VALUATIONS AND HYPERBOLICITY IN DYNAMICS

THOMAS WARD

PRODYN Summer School June-July 2001
Georg-August-Universität Göttingen

Contents

1. Introduction

One of the most basic dynamical ideas is that of a *local portrait of hyperbolicity* (or non-hyperbolicity). This is a picture of how the map acts in a neighbourhood of a point (or, equivalently, on a covering space).

Example 1.1. [A contracting homothety] Consider the map on $\mathbb{R}^2$ given by $f : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}$ with $\lambda \in (0,1)$. The local portrait Figure 1 around the fixed point 0 shows the dynamics of iterating f: all orbits are sucked exponentially towards 0.

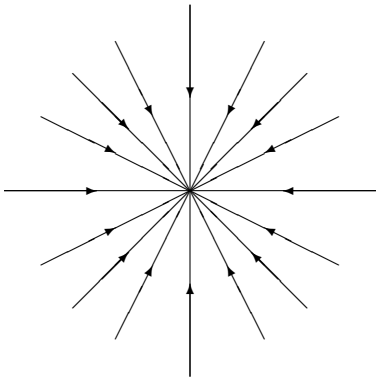

Figure 1. A contracting homothety

A more realistic example is given by a hyperbolic toral automorphism.

Example 1.2. Consider the map $f : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ on $\mathbb{R}^2$. Figure 2 shows the eigenvectors in bold, and orbits of points being attracted to the unstable direction.

Our purpose in these notes is to explore several questions.

(1) In which dynamical settings can these kind of portraits be usefully made?
(2) More generally, in which dynamical settings does the action seen through a valuation tell you anything?
(3) Finally, can valuations in low-dimensional systems help us to understand actions of higher-rank groups?

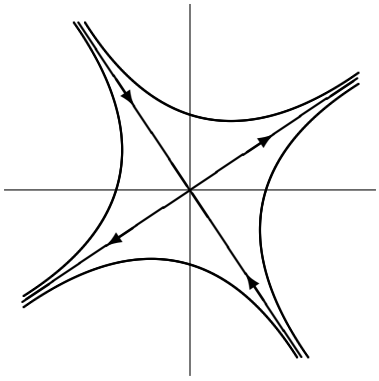

FIGURE 2. A hyperbolic automorphism

2. S-INTEGER DYNAMICAL SYSTEMS

2.1. **Definition and examples.** The S-integer dynamical systems are a very simple collection of dynamical systems which are the pieces from which group automorphisms may be built up. Most of the material here is taken from [11]. An excellent modern treatment of Tate's thesis and related material is the text of Ramakrishnan and Valenza, [57].

Let k be an $\mathbb{A}$–field in the sense of Weil (that is, k is an algebraic extension of the rational field $\mathbb{Q}$ or of $\mathbb{F}_q(t)$ for some rational prime q), and let $\mathbb{P}(k)$ denote the set of places of k. A place $w \in \mathbb{P}(k)$ is *finite* if w contains only non–archimedean valuations and is *infinite* otherwise (with one exception: for the case $\mathbb{F}_p(t)$ the place given by t^{-1} is regarded as being an *infinite* place despite giving rise to a non–archimedean valuation).

Example 2.1. For the case $k_0 = \mathbb{Q}$ or $k_0 = \mathbb{F}_q(t)$, the places are defined as follows.

THE RATIONALS $\mathbb{Q}$. The places of $\mathbb{Q}$ are in one–to–one correspondence with the set of rational primes $\{2, 3, 5, 7, \dots\}$ together with one additional place ∞ at infinity. The corresponding valuations are $|r|_\infty = |r|$ (the usual archimedean valuation), and for each p, $|r|_p = p^{-\operatorname{ord}_p(r)}$, where $\operatorname{ord}_p(r)$ is the (signed) multiplicity with which the rational prime p divides the the rational r.

