 5m_3 & -m_1 + 2m_2 - 2m_3 \\ -3m_1 + 5m_2 - 7m_3 & -7m_1 + 12m_2 - 16m_3 & 5m_1 - 7m_2 + 12m_3 \end{pmatrix} \\ &= 3m_1^3 + 18m_1^2 m_3 - 9m_1 m_2^2 - 9m_1 m_2 m_3 \\ &\qquad + 27m_1 m_3^2 + 3m_2^3 - 9m_2 m_3^2 + 3m_3^3 = 1. \end{aligned} \tag{8.31}$$

This contradiction shows that A' has no cyclic vector, and since $B' = 2 - 4A' - A'^2$, the action α' generated by A' and B' does not have a cyclic dual. By Theorem 8.4 the finitely equivalent actions α and α' are not measurably conjugate.

Example 8.17. Consider the totally real cubic field K given by the irreducible polynomial $f(x) = x^3 - 7x^2 + 11x - 1$. Then $K = \mathbb{Q}(\gamma)$ where γ is one of its roots. In this field the ring of integers $\mathfrak{o}_K$ has basis $\{1, \gamma, \frac{1}{2}\gamma^2 + \frac{1}{2}\}$ and hence $[\mathfrak{o}_K : \mathbb{Z}[\gamma]] = 2$. The fundamental units in $\mathfrak{o}_K$ are $\{\frac{1}{2}\gamma^2 - 2\gamma + \frac{1}{2}, \gamma - 2\}$. We choose the units $\gamma = \gamma_1 = (\frac{1}{2}\gamma^2 - 2\gamma + \frac{1}{2})^2$ and $\gamma_2 = \gamma - 2$ which are contained in both orders, $\mathfrak{o}_K$ and $\mathbb{Z}[\gamma]$.

In $\mathbb{Z}[\gamma]$ we consider the basis $\{1,\gamma,\gamma^2\}$ relative to which the multiplication by γ_1 is represented by the companion matrix $A = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -11 & 7 \end{smallmatrix}\right)$ and multiplication by γ_2 is represented by the matrix $B = \left(\begin{smallmatrix} -2 & 1 & 0 \\ 0 & -2 & 1 \\ 1 & -11 & 5 \end{smallmatrix}\right)$.

For $\mathfrak{o}_K$ with the basis $\{1,\gamma,\frac{1}{2}\gamma^2+\frac{1}{2}\}$, multiplication by γ_1 and γ_2 is represented by the matrices

$$A' = \left(\begin{smallmatrix} 0 & 1 & 0 \\ -1 & 0 & 2 \\ -3 & -5 & 7 \end{smallmatrix}\right), \qquad B' = \left(\begin{smallmatrix} -2 & 1 & 0 \\ -1 & -2 & 2 \\ -3 & -5 & 5 \end{smallmatrix}\right),$$

respectively. Here α and α' are not algebraically conjugate since A is cyclic on $\mathbb{Z}^3$, whereas A' not (the determinant corresponding to (8.31) is equal to

$$\begin{aligned} &2m_1^3 + 4m_1^2m_2 + 22m_1m_2^2 - 8m_2^3 + 30m_1^2m_3 \\ &\qquad + 138m_1m_2m_3 - 12m_2^2m_3 + 82m_1m_3^2 + 46m_2m_3^2 + 34m_3^3 \end{aligned}$$

and is thus divisible by 2). A second reason for non-conjugacy is that the action α has 2 fixed points on $\mathbb{T}^3$: $(0,0,0)$ and $(\frac{1}{2},\frac{1}{2},\frac{1}{2})$, while α' has 4 fixed points: $(0,0,0)$, $(\frac{1}{2},\frac{1}{2},\frac{1}{2})$, $(\frac{1}{2},\frac{1}{2},0)$, and $(0,0,\frac{1}{2})$.

For our final set of examples we introduce a definition.

Definition 8.18. Let K be an algebraic number field, S a finite number of places of K containing all infinite places, and let $\mathcal{R}_S$ be defined as in (8.8) with S replacing $S_{\mathbf{c}}$. A d-tuple $\mathbf{c}=(c_1,\dots,c_d)$ in $\mathcal{R}_S^\times$ is a *free S-unit system* if it generates a free abelian group, i.e. if the equation $\mathbf{c}^{\mathbf{n}} = c_1^{n_1}\cdots c_d^{n_d} = 1$ with $\mathbf{n}=(n_1,\dots,n_d)\in\mathbb{Z}^d$ implies that $\mathbf{n}=\mathbf{0}$.

A free S-unit system $\mathbf{c}=(c_1,\dots,c_d)$ is *fundamental* if every $a\in\mathcal{R}_S^\times$ can be written uniquely as $a = uc_1^{k_1}\cdots c_d^{k_d}$ with $u\in F$ and $k_1,\dots,k_d\in\mathbb{Z}$, where F is the finite cyclic group consisting of all roots of unity in K.

Examples 8.19. (a) Let $K=\mathbb{Q}(\gamma)$, where γ has minimal polynomial $f(x) = x^3-2x^2-8x-1$. In this field the ring of integers is equal to $\mathfrak{o}_K = \mathbb{Z}[\gamma]$ with fundamental units $\gamma_1=\gamma$ and $\gamma_2=\gamma+2$. Two actions are constructed with this set of units on two different lattices, $\mathfrak{o}_K$ with the basis $\{1,\gamma,\gamma^2\}$, representing the principal ideal class, and $\mathfrak{L}$ with the basis $\{2,1+\gamma,1+\gamma^2\}$, representing to the second ideal class. Notice that the units γ_1 and γ_2 do not belong to $\mathfrak{L}$, but $\mathfrak{L}$ is a $\mathbb{Z}[\gamma]$-module. The first action α is generated by the matrices

$$A = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 8 & 2 \end{smallmatrix}\right), \qquad B = \left(\begin{smallmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 1 & 8 & 4 \end{smallmatrix}\right),$$

which represent multiplication by γ_1 and γ_2, respectively, on $\mathfrak{o}_K$. The second action α' is generated by matrices

$$A' = \left(\begin{smallmatrix} -1 & 2 & 0 \\ -1 & 1 & 1 \\ -5 & 9 & 2 \end{smallmatrix}\right), \qquad B' = \left(\begin{smallmatrix} 1 & 2 & 0 \\ -1 & 3 & 1 \\ -5 & 9 & 5 \end{smallmatrix}\right),$$

which represent multiplication by γ_1 and γ_2, respectively, on $\mathfrak{L}$ in the given basis. By Proposition 8.7 these actions are finitely equivalent, but by Theorem 8.13 they are not algebraically and hence not measurably conjugate.

The action α has 2 fixed points on $\mathbb{T}^3$: $(0,0,0)$ and $(\frac{1}{2},\frac{1}{2},\frac{1}{2})$, while the action α' has a single fixed point $(0,0,0)$. This gives another proof that the actions are not measurably conjugate.

(b) This example is obtained from a totally real cubic field with class number 3, Galois group S_3, and discriminant 2597. It can be represented as $K = \mathbb{Q}(\gamma)$ where γ is a unit in K with minimal polynomial $f(x) = x^3 - 2x^2 - 8x + 1$. In this field the ring of integers $\mathfrak{o}_K = \mathbb{Z}[\gamma]$ and the fundamental units are $\gamma_1 = \gamma$ and $\gamma_2 = \gamma + 2$. Three actions are constructed with this set of units on three different lattices, $\mathfrak{o}_K$ with the basis $\{1, \gamma, \gamma^2\}$, representing the principal ideal class, $\mathfrak{L}$ with the basis $\{2, 1+\gamma, 1+\gamma^2\}$ representing the second ideal class, and $\mathfrak{L}^2$ with the basis $\{4, 3+\gamma, 3+\gamma^2\}$ representing the third ideal class.

Multiplication by γ_1 and γ_2 generates the following three finitely equivalent actions which are not algebraically conjugate by Theorem 8.13, and therefore not measurably conjugate:

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 8 & 2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ -1 & 8 & 4 \end{pmatrix};$$

$$A' = \begin{pmatrix} -1 & 2 & 0 \\ -1 & 1 & 1 \\ -6 & 9 & 2 \end{pmatrix} \quad \text{and} \quad B' = \begin{pmatrix} 1 & 2 & 0 \\ -1 & 3 & 1 \\ -6 & 9 & 4 \end{pmatrix};$$

$$A'' = \begin{pmatrix} -3 & 4 & 0 \\ -3 & 3 & 1 \\ -10 & 11 & 2 \end{pmatrix} \quad \text{and} \quad B'' = \begin{pmatrix} -1 & 4 & 0 \\ -3 & 5 & 1 \\ -10 & 11 & 4 \end{pmatrix}.$$

Each action has 2 fixed point in $\mathbb{T}^3$, $(0,0,0)$ and $(\frac{1}{2},\frac{1}{2},\frac{1}{2})$, but they are distinguished by Theorem 8.13.