THE FUNCTION FIELD $\mathbb{F}_q(t)$. For $\mathbb{F}_q(t)$ there are no archimedean places. For each monic irreducible polynomial $v(t) \in \mathbb{F}_q[t]$ there is a distinct place v, with corresponding valuation given by

$$|f|_v = q^{-\operatorname{ord}_v(f)\cdot\deg(v)},$$

where $\operatorname{ord}_v(f)$ is the signed multiplicity with which v divides the rational function f. There is one additional place given by $v(t) = t^{-1}$,

and this place will be called an infinite place even though the corresponding valuation is non–archimedean. This 'infinite' place is defined by $|f|_\infty = q^{-\operatorname{ord}_t(f(t^{-1}))}$.

Let k be a finite extension of k_0. A place $w \in \mathbb{P} = \mathbb{P}(k)$ is said to lie above a place v of $k_0 = \mathbb{Q}$ or $\mathbb{F}_q(t)$, denoted $w|v$, if $|\cdot|_w$ rectricted to the base field $k_0 \subset k$ coincides with $|\cdot|_v$. Denote by k_w the (metric) completion of k under the metric $d_w(x,y) = |x-y|_w$ on k. The *local degree* is defined by $d_w = [k_w : (k_0)_v]$. Choose a normalized valuation $|\cdot|_w$ corresponding to the place w to have

$$|x|_w = |x|_v^{d_w/d}$$

for each $x \in k_0\backslash\{0\}$, where $d = [k : k_0]$ is the global degree. With the above normalizations we have the Artin product formula [80, p. 75]

$$\prod_{w\in\mathbb{P}(k)} |x|_w = 1 \tag{2.1}$$

for all $x \in k\backslash\{0\}$.

For each finite place w of k, the field k_w is a local field, and the maximal compact subring of k_w is

$$r_w = \{x \in k\colon |x|_w \leq 1\}.$$

Elements of r_w are called w–adic integers in k_w. The group of units in the ring r_w is

$$r_w^* = \{x \in k\colon |x|_w = 1\}.$$

Let $\mathbb{P}_\infty = \mathbb{P}_\infty(k)$ denote the set of infinite places of k.

Definition 2.2. Let k be an $\mathbb{A}$–field. Given an element $\xi \in k^*$, and any set $S \subset \mathbb{P}(k)\backslash\mathbb{P}_\infty(k)$ with the property that $|\xi|_w \leq 1$ for all $w \notin S\cup\mathbb{P}_\infty$, define a dynamical system $(X,\alpha) = (X^{(k,S)}, \alpha^{(k,S,\xi)})$ as follows. The compact abelian group X is the dual group to the discrete countable group of S–integers R_S in k, defined by

$$R_S = \{x \in k\colon |x|_w \leq 1 \text{ for all } w \notin S \cup \mathbb{P}_\infty(k)\}.$$

The continuous group endomorphism $\alpha : X \to X$ is dual to the monomorphism $\widehat{\alpha} : R_S \to R_S$ defined by $\widehat{\alpha}(x) = \xi x$.

Dynamical systems of the form $(X^{(k,S)}, \alpha^{(k,S,\xi)})$ are called S–integer dynamical systems. Following conventions from number theory, we shall divide these into two classes: *arithmetic* systems when k is a number field, and *geometric* when k has positive characteristic. To clarify this definition – and to show how these systems connect with previously studied ones – several examples follow.

Example 2.3. (1) Let $k = \mathbb{Q}$, $S = \emptyset$, and $\xi = 2$. Then

$$R_S = \{x \in \mathbb{Q} \colon |x|_p \leq 1 \text{ for all primes } p\} = \mathbb{Z},$$

so $X = \mathbb{T}$ and α is the circle doubling map.

(2) Let $k = \mathbb{Q}$, $S = \{2\}$, and $\xi = 2$. Then

$$R_S = \{x \in \mathbb{Q} \colon |x|_p \leq 1 \text{ for all primes } p \neq 2\} = \mathbb{Z}[\tfrac{1}{2}],$$

so X is the solenoid $\widehat{\mathbb{Z}[\frac{1}{2}]}$, and α is the automorphism of X dual to the automorphism $x \mapsto 2x$ of R_S. This is the natural invertible extension of the circle doubling map [13, Example (c)] or [31, Sect. 2].