(c) Let $K = \mathbb{Q}(\gamma)$ with class number 1 and discriminant 1304 given by the polynomial $x^3 - x^2 - 11x - 1$. For this field we have $[\mathfrak{o}_K : \mathbb{Z}(\gamma)] = 2$. Generators in $\mathfrak{o}_K$ can be taken to be $\{1, \gamma, \beta = \frac{\gamma^2+1}{2}\}$. Fundamental units are $\gamma_1 = -\gamma$, $\gamma_2 = -5 + 14\gamma + 10\beta = 14\gamma + 5\gamma^2 \in \mathbb{Z}[\gamma]$. Thus the whole group of units lies in $\mathbb{Z}[\gamma]$. To construct the generators for two non-conjugate action α and α' we consider multiplication by γ_1 and γ_2 in the bases $\{1, \alpha, \alpha^2\}$ and $\{1, \alpha, \beta\}$, respectively. The resulting matrices are:

$$A = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & -1 \\ 1 & 11 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 14 & 5 \\ 5 & 55 & 19 \\ 19 & 214 & 74 \end{pmatrix},$$

$$A' = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & -2 \\ 0 & -6 & -1 \end{pmatrix} \quad B = \begin{pmatrix} -5 & 14 & 10 \\ -14 & 55 & 38 \\ -30 & 114 & 79 \end{pmatrix}.$$

The first action has only one fixed point, the origin; the second has four fixed points $(0,0,0)$, $(\frac{1}{2},\frac{1}{2},\frac{1}{2})$, $(\frac{1}{2},\frac{1}{2},0)$, and $(0,0,\frac{1}{2})$. This proves nonconjugacy.

8.2. **Irreducible $\mathbb{Z}^d$-actions on zero-dimensional compact abelian groups.**

Example 8.20 (The trivial centralizer of Ledrappier's example)**.** In Example 7.1 (1) we considered the $\mathbb{Z}^2$-action $\alpha = \alpha_{R_2^{(2)}/(f)}$ with $f = 1+u_1+u_2 \in R_2^{(2)}$. We claim that

$$\mathcal{C}_0(\alpha) = \mathcal{C}_{\mathrm{aff}}(\alpha) = \mathcal{C}_{\lambda_X}(\alpha) = \{\alpha^{\mathbf{n}} : \mathbf{n} \in \mathbb{Z}^2\}$$

(cf. Definition 8.14 on page 40).

Since 0 is the only fixed point of α, $\mathcal{C}_0(\alpha) = \mathcal{C}_{\mathrm{aff}}(\alpha) = \mathcal{C}_{\lambda_X}(\alpha)$ by Theorem 8.4. As α has cyclic dual, every automorphism $\beta \in \mathcal{C}_0(\alpha)$ is completely determined by the element $g + (f) = \hat{\beta}(1 + (f)) \in \widehat{X} = R_2^{(2)}/(f)$, where β is the automorphism of $\widehat{X}$ dual to β. As β is a group automorphism, its kernel is trivial, which translates into the statement that the varieties

$$\begin{aligned} V(f) &= \{(c_1, c_2) \in (\bar{F}_2)^{\times} \times (\bar{F}_2)^{\times} : f(c_1, c_2) = 0\} \\ &= \{(c_1, 1 + c_1) : c_1 \in (\bar{F}_2)^{\times},\ 1 + c_1 \in (\bar{F}_2)^{\times}\}, \\ V(g) &= \{(c_1, c_2) \in (\bar{F}_2)^{\times} \times (\bar{F}_2)^{\times} : g(c_1, c_2) = 0\} \end{aligned}$$

of f and g do not intersect (this statement is meaningful in spite of the fact that g is determined only up to addition of an element in (f)). After modifying g by an element of (f) we may assume that

$$g(u_1, u_2) = \sum_{\mathbf{m}=(m_1,m_2)\in F} u_1^{m_1}(1 + u_1)^{m_2} = h(u_1),$$

say, for some finite subset $F \subset \mathbb{Z}^2$. Our hypothesis on the intersection of varieties guarantees that $h(u_1) \neq 0$ for every $u_1 \in (\bar{F}_2)^{\times}$, and hence that $h(u_1) = u_1^{k_1}(1 + u_1)^{k_2}$ and $g = u^{\mathbf{k}} \pmod{(f)}$ for some $\mathbf{k} = (k_1, k_2) \in \mathbb{Z}^2$. This proves that $\beta = \alpha^{\mathbf{k}}$ for some $\mathbf{k} \in \mathbb{Z}^2$.

Example 8.21. Consider the $\mathbb{Z}^2$-action $\alpha = \alpha_M$ and α_N with $M = R_2^{(2)}/\mathfrak{p}$ and $N = R_2^{(4)}/\mathfrak{q}$ in Example 7.5 (1), where $\mathfrak{p} = (1+u_1+u_2+u_1^2+u_1u_2+u_2^2) \subset R_2^{(2)}$ and $\mathfrak{q} = (1+\omega u_1+\omega^2 u_2) \subset R_2^{(4)}$. There we found a two-to-one algebraic factor map from $(X', \alpha') = (X_N, \alpha_N)$ to $(X, \alpha) = (X_M, \alpha_M)$. However, the dual module $\widehat{X} = M$ is obviously cyclic in the sense of Definition 8.11, whereas the module $\widehat{X'} = N$ is not. Theorem 8.4 shows that the finitely equivalent actions α and α' are not measurably conjugate.

By exploiting the fact that the polynomials $f' = 1 + u_1^2 + u_2 + u_1u_2 + u_2^2$ and $f'' = 1 + u_1 + u_1^2 + u_2 + u_2^2$ are irreducible in $R_2^{(2)}$, but not in $R_2^{(4)}$, one can construct further examples of this kind.

Example 8.22 (Nonconjugacy of $\mathbb{Z}^2$-actions with positive entropy)**.** Let

$$f_1 = 1 + u_1 + u_1^2 + u_1u_2 + u_2^2,$$

$$
\begin{aligned}
f_2 =& 1 + u_1^2 + u_2 + u_1 u_2 + u_2^2,\\
f_3 =& 1 + u_1 + u_1^2 + u_2 + u_2^2,\\
f_4 =& 1 + u_1 + u_1^2 + u_2 + u_1 u_2 + u_2^2,
\end{aligned}
$$

in R_2, put $\mathfrak{p}_i = (2, f_i) \subset R_2$, $J_i = (4, 2f_i) \subset R_2$, $M_i = R_2/J_i$, $N_i = R_2/\mathfrak{p}_i$, and define the algebraic $\mathbb{Z}^2$-actions $\alpha_i = \alpha_{M_i}$ on $X_i = X_{M_i}$ and $\beta_i = \alpha_{N_i}$ on $Y_i = X_{N_i}$ as in Example 4.1 (2). For every $i = 1, \dots, 4$, the prime ideals associated with the module M_i are $(2) = 2R_2$ and $\mathfrak{p}_i$, and the inclusion of $2M_i \cong N_i$ in M_i is dual to an algebraic factor map $\phi_i \colon X_i \longrightarrow Y_i$ from (X_i, α_i) to (Y_i, β_i). Since $\ker \phi_i \cong \widehat{R_2/2R_2} = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{Z}^2}$ and the actions β_i have zero entropy, the Pinsker algebra $\pi(\alpha_i)$ of α_i is the sigma-algebra $\mathcal{B}_{X_i/\ker \phi_i}$ of $\ker \phi_i$-invariant Borel sets in X_i. In other words, the $\mathbb{Z}^2$-action induced by α_i on the Pinsker algebra $\pi(\alpha_i)$ is measurably conjugate to β_i.

Since any measurable conjugacy of α_i and α_j would map $\pi(\alpha_i)$ to $\pi(\alpha_j)$ and induce a conjugacy of β_i and β_j, Theorem 8.4 implies that α_i and α_j are measurably nonconjugate for $1 \le i < j \le 4$.

9. Isomorphism rigidity of algebraic $\mathbb{Z}^d$-actions: the general case

In Section 8 we investigated the isomorphism problem for irreducible algebraic $\mathbb{Z}^d$-actions. Although the discussion below shows that one can relax the hypothesis of irreducibility in Theorem 8.4 to some extent, the methods currently do not extend significantly beyond the class of expansive and mixing algebraic $\mathbb{Z}^d$-actions α on compact abelian groups X with the property that $h(\alpha^{\mathbf{n}}) < \infty$ for every $\mathbf{n} \in \mathbb{Z}^d$ (i.e. the *rank one case* in the terminology of [10]). For example, if $\mathfrak{p}, \mathfrak{q} \subset R_3$ are nonprincipal prime ideals with 2 generators such that the zero-entropy $\mathbb{Z}^3$-actions $\alpha = \alpha_{R_3/\mathfrak{p}}$ and $\beta = \alpha_{R_3/\mathfrak{q}}$ are measurably conjugate (cf. Table 1 (6)), and if the groups $X = X_{R_d/\mathfrak{p}}$ and $Y = X_{R_d/\mathfrak{q}}$ are connected, there are at present no general results about isomorphism rigidity of such actions. As far as I know, the following 'cautious conjecture' from [44] may have a positive answer under the hypothesis that the groups X and Y are connected (it is now known to be wrong without this hypothesis by [3] and [4]).