As pointed out in [6, Chap. 1 Example D], this dynamical system is topologically conjugate to the system (Y, β) defined as follows. Let $D = \{z \in \mathbb{C} \colon |z| \leq 1\}$ and $S^1 = \{z \in \mathbb{C} \colon |z| = 1\}$. Define a map $f : S^1 \times D \to S^1 \times D$ by

$$f(z, \omega) = (z^2, \tfrac{1}{2}z + \tfrac{1}{4}\omega).$$

Let $Y = \bigcap_{n \in \mathbb{N}} f^n(S^1 \times D)$ and let β be the map induced by f on Y. Then there is a homeomorphism $Y \to X$ that intertwines the maps β and α. For more details on this example and related "DE" (derived from expanding) examples, see, [69, Section I.9]; for a thorough and detailed treatment of this dyadic example see [34, Sect. 17.1].

(3) Let $k = \mathbb{Q}$, $S = \{2, 3\}$, $\xi = \frac{3}{2}$. Then $R_S = \mathbb{Z}[\frac{1}{6}]$, and α is the map dual to multiplication by $\frac{3}{2}$ on R_S. This map has dense periodic points by [47, Sect. 3] and has topological entropy $\log 3$ by [47, Sect. 2].

(4) Let $k = \mathbb{Q}$, $S = \{2, 3, 5, 7, 11, \dots\}$, and $\xi = \frac{3}{2}$. Then $R_S = \mathbb{Q}$ and α is the automorphism of the full solenoid $\widehat{\mathbb{Q}}$ dual to multiplication by $\frac{3}{2}$ on $\mathbb{Q}$. This map has only one periodic point for any period by [47, Sect. 3] and has topological entropy $\log 3$ by [47, Sect. 2].

(5) Let ξ be an algebraic integer, $k = \mathbb{Q}(\xi)$ and $S = \emptyset$. Then R_S is the ring of algebraic integers in k. Taking $\xi = \sqrt{2} - 1 + i\sqrt{2\sqrt{2} - 2}$ gives a non–expansive quasihyperbolic automorphism of the 4–torus as pointed out in [44, Sect. 3]

(6) Let $k = \mathbb{F}_q(t)$, $S = \emptyset$, and $\xi = t$. Then $R_S = \mathbb{F}_q[t]$, and so $X = \widehat{R_S} = \prod_{i=0}^{\infty} \{0, 1, \dots, q-1\}$. The map α is therefore the full one–sided shift on q symbols.

(7) Let $k = \mathbb{F}_q(t)$, $S = \{t\}$, and $\xi = t$. Recall that the valuation corresponding to t is $|f|_t = q^{-\operatorname{ord}_t(f)}$, so $|t|_t = q^{-1}$. The ring of S–integers is

$$R_S = \{f \in \mathbb{F}_q(t) \colon |f|_w \leq 1 \text{ for all } w \neq t, t^{-1}\} = \mathbb{F}_q[t^{\pm 1}].$$

The dual of R_S is then $\prod_{-\infty}^{\infty}\{0,1,\ldots,q-1\}$, and in this case α is the full two–sided shift on q symbols.

(8) Let $k=\mathbb{F}_q(t)$, $S=\{t\}$, and $\xi=1+t$. Then X is the two–sided shift space on q symbols, and α is the cellular automaton defined by

$$(\alpha(x))_k = x_k + x_{k+1} \bmod q.$$

(9) Let $k=\mathbb{F}_q(t)$, $S=\{t,1+t\}$, and $\xi=1+t$. Then α is the invertible extension of the cellular automaton in (8).

(10) Let α be an ergodic automorphism of a finite–dimensional torus. For each subset S of the rational primes let $\Gamma_S=\widehat{X}\otimes_{\mathbb{Z}}\mathbb{Z}[\frac{1}{S}]$. Then α defines an endomorphism $\alpha_S:\widehat{\Gamma_S}\to\widehat{\Gamma_S}$. Each α_S has the same entropy as α by [47] (and is therefore measurably isomorphic to α), but they are all topologically distinct, so $\{\alpha_S\}$ forms an uncountable family of topological dynamical systems all measurably isomorphic to each other.

(11) Not all toral endomorphisms are S–integer dynamical systems. Let $\alpha_A:\mathbb{T}^n\to\mathbb{T}^n$ be the toral endomorphism corresponding to the integer matrix $A\in M_n(\mathbb{Z})$. Assume that the characteristic polynomial χ_A of A is irreducible, let λ have $\chi_A(\lambda)=0$ and let $\mathbf{a}=(a_1,\ldots,a_n)^t$ be a vector in $\mathbb{Q}(\lambda)^n$ with $A\mathbf{a}=\lambda\mathbf{a}$ with the property that $\mathfrak{a}=a_1R_\lambda+\cdots+a_nR_\lambda$ is an ideal in the ring $R_\lambda=\mathbb{Z}[\lambda]$. Two ideals determined in this way from the same matrix belong to the same ideal class by [71, Th. 2].

Lemma 2.4. *The toral endomorphism α is topologically conjugate to the S–integer dynamical system given by $k=\mathbb{Q}(\lambda)$, $\xi=\lambda$, $S=\emptyset$ if and only if $\mathfrak{a}$ defines a trivial element in the ideal class group of R_λ.*

Proof. Let B be the companion matrix to the polynomial χ_A. Then there is an isomorphism from $\left(X^{(k,S)},\alpha^{(k,\xi,S)}\right)$ to $(\mathbb{T}^n,\alpha_B)$. If $\mathfrak{a}$ defines a trivial element in the ideal class group of R_λ, then by [71], there is a matrix $S\in GL_n(\mathbb{Z})$ such that $A=SBS^{-1}$, so there is an isomorphism from $(\mathbb{T}^n,\alpha_B)$ to $(\mathbb{T}^n,\alpha_A)$.

Conversely, let $\theta:(\mathbb{T}^n,\alpha_A)\to\left(X^{(k,S)},\alpha^{(k,\xi,S)}\right)$ be a topological conjugacy. Let H_1 denote the first Čech homology functor with coefficients in $\mathbb{T}$; H_1 sends any diagram of solenoids and endomorphisms to an isomorphic diagram by [36, Lemma 6.3]. Then $H_1(\theta)$ defines an isomorphism from $(\mathbb{T}^n,\alpha_A)$ to $\left(X^{(k,S)},\alpha^{(k,\xi,S)}\right)$; since $X^{(k,S)}$ is an n–dimensional torus, $\alpha^{(k,\xi,S)}$ corresponds to some matrix $C\in M_n(\mathbb{Z})$, and this isomorphism is given by a matrix $S\in GL_n(\mathbb{Z})$ with $A=SCS^{-1}$. It follows by [71] that $\mathfrak{a}$ defines a trivial element in the ideal class group of R_λ. □

2.2. **Background on adeles.** In this section we assemble some basic facts about the ring R_S. For the case $S = \emptyset$ most of this is straightforward. At the opposite extreme, when S contains all finite places (so $R_S = k$), the adelic constructions of [80, Chap. IV] show how to cover the group $X^{(k,S)}$. In the intermediate case, straightforward modifications of Weil's arguments are needed. The construction is also given in Tate's thesis, and we indicate below how to read off the results we shall need from this.

Fix an $\mathbb{A}$–field k and a set S of finite places of k.

Definition 2.5. The S–adele ring of k is the ring

$$k_{\mathbb{A}}(S) = \left\{ x = (x_\nu) \in \prod_{\nu \in S \cup \mathbb{P}_\infty} k_\nu : |x_\nu|_\nu \leq 1 \text{ for all but finitely many } \nu \right\},$$

with the topology induced by the following property. For each finite set $S' \subset S$, the locally compact subring $k_{\mathbb{A}}^{S'} \subset k_{\mathbb{A}}(S)$ defined by

$$k_{\mathbb{A}}^{S'} = \prod_{\nu \in S' \cup \mathbb{P}_\infty} k_\nu \times \prod_{\nu \in S \setminus S'} r_\nu$$

(with the product topology) is an open subring of $k_{\mathbb{A}}(S)$, and a fundamental system of open neighbourhoods of 0 in the additive group of $k_{\mathbb{A}}(S)$ is given by a fundamental system of neighbourhoods of 0 in any one of the subrings $k_{\mathbb{A}}^{S'}$.

Notice that $k_{\mathbb{A}}(S)$ is locally compact since each r_ν is compact.