Conjecture 9.1. *Let $d > 1$, and let α and β be expansive and mixing algebraic $\mathbb{Z}^d$-actions on compact connected abelian groups X and Y, respectively. If α and β have zero entropy, then any measurable conjugacy between them is* a.e. *equal to an affine map.*

Conjecture 9.1 would be implied by a positive answer to the following problem.

Problem 9.2. Let $d \geq 2$, and let α_1 and α_2 be expansive and mixing algebraic $\mathbb{Z}^d$-actions on compact abelian groups X_1 and X_2 with normalized Haar measures λ_{X_1} and λ_{X_2}, respectively. We write $\alpha = \alpha_1 \times \alpha_2$ for the product-$\mathbb{Z}^d$-action on $X = X_1 \times X_2$ and assume that μ is an α-invariant probability measure on X with the following property: if $\pi_i \colon X \longrightarrow X_i$ denotes the i-th coordinate projection, then $\mu\pi_i^{-1} = \lambda_{X_i}$, and π_i is a measurable conjugacy of the $\mathbb{Z}^d$-actions α on (X, μ) and α_i on (X_i, λ_{X_i}).

Does there exists a closed α-invariant subgroup $Y \subset X$ such that μ is a translate of the Haar measure λ_Y?

Theorem 8.5 is, of course, a special case of this problem, which is in turn part of a much more general quest to determine all invariant and ergodic probability measures of a zero entropy mixing algebraic $\mathbb{Z}^d$-action α with $d \geq 2$ (where the mixing hypothesis is imposed only to ensure that there is no single group automorphism β such that $\alpha^{\mathbf{n}}$ is a power of β for all $\mathbf{n}$ in some subgroup of finite index in $\mathbb{Z}^d$). The first instance of this problem is due to Furstenberg (cf. [14]): *Is every nonatomic probability measure μ on $\mathbb{T}$ which is simultaneously invariant under multiplication by* 2 *and by* 3 *equal to Lebesgue measure?* In spite of some remarkable progress due to Rudolph in [37], who proved that any such measure with positive entropy under either of these multiplications has to be equal to $\lambda_{\mathbb{T}}$, Furstenberg's original question is still open, and several ingenious proofs by Host and others depend in a very crucial way on positive entropy. For extensions of Rudolph's results to commuting automorphisms of finite-dimensional tori or solenoids we refer to the paper by Katok and Spatzier [19] and to recent work in progress by Einsiedler and Lindenstrauss [11], which contains the currently most general statement about invariant probability measures for irreducible and mixing algebraic $\mathbb{Z}^d$-actions on compact connected abelian groups.

Theorem 9.3. *Let $d \geq 2$, and let α be an irreducible and mixing algebraic $\mathbb{Z}^d$-action on a finite-dimensional torus or solenoid X. If μ is an α-invariant and ergodic probability measure on X which has positive entropy under some $\alpha^{\mathbf{n}}$, $\mathbf{n} \in \mathbb{Z}^d$, then there exists a finite index subgroup $\Lambda \subset \mathbb{Z}^d$ with the following properties.*

(1) *Let $\mathbf{n}_1, \dots, \mathbf{n}_k \in \mathbb{Z}^d$ be a complete set of representatives of $\mathbb{Z}^d/\Lambda$, let α^Λ be the restriction of α to Λ, and let $\mu = \frac{1}{k}\sum_{i=1}^k \mu_i$ be the α^Λ-ergodic decomposition of μ. There exists an infinite closed α^Λ-invariant subgroup $Y \subset X$ such that each μ_i is invariant under translation by the subgroup $Y_i = \alpha^{\mathbf{n}_i}(Y)$.*

(2) *For every $i = 1, \dots, k$, the measure μ_i and the Λ-action α^Λ descend naturally to the factor X/Y_i, and every $\alpha^{\mathbf{n}}$, $\mathbf{n} \in \Lambda$, has zero entropy on X/Y_i with respect to μ_i.*

Although much more is known about isomorphism rigidity of algebraic $\mathbb{Z}^d$-actions on zero-dimensional compact abelian groups than in the connected case (cf. Section 10), the problem of describing the invariant probability measures of even the simplest examples is in no better state than in the connected case. Here are two unresolved questions about Ledrappier's Example 7.1 (1).

Problem 9.4. Let $\alpha = \alpha_{R_2^{(2)}/(1+u_1+u_2)}$ be the shift-action on the group $X = X_{R_2^{(2)}/(1+u_1+u_2)}$ in Example 7.1 (1).

(1) If μ is an α-invariant probability measure on X with full support (i.e. with $\mu(\mathcal{O}) > 0$ for every nonempty open subset $\mathcal{O} \subset X$), is $\mu = \lambda_X$?

(2) If μ is a nonatomic α-invariant probability measure on X which is ergodic under some $\alpha^{\mathbf{n}}$, is $\mu = \lambda_X$?

10. Isomorphism rigidity of algebraic $\mathbb{Z}^d$-actions: the disconnected case

This chapter is devoted to isomorphism rigidity results (and counterexamples) for expansive and mixing algebraic $\mathbb{Z}^d$-actions on zero-dimensional compact abelian groups. The exposition follows [4] and [5].

10.1. **Measurable polynomials.**

Definition 10.1. Let X, Y be compact abelian groups, and let $U(X, Y)$ be the group of all λ_X-equivalence classes of Borel maps $f\colon X \longrightarrow Y$, furnished with pointwise addition as composition and the topology of convergence in Haar measure. For every $x \in X$ we denote by $\partial_x\colon U(X, Y) \longrightarrow U(X, Y)$ the continuous map defined by

$$\partial_x(f)(x') = f(x + x') - f(x')$$

for every $x' \in X$ and $f \in U(X, Y)$, and we set

$$\partial_{\mathbf{x}} = \partial_{x_1} \circ \partial_{x_2} \circ \cdots \circ \partial_{x_k}\colon U(X, Y) \longrightarrow U(X, Y)$$

for every $k \geq 1$ and $\mathbf{x} = (x_1, \ldots, x_k) \in X^k$.

An element $f \in U(X, Y)$ is a *measurable polynomial* if there exists an integer $k \geq 1$ with $\partial_{\mathbf{x}}(f) = 0 \pmod{\lambda_X}$ for every $\mathbf{x} \in X^k$. If k is the smallest such integer, then the *degree* $\deg(f)$ of the measurable polynomial f is equal to $k - 1$.

For every $a \in \widehat{Y}$ and $f \in U(X, Y)$ we denote by $\langle a, f\rangle \in U(X, \mathbb{S})$ the map $x \mapsto \langle a, f(x)\rangle$, where $\langle a, x\rangle$ is the value of the character $a \in \widehat{Y}$ at the point $x \in X$.

Lemma 10.2. *An element $f \in U(X,Y)$ is a measurable polynomial if and only if $\langle a, f\rangle \in U(X,\mathbb{S})$ is a measurable polynomial for every $a \in \widehat{Y}$, and f has degree $\le k$ if and only if* $\deg(\langle a, f\rangle) \le k$ *for every $a \in \widehat{Y}$. Finally, f is continuous if and only if $\langle a, f\rangle$ is continuous for every $a \in \widehat{Y}$.*

Proof. We set $\Omega = \mathbb{S}^{\widehat{Y}}$ and write every $\omega \in \Omega$ as $\omega = (\omega_a,\, a \in \widehat{Y})$ with $\omega_a \in \mathbb{S}$ for every $a \in \widehat{Y}$. Define a continuous injective group homomorphism $\Phi\colon Y \longrightarrow \mathbb{S}^{\widehat{Y}}$ by setting

$$\Phi(y)_a = \langle a, y\rangle$$

for every $a \in \widehat{Y}$ and $y \in Y$. Then $Z = \Phi(Y)$ is a closed subgroup of Ω, and the map $f' = \Phi \circ f\colon X \longrightarrow Z$ is a measurable polynomial (of degree $\le k$) if and only if each coordinate $x \mapsto f'(x)_a = \langle a, f(x)\rangle$ of the map f' is an $\mathbb{S}$-valued measurable polynomial (of degree $\le k$) for every $a \in \widehat{Y}$. Since $\Phi\colon X \longrightarrow Z$ is a topological group isomorphism, the last statement is obvious. □

Lemma 10.3. *Let $f \in U(X,Y)$ and $k \ge 1$. Then the map $\mathbf{x} \mapsto \partial_{\mathbf{x}}(f)$ from X^k to $U(X,Y)$ is continuous.*

Proof. The same argument as in Lemma 10.2 allows us to assume without loss in generality that $Y = \mathbb{S}$.

Consider the special case where $k = 2$. For any $f \in U(X,\mathbb{S})$ and $x \in X$ we denote by $\bar{f}$ the complex conjugate of f and write $f_x \in U(X,\mathbb{S})$ for the map given by $f_x(x') = f(x + x')$. Define maps $S_1,\dots,S_4\colon X^2 \longrightarrow U(X,\mathbb{S})$ by

$$S_1(x_1,x_2) = f_{x_1+x_2},\;\; S_2(x_1,x_2) = \overline{f_{x_1}},\;\; S_3(x_1,x_2) = \overline{f_{x_2}},\;\; S_4(x_1,x_2) = f,$$

where the bar denotes complex conjugation. For every $\mathbf{x} \in X^2$, $\partial_{\mathbf{x}}(f) = S_1(\mathbf{x}) \cdot S_2(\mathbf{x}) \cdot S_3(\mathbf{x}) \cdot S_4(\mathbf{x})$. Since the right regular representation of X on $L^2(X,\lambda_X)$ is continuous, each S_i is a continuous map from X^2 into $L^2(X,\lambda_X)$ and hence also a continuous map from X^2 into $U(X,\mathbb{S})$. As multiplication is continuous in $U(X,\mathbb{S})$, this proves our assertion for $k = 2$. In the general case we define $S_1,\dots,S_{2^k}$ in an analogous way and apply the same argument as above. □

Proposition 10.4 ([4])**.** *Let X, Y be compact abelian groups, and let $f \in U(X,Y)$ be a measurable polynomial.*

1. *There exists a unique continuous map $f'\colon X \longrightarrow Y$ such that $f = f'$* (mod λ_X).
2. *The map f' is constant if and only if* $\deg(f) = 0$, *and affine if and only if* $\deg(f) \le 1$.
3. *If X is connected, then f has degree ≤ 1.*

Proof. For $k \geq 0$ we denote by $P_k \subset U(X,Y)$ the topological space consisting of all measurable polynomials $p\colon X \longrightarrow Y$ of degree at most k, furnished with the subspace topology. If f is a measurable polynomial of degree 0, then f is λ_X-*a.e.* equal to a constant $y \in Y$. If $\deg(f) = 1$, then there exists, for every $x \in X$, a unique constant $c(x) \in Y$ with $\partial_x(f) = c(x) \pmod{\lambda_X}$, and the map $x \mapsto c(x)$ is a Borel measurable — and thus continuous — group homomorphism. Hence there exists, for every $x \in X$, a Borel set $B_x \subset X$ with $\lambda_X(B_x) = 1$ such that

$$f(x + x') = c(x) + f(x') \tag{10.1}$$

for every $x \in X$ and $x' \in B_x$. Fubini's Theorem implies that there exists a Borel set $B \subset X$ with $\lambda_X(B) = 1$ such that (10.1) holds for every $x' \in B$ and λ_X-*a.e.* $x \in X$, which shows that f is *a.e.* equal to an affine map.

We have proved that every map in P_1 is *a.e.* equal to a continuous map. Continuing by induction, we assume that k is a positive integer such that every measurable polynomial of degree $\leq k$ is *a.e.* equal to a continuous map and consider a polynomial $f \in P_{k+1} \subset U(X,Y)$. According to Lemma 10.3 it suffices to prove the continuity of f in the special case where $Y = \mathbb{S}$, and we assume therefore without loss in generality that $f \in U(X,\mathbb{S})$.

Since the characters form an orthonormal basis of $L^2(X,\lambda_X)$ we deduce that P_1 is homeomorphic to $P_0 \times \widehat{X}$, where $\widehat{X}$ is equipped with the discrete topology, and we write $\theta\colon P_1 \longrightarrow \widehat{X}$ for the projection map. The map

$$\mathbf{x} \mapsto q(\mathbf{x}) = \theta \circ \partial_{\mathbf{x}}(f)$$

from X^k to $\widehat{X}$ is continuous by Lemma 10.3. Since $\widehat{X}$ is discrete, $q(X^k)$ is finite, and there exists an open subgroup $K_1 \subset X^k$ such that q is constant on each coset of K_1 in X^k. We choose an open subgroup $K \subset X$ with $K^k \subset K_1$. Then $\partial_{\mathbf{x}}(f)$ lies in P_0 for all $\mathbf{x} \in K^k$, so that the restriction of f to K is a measurable polynomial of degree at most k. Let $K + z_1, \dots, K + z_l$ be the distinct cosets of K in X, and let, for $i = 1, \dots, l$, $f_i\colon X \longrightarrow \mathbb{S}$ be the map defined by $f_i(x) = f(z_i + x)$. Since $\partial_{\mathbf{x}}(f_i)(x) = \partial_{\mathbf{x}}(f)(z_i + x)$ for each i, we conclude that restriction of each f_i to K is a measurable polynomial of degree at most k. By the induction hypothesis, the restriction of each f_i to K agrees λ_K-a.e. with a continuous map, i.e. f agrees λ_X-a.e. with a continuous map.

If X is connected then q is trivial, i.e. the degree of f is $\leq k$. By a slight modification of the above induction argument, f agrees λ_X-a.e. with an affine map. □

10.2. **Topological rigidity.**

Theorem 10.5 ([4])**.** *Let α and β be mixing algebraic $\mathbb{Z}^d$-actions on compact abelian groups X and Y, respectively. Suppose furthermore that there exists* *an integer $k \geq 2$ with the following property: for every closed β-invariant subgroup $Z \subset Y$, the restriction β_Z of β to Z is not $(k+1)$-mixing. Then every equivariant Borel map $\phi\colon (X,\alpha) \longrightarrow (Y,\beta)$ is a measurable polynomial of degree $\leq k-1$ and hence* a.e. *equal to a continuous map.*

We begin the proof of Theorem 10.5 with a lemma.

Lemma 10.6. *Let α be a mixing algebraic $\mathbb{Z}^d$-action on a compact abelian group X, $k \geq 1$, and let $f_i\colon X^k \longrightarrow \mathbb{R}_+$, $i = 0, \dots, k$, be continuous maps with the following properties.*

(1) *For every $i = 1, \dots, k$ and $(x_1, \dots, x_k) \in X^k$, $f_i(x_1, \dots, x_k) = 0$ whenever $x_j = 0$ for some $j \in \{1, \dots, k\}$;*
(2) *There exist sequences $(\mathbf{n}_m^{(i)}, m \geq 1)$, $i = 1, \dots, k$, in $\mathbb{Z}^d$ with*
$$\lim_{m\to\infty} \mathbf{n}_m^{(i)} = \infty$$
for $i = 1, \dots, k$, and
$$f_0 \leq \sum_{i=1}^{k} f_i \circ \bar{\alpha}^{\mathbf{n}_m^{(i)}} \tag{10.2}$$
for every $m \geq 1$, where $\bar{\alpha}\colon \mathbf{n} \longrightarrow \alpha^{\mathbf{n}} \times \dots \times \alpha^{\mathbf{n}}$ is the diagonal $\mathbb{Z}^d$-action on X^k induced by α.

Then $f_0 \equiv 0$.

Proof. If $f_0 \not\equiv 0$, then there exist nonempty open subsets $\mathcal{U}_1, \dots, \mathcal{U}_k$ in X and an $\varepsilon > 0$ such that
$$f_0(x_1, \dots, x_k) > \varepsilon \text{ for every } (x_1, \dots, x_k) \in \mathcal{U}_1 \times \dots \times \mathcal{U}_k. \tag{10.3}$$
Since each f_i is continuous, it is uniformly continuous on X^k, and there exists an open neighbourhood $\mathcal{U}$ of 0 in X such that
$$f_i(x_1, \dots, x_k) < \varepsilon/k \tag{10.4}$$
whenever $i \in \{1, \dots, k\}$ and $x_j \in \mathcal{U}$ for some $j \in \{1, \dots, k\}$.

As α is mixing, there exists an integer $M \geq 1$ with $\alpha^{-\mathbf{n}_m^{(i)}}(\mathcal{U}) \cap \mathcal{U}_i \neq \varnothing$ for every $i = 1, \dots, k$ and $m \geq M$. Fix $x_i \in \alpha^{-\mathbf{n}_M^{(i)}}(\mathcal{U}) \cap \mathcal{U}_i$ for $i = 1, \dots, k$. Then $\alpha^{\mathbf{n}_M^{(i)}} x_i \in \mathcal{U}$ and hence, by (10.3),
$$f_i \circ \bar{\alpha}^{\mathbf{n}_M^{(i)}}(x_1, \dots, x_k) < \varepsilon/k$$
for $i = 1, \dots, k$, which violates (10.2)–(10.3). □

Proof of Theorem 10.5. It suffices to show that $\langle a, \phi \rangle\colon X \longrightarrow Y$ is a measurable polynomial of degree $\leq k-1$ for every character $a \in \widehat{Y}$. We set
$$A = \{a \in \widehat{Y} : \langle a, \phi \rangle \text{ is a measurable polynomial of degree } \leq k-1\}$$
and assume that $A \subsetneq \widehat{Y}$.

The group A is obviously invariant under $\widehat{\beta}$, and its annihilator

$$Z = A^{\perp} = \{y \in Y : \langle a, y\rangle = 1 \text{ for every } a \in A\}.$$

is a closed β-invariant subgroup of Y.

By assumption, β_Z is not $(k+1)$-mixing. Hence there exist characters $b_0, \dots, b_k \in \widehat{Z}$ with $b_0 \neq 0$, and sequences $(\mathbf{n}_m^{(i)}, m \geq 1)$, $i = 1, \dots, k$, in $\mathbb{Z}^d$ with

$$\lim_{m\to\infty} \mathbf{n}_m^{(i)} = \infty$$

for $i = 1, \dots, k$, such that

$$b_0 = \sum_{i=1}^{k} \widehat{\beta}_Z^{\mathbf{n}_m^{(i)}} b_i$$

for every $m \geq 1$. We extend each $b_i \in \widehat{Z}$ to an element $b_i' \in \widehat{Y}$ and obtain elements $a_m \in A$, $m \geq 1$, with

$$b_0' = \sum_{i=1}^{k} \widehat{\beta}^{\mathbf{n}_m^{(i)}} b_i' + a_m$$

for every $m \geq 1$. By composing this equation with ϕ we obtain that

$$\langle b_0', \phi\rangle = \langle a_m, \phi\rangle \cdot \prod_{i=1}^{k} \langle \widehat{\beta}^{\mathbf{n}_m^{(i)}} b_i', \phi\rangle = \langle a_m, \phi\rangle \cdot \prod_{i=1}^{k} \langle b_i', \phi \circ \alpha^{\mathbf{n}_m^{(i)}}\rangle$$

for every $m \geq 1$. Put

$$f_i(x_1, \dots, x_k) = \|\partial_k(x_1, \dots, x_k)(\langle b_i', \phi\rangle) - 1\|_2$$

for every $(x_1, \dots, x_k) \in X^k$ and $i = 0, \dots, k$, and note that

$$f_0 \leq \sum_{i=1}^{k} f_i \circ \bar{\alpha}^{\mathbf{n}_m^{(i)}} + \|\partial_k(x_1, \dots, x_k)(\langle a_m, \phi\rangle) - 1\|_2 \tag{10.5}$$

for every $m \geq 1$, where we are using the same notation as in Lemma 10.6. As $a_m \in A$, $\langle a_m, \phi\rangle$ is a measurable polynomial of degree $\leq k$, and hence $\partial_k(x_1, \dots, x_k)(\langle a_m, \phi\rangle) = 1$ λ_Y-a.e. The inequality (10.5) thus reduces to

$$f_0 \leq \sum_{i=1}^{k} f_i \circ \bar{\alpha}^{\mathbf{n}_m^{(i)}}$$

for every $m \geq 1$, and Lemma 10.6 guarantees that $f_0 \equiv 0$. This shows that $b_0' \in A$ and hence $b_0 = 0$, and the resulting contradiction to our choice of b_0 implies that $A = \widehat{Y}$ and that ϕ is a measurable polynomial of degree $\leq k-1$, as claimed. □

Corollary 10.7. *Let $d > 1$, and let α and β be algebraic $\mathbb{Z}^d$-actions on compact abelian groups X and Y, respectively. Suppose that Y is zero-dimensional and that β has zero entropy. Then there exists a continuous factor map $\phi' \colon (X, \alpha) \longrightarrow (Y, \beta)$ such that $\phi = \phi'$* λ_X-a.e.

Proof. Let $N = \widehat{Y}$ be the dual module of β. Then there exists an increasing sequence $(N_k,\ k \geq 1)$ of submodules of N such that $N = \bigcup_{k\geq 1} N_k$ and each N_k is Noetherian. For every $k \geq 1$, the annihilator $Y_k = N_k^{\perp} \subset Y$ is a closed β-invariant subgroup, and we denote by $\pi_k \colon Y \longrightarrow Y/Y_k$ the quotient map.

Let $\phi\colon (X,\alpha) \longrightarrow (Y,\beta)$ be a measurable factor map such that $\phi_k = \pi_k \circ \phi$ is a measurable polynomial for every $k \geq 1$. Then $\pi_k \circ \phi$ is λ_X-*a.e.* equal to a continuous factor map $\phi_k\colon (X,\alpha) \longrightarrow (Y/Y_k, \beta_{Y/Y_k})$ for every $k \geq 1$, where β_{Y/Y_k} is the $\mathbb{Z}^d$-action on Y/Y_k induced by β. As $\bigcap_{k\geq 1} Y_k = \{0_Y\}$, compactness implies that there exists, for every neighbourhood $\mathcal{U}$ of the identity in Y, an integer $K \geq 1$ with $Y_k \subset \mathcal{U}$ for every $k \geq K$. If ϕ is not equal to a continuous map λ_X-*a.e.*, then the same is true for some ϕ_k, which leads to a contradiction. This observation allows us to assume without loss in generality that $N = \widehat{Y}$ is Noetherian.

As $\bigcup_{k\geq 1} N_k = N$ we know that $\bigcap_{k\geq 1} Y_k = \{0_Y\}$. By compactness there exists, for every neighbourhood $\mathcal{U}$ of the identity in Y, an integer $K \geq 1$ with $Y_k \subset \mathcal{U}$ for every $k \geq K$. If ϕ is not equal to a continuous map λ_X-*a.e.*, then the same is true for some $\phi_k = \pi_k \circ \phi$, which contradicts the hypothesis in preceding paragraph. This allows us to assume without loss in generality that $N = \widehat{Y}$ is Noetherian.

Let therefore N be Noetherian, and let $\mathrm{Asc}(N)$ be the set of associated prime ideals of N. Since Y is zero-dimensional, every $\mathfrak{p} \in \mathrm{Asc}(N)$ contains a rational prime constant $p(\mathfrak{p}) > 1$ by Lemma 5.1, and Table 1 (6) implies that $\mathfrak{p} \supsetneq (p(\mathfrak{p})) = p(\mathfrak{p})R_d$, since β has zero entropy. We choose and fix, for every $\mathfrak{p} \in \mathrm{Asc}(N)$, a Laurent polynomial $f(\mathfrak{p}) \in \mathfrak{p} \smallsetminus (p(\mathfrak{p}))$, observe that the polynomial $f(\mathfrak{p})_{/p(\mathfrak{p})} \in R_d^{(p(\mathfrak{p}))}$ in (7.1) is nonzero, and denote by $K = \max_{\mathfrak{p}\in\mathrm{Asc}(N)} |\mathcal{S}(f(\mathfrak{p})_{/p(\mathfrak{p})})|$ the maximal cardinality of the supports of these polynomials.

Suppose that $Z \subset Y$ is a closed β-invariant subgroup. We write $L = \widehat{Z}$ for the dual module of Z, choose a prime ideal $\mathfrak{q} \in \mathrm{Asc}(L)$ and an element $a \in L$ with $\mathfrak{q} = \mathrm{ann}(a)$, and set $L' = R_d \cdot a \cong R_d/\mathfrak{q}$. Since L is a quotient of N, $\mathfrak{q}$ contains some $\mathfrak{p} \in \mathrm{Asc}(N)$, and Example 7.1 (2) shows that $\alpha_{L'} \cong \alpha_{R_d/\mathfrak{q}}$ — and hence $\beta_Z = \alpha_L$ — is not mixing of order $|\mathcal{S}(f(\mathfrak{q}))| \leq K$. By Theorem 10.5, ϕ is a measurable polynomial and thus coincides λ-*a.e.* with a continuous factor map. □

10.3. **Homoclinic points and isomorphism rigidity.** Once we know that measurable conjugacies and factor maps between two algebraic $\mathbb{Z}^d$-actions (X,α) and (Y,β) are automatically continuous it is not too difficult to verify that they have to be polynomials (the approach using homoclinic points described below is one such method). If the groups X and Y are connected, these polynomials are affine by Proposition 10.4, which proves isomorphism rigidity. However, if the groups X and Y are zero-dimensional, polynomials may have degrees > 1, and one needs additional hypotheses (whose necessity will be illustrated below in Example 10.15) to ensure that the measurable conjugacies and factor maps are affine.

Definition 10.8. Let α be an algebraic $\mathbb{Z}^d$-action on a compact abelian group X, and let $\Gamma \subset \mathbb{Z}^d$ be a subgroup. An element $x \in X$ is (α, Γ)-*homoclinic* (to the identity element 0_X of X), if

$$\lim_{\substack{\mathbf{n}\to\infty\\ \mathbf{n}\in\Gamma}} \alpha^{\mathbf{n}} x = 0_X.$$

The α-invariant subgroup $\Delta_{(\alpha,\Gamma)}(X) \subset X$ of all (α, Γ)-homoclinic points is an R_d-module under the operation

$$f \cdot x = f(\alpha)(x)$$

for every $f \in R_d$ and $x \in \Delta_{(\alpha,\Gamma)}(X)$ (cf. (4.5)), and is called the Γ-*homoclinic module of* α (cf. [26]).

Proposition 10.9. *Let α be an expansive algebraic $\mathbb{Z}^d$-action on a compact abelian group X, and let $\Gamma \subset \mathbb{Z}^d$ be a subgroup. Then $\Delta_{(\alpha,\Gamma)} \neq \{0_X\}$ if and only if the entropy $h(\alpha^\Gamma)$ of the algebraic Γ-action α^Γ on X is positive, and $\Delta_{(\alpha,\Gamma)}$ is dense in X if and only if α^Γ has completely positive entropy* (*where entropy is always taken with respect to Haar measure*).

Proof. This is [26, Theorems 4.1 and 4.2]. □

If an expansive and mixing algebraic $\mathbb{Z}^d$-action α on a compact abelian group X has zero entropy, then the homoclinic group $\Delta_\alpha(X)$ of this $\mathbb{Z}^d$-action is trivial by Proposition 10.9, but $\Delta_{(\alpha,\Gamma)}$ will be dense in X for appropriate subgroups $\Gamma \subset \mathbb{Z}^d$. We investigate this phenomenon in the special case where $p > 1$ is a rational prime, $f \in R_d^{(p)}$ an irreducible Laurent polynomial such that the convex hull $\mathcal{C}(f) \subset \mathbb{R}^d$ of the support $\mathcal{S}(f) \subset \mathbb{Z}^d$ of f contains an interior point (cf. (7.4)), and where $\alpha = \alpha_{R_d^{(p)}/(f)}$ is the shift-action of $\mathbb{Z}^d$ on the compact abelian group $X = X_{R_d^{(p)}/(f)} \subset F_p^{\mathbb{Z}^d}$ defined in (7.2)–(7.3).

We write $[\,.\,,.\,]$ and $\|\cdot\|$ for the Euclidean inner product and norm on $\mathbb{R}^d$ and

$$\mathsf{S}_{d-1} = \{\mathbf{v} \in \mathbb{R}^d \colon \|\mathbf{v}\| = 1\}$$

for the unit sphere in $\mathbb{R}^d$ and set, for every nonzero element $\mathbf{m} \in \mathbb{Z}^d$,

$$\begin{aligned} \mathbf{m}^* &= \tfrac{\mathbf{m}}{\|m\|}, \\ \Gamma_{\mathbf{m}} &= \{\mathbf{n} \in \mathbb{Z}^d \colon [\mathbf{m}, \mathbf{n}] = 0\}. \end{aligned} \tag{10.6}$$

Proposition 10.10. [5] *Let $d > 1$, $p > 1$ a rational prime, $f \in R_d^{(p)}$ an irreducible Laurent polynomial such that the shift-action $\alpha = \alpha_{R_d^{(p)}/(f)}$ of $\mathbb{Z}^d$ on the compact abelian group $X = X_{R_d^{(p)}/(f)} \subset F_p^{\mathbb{Z}^d}$ in* (7.2)–(7.3) *is mixing, and let $\mathbf{m} \subset \mathbb{Z}^d$ be a nonzero element such that the restriction $\alpha^{\Gamma_\mathbf{m}}$ of α to the subgroup $\Gamma_\mathbf{m}$ in* (10.6) *is expansive. Then the homoclinic group $\Delta_{(\alpha,\Gamma_\mathbf{m})}(X)$ is dense in X. Furthermore there exists an open subset $W \subset \mathsf{S}_{d-1}$ such that every nonzero element $\mathbf{n} \in \mathbb{Z}^d$ with $\mathbf{n}^* \in \mathsf{S}_{d-1}$ has the following properties.*

(1) $\Delta_{(\alpha,\Gamma_\mathbf{n})}(X)$ *is dense in X;*
(2) $\Delta_{(\alpha,\Gamma_\mathbf{m})}(X) \cap \Delta_{(\alpha,\Gamma_\mathbf{n})}(X) = \{0_X\}$.

The proof of Proposition 10.10 is given in [5]. By using this proposition and some algebraic structure theory one obtains the following rigidity result for measurable factor maps between algebraic $\mathbb{Z}^d$-actions on zero-dimensional compact abelian groups.

Theorem 10.11. *Let $d > 1$, and let α and β be mixing algebraic $\mathbb{Z}^d$-actions on zero-dimensional compact abelian groups X and Y, respectively. Suppose that there exists a subgroup $\Gamma \subset \mathbb{Z}^d$ of of infinite index such that the restriction α^Γ of α to Γ is expansive and has completely positive entropy. Then every measurable factor map $\phi\colon (X,\alpha) \longrightarrow (Y,\beta)$ is λ_X-a.e. equal to an affine map.*

Theorem 10.11 was proved independently in [5] and [9]; the latter proof depends on a characterization of invariant measures analogous to the connection between the Theorems 8.5 and 8.4. Here we follow the 'homoclinic' route in [5]; however, before turning to the proof of this result, we mention a couple of corollaries which generalize the main result in [21] in different directions.

Corollary 10.12. *Let $d > 1$, and let α and β be mixing algebraic $\mathbb{Z}^d$-actions on zero-dimensional compact abelian groups X and Y, respectively. Suppose that there exists a nonzero element $\mathbf{n} \in \mathbb{Z}^d$ such that the automorphism $\alpha^\mathbf{n}$ is expansive. Then every measurable factor map $\phi\colon (X,\alpha) \longrightarrow (Y,\beta)$ is λ_X-a.e. equal to an affine map.*

Proof. Since every mixing (= ergodic) group automorphism has completely positive entropy, this is Theorem 10.11 with Γ of rank one. □

Corollary 10.13. *Let $d > 1$, p a rational prime, and $\mathfrak{p}, \mathfrak{q} \subset R_d^{(p)}$ nonzero prime ideals such that the $\mathbb{Z}^d$-actions $\alpha = \alpha_{R_d^{(p)}/\mathfrak{p}}$ and $\beta = \alpha_{R_d^{(p)}/\mathfrak{q}}$ on the compact zero dimensional groups $X = X_{R_d^{(p)}/\mathfrak{p}}$ and $Y = X_{R_d^{(p)}/\mathfrak{q}}$ in* (7.2)–(7.3) *are mixing. Then α and β are measurably conjugate if and only if they are algebraically conjugate, and hence if and only if $\mathfrak{p} = \mathfrak{q}$. Furthermore,* *every measurable conjugacy* $\phi\colon (X,\alpha) \longrightarrow (Y,\beta)$ *is* λ_X-a.e. *equal to an affine map.*

Proof. The existence of a subgroup $\Gamma \subset \mathbb{Z}^d$ of infinite index with the properties required by Theorem 10.11 is proved in [10] (the rank of Γ is the maximal number of algebraically independent elements in the set $\{u^{\mathbf{n}} + \mathfrak{p} \colon \mathbf{n} \in \mathbb{Z}^d\} \subset R_d^{(p)}/\mathfrak{p}$). Let $\phi\colon (X,\alpha) \longrightarrow (Y,\beta)$ be a measurable conjugacy. By Theorem 10.11, there exist $y \in Y$ and a continuous homomorphism $\theta\colon X \longrightarrow Y$ such that $\phi(x) = y + \theta(x)$ for λ_X-a.e. $x \in X$. It is easy to verify that θ is an algebraic conjugacy of (X,α) and (Y,β).

In order to see that algebraic conjugacy implies that $\mathfrak{p} = \mathfrak{q}$ we note that, for every $f \in R_d^{(p)}$, the maps $f(\alpha)$ and $f(\beta)$ in (4.5) are surjective if and only if $f \notin \mathfrak{p}$ (resp. $f \notin \mathfrak{q}$). □

We begin our sketch of the proof of Theorem 10.11 with a lemma.

Lemma 10.14. *For* $i = 1,2,3$, *let* α_i *be a mixing algebraic* $\mathbb{Z}^d$*-action on a compact abelian group* X_i, *and let* $\phi\colon (X_1 \times X_2, \alpha_1 \times \alpha_2) \longrightarrow (X_3, \alpha_3)$ *be a continuous factor map such that* $\phi(x_1,x_2) = 0_{X_3}$ *whenever* $x_1 = 0_{X_1}$ *or* $x_2 = 0_{X_2}$. *Suppose furthermore that there exist subgroups* Γ_1, Γ_2 *in* $\mathbb{Z}^d$ *such that the homoclinic groups* $\Delta_{(\alpha_i,\Gamma_i)}(X_i)$ *are dense in* X_i *for* $i = 1,2$, *and that* $\Delta_{(\alpha_3,\Gamma_1)}(X_3) \cap \Delta_{(\alpha_3,\Gamma_2)}(X_3) = \{0_{X_3}\}$. *Then* $\phi(X_1 \times X_2) = \{0_{X_3}\}$.

Proof. Since ϕ is a continuous factor map,

$$\begin{aligned}\lim_{\substack{\mathbf{m}\to\infty\\ \mathbf{m}\in\Gamma_1}} \alpha_3^{\mathbf{m}}\phi(x_1,x_2) &= \lim_{\substack{\mathbf{m}\to\infty\\ \mathbf{m}\in\Gamma_1}} \phi(\alpha_1^{\mathbf{m}}x_1, \alpha_2^{\mathbf{m}}x_2) = 0_{X_3}\\ &= \lim_{\substack{\mathbf{n}\to\infty\\ \mathbf{n}\in\Gamma_2}} \alpha_3^{\mathbf{n}}\phi(x_1,x_2) = \lim_{\substack{\mathbf{n}\to\infty\\ \mathbf{n}\in\Gamma_2}} \phi(\alpha_1^{\mathbf{n}}x_1, \alpha_2^{\mathbf{n}}x_2)\end{aligned}$$

for every $x_i \in \Delta_{(\alpha_i,\Gamma_i)}(X_i)$, $i = 1,2$. Hence

$$\phi(x_1,x_2) \in \Delta_{(\alpha_3,\Gamma_1)}(X_3) \cap \Delta_{(\alpha_3,\Gamma_2)}(X_3) = \{0_{X_3}\}.$$

As $\Delta_{(\alpha_i,\Gamma_i)}(X_i) \subset X_i$ is dense for $i = 1,2$ and ϕ is continuous this implies our assertion. □

Leaving technicalities and a bit of algebra aside, the basic idea of the proof of Theorem 10.11 is the fact that there exist two subgroups $\Gamma_1, \Gamma_2 \subset \mathbb{Z}^d$ such that each action α_{Γ_i} has a dense group of homoclinic points and there are no nonzero common homoclinic points for the actions β_{Γ_i}. Since we know already that the factor map $\phi\colon X \longrightarrow Y$ is continuous, we can form a new map $\psi\colon X \times X \longrightarrow Y$ by setting

$$\psi(x_1,x_2) = \psi(x_1 + x_2) - \psi(x_1) - \psi(x_1) + \psi(0).$$

Since $\psi \circ (\alpha^{\mathbf{n}} \times \alpha^{\mathbf{n}}) = \beta^{\mathbf{n}} \circ \psi$ for all $\mathbf{n} \in \mathbb{Z}^d$, and since ψ is continuous and hence uniformly continuous, $\psi(x_1,x_2) \in \Delta_{(\beta,\Gamma_1)} \cap \Delta_{(\beta,\Gamma_2)} = \{0\}$ whenever

$x_i \in \Delta_{(\alpha,\Gamma_i)}$, $i = 1, 2$. Hence ψ vanishes on the dense set $\Delta_{(\alpha,\Gamma_1)} \times \Delta_{(\alpha,\Gamma_1)} \subset X \times X$ and is thus equal to zero by continuity. This shows that ϕ is affine.

The crucial point in this argument is that *two* such subgroups Γ_1, Γ_2 suffice under the hypotheses of Theorem 10.11. In general one can find finitely many such subgroups $\Gamma_1, \dots, \Gamma_n \subset \mathbb{Z}^d$ such that each action α_{Γ_i} has a dense group of homoclinic points and there are no nonzero common homoclinic points for the actions β_{Γ_i}, $i = 1, \dots, n$, and obtains that the map $\psi \colon X^n \longrightarrow Y$ with

$$\psi(x_1, \dots, x_n) = \sum_{F \subset \{1,\dots,n\}} (-1)^{|F|} \, \phi\Bigl(\sum_{i \in F} x_i\Bigr)$$

vanishes on X^n. This implies that ϕ is a polynomial of degree $n-1$, but not necessarily of degree 1.

The following examples from [5] show that Theorem 10.11 and Corollary 10.13 need not hold if any of the assumptions are dropped.

Examples 10.15. (1) *A non-surjective and non-affine equivariant map.* Let $d = 3$, $p = 2$, and consider the polynomials $f_1, f_2 \in R_3^{(2)}$ defined by $f_1 = 1 + u_1 + u_2, f_2 = 1 + u_1 + u_2 + u_1^2 + u_1 u_2 + u_2^2 + u_3$. Let $\mathfrak{p} = (f_1, f_2) \subset R_3^{(2)}$ denote the ideal generated by f_1 and f_2, and let $\mathfrak{q} = (f_2) \subset R_3^{(2)}$ be the principal ideal generated by f_2. It is easy to see that $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals. We define the shift-actions $\alpha_1 = \alpha_{R_3^{(2)}/\mathfrak{p}}$ and $\alpha_2 = \alpha_{R_3^{(2)}/\mathfrak{q}}$ on $X_1 = X_{R_3^{(2)}/\mathfrak{p}} \subset F_2^{\mathbb{Z}^3}$ and $X_2 = X_{R_3^{(2)}/\mathfrak{q}} \subset F_2^{\mathbb{Z}^3}$, respectively, by (7.2)–(7.3). From Table 1 it is clear that α_1 and α_2 are mixing and have zero entropy.

We write $\star$ for the component-wise multiplication $(z \star z')_{\mathbf{n}} = z_{\mathbf{n}} z'_{\mathbf{n}}$ in $F_2^{\mathbb{Z}^3}$ and observe that

$$\sigma^{\mathbf{n}}(z \star z') = (\sigma^{\mathbf{n}} z) \star (\sigma^{\mathbf{n}} z')$$

for every $z, z' \in F_2^{\mathbb{Z}^3}$ and $\mathbf{n} \in \mathbb{Z}^3$ (cf. (3.1)). We claim that

$$x \star x' \in X_2 \text{ for every } x, x' \in X_1. \tag{10.7}$$

In order to verify this we define subsets $S_i \subset \mathbb{Z}^3$, $i = 0, \dots, 3$, by

$$\begin{gathered} S_0 = \mathcal{S}(f_2), \;\; S_1 = \mathcal{S}(f_1), \\ S_2 = \{(1,0,0), (1,1,0), (2,1,0)\} = \mathcal{S}(u_1 f_1), \\ S_3 = \{(0,1,0), (0,2,0), (1,1,0)\} = \mathcal{S}(u_2 f_1), \end{gathered}$$

and consider the set Z of all $z \in F_2^{S_0}$ with $\sum_{\mathbf{n} \in S_i} z_{\mathbf{n}} = 0$ for $i = 0, \dots, 3$. A calculation shows that, for every $z, z' \in Z$, the component-wise product $w = z \star z' \in F_2^{S_0}$ satisfies that $\sum_{\mathbf{n} \in S_0} w_{\mathbf{n}} = 0$. This implies (10.7).

Take a non-zero $\mathbf{m} \in \mathbb{Z}^3$ such that $\alpha_1^{\mathbf{m}} z = z$ for some non-zero $z \in X_1$ and define $\phi \colon X_1 \longrightarrow X_2$ by $\phi(x) = x \star \alpha_1^{\mathbf{m}} x$. Clearly ϕ is a $\mathbb{Z}^3$-equivariant map from (X_1, α_1) to (X_2, α_2). We choose $y \in X_1$ such that $z \star (\alpha_1^{\mathbf{m}} y - y) \neq 0_{X_2}$.

Since $\phi(0_{X_1}) = 0_{X_2}$ and $\phi(z+y) - \phi(z) - \phi(y) = z \star (\alpha_1^{\mathbf{m}} y - y) \neq 0_{X_2}$, the map ϕ is not affine.

(2) *A non-affine factor map $\psi\colon (X,\alpha) \longrightarrow (X',\alpha')$ between expansive and mixing zero-entropy algebraic $\mathbb{Z}^3$-actions, where α' has an expansive $\mathbb{Z}^2$-sub-action with completely positive entropy.* We use the same notation as in Example (1). Let $\mathfrak{r} = \mathfrak{pq} = (f_1 f_2, f_2^2) \subset R_3^{(2)}$ be the ideal generated by $f_1 f_2$ and f_2^2 and let β denote the algebraic $\mathbb{Z}^3$-action $\alpha_{R_3^{(2)}/\mathfrak{r}}$ on $Y = X_{R_3^{(2)}/\mathfrak{r}} \subset F_2^{\mathbb{Z}^3}$. From Table 1 it follows that the action (Y,β) is mixing and has zero entropy. We define continuous group homomorphisms $\theta_1\colon Y \longrightarrow X_1$ and $\theta_2\colon Y \longrightarrow X_2$ by

$$\theta_1(y) = f_2(\sigma)(y), \qquad \theta_2(y) = f_1(\sigma)(y).$$

It is easy to verify that for $i = 1,2$, $\theta_i\colon (Y,\beta) \longrightarrow (X_i,\alpha_i)$ is an algebraic factor map. Let $\psi\colon (Y,\beta) \longrightarrow (X_2,\alpha_2)$ be the $\mathbb{Z}^3$-equivariant continuous map defined by

$$\psi(x) = \theta_2(x) + \phi \circ \theta_1(x),$$

where $\phi\colon X_1 \longrightarrow X_2$ is as in the previous example. Since θ_1 is a surjective homomorphism and ϕ is non-affine, it follows that $\phi \circ \theta_1$ is non-affine, i.e. that ψ is a non-affine map. It is easy to see that the restriction of θ_2 to X_2 is a surjective map from X_2 to itself. Since $\theta_1(x) = 0$ for all $x \in X_2 \subset Y$, this shows that ψ is a non-affine factor map from (Y,β) to (X_2,α_2).

(3) *Two measurably conjugate expansive and mixing zero-entropy algebraic $\mathbb{Z}^3$-actions on non-isomorphic compact zero-dimensional abelian groups.* Let (X_1,α_1) and (X_2,α_2) be as in Example (1), and let (X,α) denote the product action $(X_1,\alpha_1) \times (X_2,\alpha_2)$. Following [3] we define a zero-dimensional compact abelian group Y and an algebraic $\mathbb{Z}^3$-action β on Y by setting $Y = X_1 \times X_2$ with composition

$$(x,y) \odot (x',y') = (x + x', x \star x' + y + y')$$

for every $(x,x'),(y,y') \in Y$, and by letting

$$\beta^{\mathbf{n}}(x,y) = (\alpha_1^{\mathbf{n}} x, \alpha_2^{\mathbf{n}} y)$$

for every $(x,y) \in Y$ and $\mathbf{n} \in \mathbb{Z}^3$. The 'identity' map $\phi\colon X \longrightarrow Y$, defined by

$$\phi(x,y) = (x,y)$$

for every $(x,y) \in X$, is obviously a topological conjugacy of (X,α) and (Y,β) with $\lambda_X \phi^{-1} = \lambda_Y$ (by Fubini's theorem). However, ϕ is not a group isomorphism. In fact, the groups X and Y are not isomorphic: since X is a subgroup $(F_2 \oplus F_2)^{\mathbb{Z}^3}$, every element in X has order 2, whereas $(x, 0_{X_2}) \in Y$ and $(x,0_{X_2}) \odot (x,0_{X_2}) = (0_{X_2}, x) \neq 0_Y$ for every nonzero $x \in X_1$.

References

[1] R.J. Baxter, *Exactly solved models in statistical mechanics*, Academic Press, New York-London, 1982.

[2] R. Berger, *The undecidability of the Domino Problem*, Mem. Amer. Math. Soc. **66** (1966).

[3] S. Bhattacharya, *Zero entropy $\mathbf{Z}^d$-actions which do not exhibit rigidity*, Duke Math. J. (to appear).

[4] S. Bhattacharya, *Higher Order Mixing and Rigidity of Algebraic Actions on Compact Abelian Groups*, Israel J. Math. (to appear), ftp://ftp.esi.ac.at/pub/Preprints/esi1127.ps.

[5] S. Bhattacharya and K. Schmidt, *Homoclinic points and isomorphism rigidity of algebraic $\mathbf{Z}^d$-actions on zero-dimensional compact abelian groups*, Israel J. Math. (to appear), ftp://ftp.esi.ac.at/pub/Preprints/esi1127.ps.

[6] R. Burton and R. Pemantle, *Local characteristics, entropy and limit theorems for spanning trees and domino tilings via transfer-impedances*, Ann. Probab. **21** (1993), 1329–1371.

[7] R. Burton and J.E. Steif, *Some 2-d symbolic dynamical systems: entropy and mixing*, in: Ergodic Theory of $\mathbb{Z}^d$-actions, ed. M. Pollicott and K. Schmidt, London Mathematical Society Lecture Note Series, vol. 228, Cambridge University Press, Cambridge, 1996, 297–305.

[8] J.W.S. Cassels, *Local Fields*, Cambridge University Press, Cambridge, 1986.

[9] M. Einsiedler, *Isomorphism and measure rigidity for algebraic actions on zero-dimensional groups*, Preprint (2002).

[10] M. Einsiedler, D. Lind, R. Miles and T.B. Ward, *Expansive subdynamics for algebraic $\mathbf{Z}^d$-actions*, Ergod. Th. & Dynam. Sys. **21** (2001), 1695–1729.

[11] M. Einsiedler and E. Lindenstrauss, *Measurable rigidity properties of $\mathbf{Z}^d$-actions on tori and solenoids*, in preparation.

[12] M. Einsiedler and K. Schmidt, *Irreducibility, homoclinic points and adjoint actions of algebraic $\mathbf{Z}^d$-actions of rank one*, in: Nonlinear Phenomena and Complex Systems, ed. A. Maass, S. Martinez and J. San Martin, Kluwer Academic Publishers, Dordrecht, 2002, 95–124.

[13] J.-H. Evertse, H.-P. Schlickewei and W. Schmidt, *Linear equations in variables which lie in a multiplicative groups*, Ann. of Math. **155** (2002), 807–836.

[14] H. Furstenberg, *Disjointness in ergodic theory, minimal sets, and a problem in diophantine approximation*, Math. Systems Theory **1** (1967), 1–49.

[15] G.A. Hedlund, *Endomorphisms and automorphisms of the shift dynamical system*, Math. Systems Theory **3** (1969), 320–375.

[16] L. Hurd, J. Kari and K. Culik, *The topological entropy of cellular automata is uncomputable*, Ergod. Th. & Dynam. Sys. **12** (1992), 255–265.

[17] P.W. Kasteleyn, *The statistics of dimers on a lattice. I*, Phys. D **27** (1961), 1209–1225.

[18] A. Katok, S. Katok and K. Schmidt, *Rigidity of measurable structure for algebraic actions of higher-rank abelian groups*, Comment. Math. Helv. **77** (2002), 718–745.

[19] A. Katok and R.J. Spatzier, *Invariant measures for higher-rank hyperbolic abelian actions*, Ergod. Th. & Dynam. Sys. **16** (1996), 751–778; *Corrections*, **18** (1998), 507–507.

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

[21] B. Kitchens and K. Schmidt, *Mixing sets and relative entropies for higher dimensional Markov shifts*, Ergod. Th. & Dynam. Sys. **13** (1993), 705–735.

[22] B. Kitchens and K. Schmidt, *Isomorphism rigidity of irreducible algebraic $\mathbf{Z}^d$-actions*, Invent. Math. **142** (2000), 559–577.

[23] S. Lang, *Algebra*, 2nd edn., Addison-Wesley, Reading, Massachusetts, 1984.

[24] F. Ledrappier, *Un champ markovien peut être d'entropie nulle et mélangeant*, C. R. Acad. Sci. Paris Sér. I Math. **287** (1978), 561–562.

[25] E.H. Lieb, *Residual entropy of square ice*, Phys. Rev. A **162** (1967), 162–172.

[26] D. Lind and K. Schmidt, *Homoclinic points of algebraic $\mathbb{Z}^d$-actions*, J. Amer. Math. Soc. **12** (1999), 953–980.

[27] D. Lind, K. Schmidt and T. Ward, *Mahler measure and entropy for commuting automorphisms of compact groups*, Invent. Math. **101** (1990), 593–629.

[28] K. Mahler, *Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen*, Nederl. Akad. Wetensch. Proc. Ser. A **38** (1935), 50–60.

[29] N.G. Markley and M.E. Paul, *Matrix subshifts for $\mathbb{Z}^n$ symbolic dynamics*, Proc. London Math. Soc. **43** (1981), 251–272.

[30] N.G. Markley and M.E. Paul, *Maximal measures and entropy for $\mathbb{Z}^n$ subshifts of finite type*, Preprint (1979).

[31] D. Masser, *Two letters to D. Berend*, dated 12th and 19th September, 1985.

[32] D. Masser, *Mixing and equations over groups in positive characteristic*, ftp://ftp.esi.ac.at/pub/Preprints/esi1216.ps, 2002.

[33] J. Milnor, *Directional entropies of cellular automaton maps*, in: Disordered Systems and Biological Organization, ed. E. Bienenstock et. al., NATO ASI Series, vol. F20, Springer Verlag, Berlin-Heidelberg-New York, 1986.

[34] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 2nd. ed., Springer Verlag, Berlin-Heidelberg-New York, 1990.

[35] D.S. Ornstein and B. Weiss, *Entropy and isomorphism theorems for actions of amenable groups*, J. Analyse Math. **48** (1987), 1–141.

[36] R.M. Robinson, *Undecidability and nonperiodicity for tilings of the plane*, Invent. Math. **12** (1971), 177–209.

[37] D.J. Rudolph, $\times 2$ *and* $\times 3$ *invariant measures and entropy*, Ergod. Th. & Dynam. Sys. **10** (1990), 395–406.

[38] D.J. Rudolph and K. Schmidt, *Almost block independence and Bernoullicity of $\mathbb{Z}^d$-actions by automorphisms of compact groups*, Invent. Math. **120** (1995), 455–488.

[39] K. Schmidt, *Mixing automorphisms of compact groups and a theorem by Kurt Mahler*, Pacific J. Math. **137** (1989), 371–384.

[40] K. Schmidt, *Algebraic ideas in ergodic theory*, CBMS Lecture Notes, vol. 76, American Mathematical Society, Providence, R.I., 1990.

[41] K. Schmidt, *Automorphisms of compact abelian groups and affine varieties*, Proc. London Math. Soc. **61** (1990), 480–496.

[42] K. Schmidt, *Dynamical Systems of Algebraic Origin*, Birkhäuser Verlag, Basel-Berlin-Boston, 1995.

[43] K. Schmidt, *Tilings, fundamental cocycles and fundamental groups of symbolic $\mathbb{Z}^d$-actions*, Ergod. Th. & Dynam. Sys. **18** (1998), 1473–1525.

[44] K. Schmidt, *The dynamics of algebraic $\mathbf{Z}^d$-actions*, in: European Congress of Mathematics (Barcelona 2000), Vol. I, ed. C. Casacuberta, R.M. Miró-Roig, J. Verdera and S. Xambó-Descamps, Progress in Mathematics, vol. 201, Birkhäuser Verlag, Basel-Berlin-Boston, 2001, 543–553.

[45] K. Schmidt and T. Ward, *Mixing automorphisms of compact groups and a theorem of Schlickewei*, Invent. Math. **111** (1993), 69–76.

[46] R. Solomyak, *On coincidence of entropies for two classes of dynamical systems*, Ergod. Th. & Dynam. Sys. **18** (1998), 731–738.

[47] H.N.V. Temperley and M.E. Fisher, *Dimer problem in statistical mechanics—an exact result*, Philos. Mag. **6** (1961), 1061–1063.

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

[49] H. Wang, *Proving theorems by pattern recognition II*, AT&T Bell Labs. Tech. J. **40** (1961), 1–41.
[50] A. Weil, *Basic Number Theory*, Springer Verlag, Berlin-Heidelberg-New York, 1974.