Define a map $\Delta : R_S \to k_{\mathbb{A}}(S)$ by $\Delta(x) = (x, x, x, \dots)$. This map is a well–defined ring homomorphism: notice that for $\alpha \in R_S$, $|\alpha|_\nu \leq 1$ for all but finitely many ν by [80, Th. III.1.3].

In [70], Tate introduces the notion of an *abstract restricted direct product*, under the hypothesis that P $(= S \cup \mathbb{P}_\infty)$ is an arbitrary countable set of indices (places). Let $G_{\mathcal{P}}$ $(= k_\nu)$ be a locally compact abelian group for $\mathcal{P} \in P$, and for all but finitely many $\mathcal{P}$, let $H_{\mathcal{P}}$ $(= r_\nu)$ be an open compact subgroup of $G_{\mathcal{P}}$. The restricted direct product is defined as

$$G(P) = \left\{ g = (g_{\mathcal{P}}) \in \prod_{\mathcal{P} \in P} G_{\mathcal{P}} : g_{\mathcal{P}} \in H_{\mathcal{P}} \text{ for all but finitely many } \mathcal{P} \right\},$$

a locally compact abelian topological group. We topologise $G(P)$ by choosing a fundamental system of neighbourhoods of 1 in $G(P)$ of the form $N = \prod_{\mathcal{P} \in P} N_{\mathcal{P}}$, where each $N_{\mathcal{P}}$ is a neighbourhood of 1 in $G_{\mathcal{P}}$ and $N_{\mathcal{P}} = H_{\mathcal{P}}$ for all but finitely many $\mathcal{P}$, which accords with the topology in Definition 2.5.

The key results proved in [70, Lem. 3.2.2, Th. 3.2.1] are the following.

(1) $\Delta(R_S)$ is discrete in $k_{\mathbb{A}}(S)$ and $k_{\mathbb{A}}(S)/\Delta(R_S)$ is compact,
(2) $R_S^{\perp} \cong R_S$, $\widehat{k_{\mathbb{A}}(S)} \cong k_{\mathbb{A}}(S)$ and so $k_{\mathbb{A}}(S)/\Delta(R_S) \cong \hat{R}_S$

where S is an arbitrary set of finite places of an $\mathbb{A}$–field k. We collect these remarks in the following Theorem, which is an extension of one of the "Main Theorems" in [80, Chap. IV, Sect. 2] to arbitrary sets of places.

Theorem 2.6. *The map $\Delta : R_S \to k_{\mathbb{A}}(S)$ embeds R_S as a discrete cocompact subring in the S–adele ring of k. There is an isomorphism between the S–adele ring $k_{\mathbb{A}}(S)$ and itself, which induces an isomorphism between $\widehat{R_S}$ and $k_{\mathbb{A}}(S)/\Delta(R_S)$.*

Remark 2.7. The S–adele ring $k_{\mathbb{A}}(S)$ covering the dynamical system $(X^{(k,S)}, \alpha^{(k,S,\xi)})$ gives a complete local portrait of the hyperbolicity. A neighbourhood of the identity in $X^{(k,S)}$ is isometric to a neighbourhood of the identity in $k_{\mathbb{A}}(S)$. The map $\alpha^{(k,S,\xi)}$ under this isometry acts on each quasi–factor k_ν by multiplication, dilating the metric on that quasi–factor by $|\xi|_\nu$. If S is infinite, then the local action is an isometry on all but finitely many quasi–factors, making such systems very far from hyperbolic ones.

2.3. **Adelic covering space.** We first recall how covering spaces arise for familiar maps. If $f : \mathbb{T} \to \mathbb{T}$ is the doubling map $x \mapsto 2x \bmod 1$ on the additive circle, then the cover $\pi : \mathbb{R} \to \mathbb{T}$ lifts the map to $\tilde{f} : \mathbb{R} \to \mathbb{R}$. Figure 3 shows the lifted map: notice that the projection π is a *local isometry*. The import of Section 2.2 is that the same thing

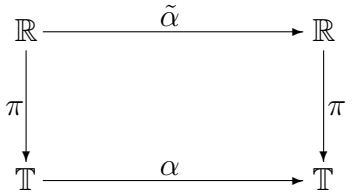

FIGURE 3. Lifting the circle doubling map

happens for any S-integer dynamical system.

Example 2.8. Let α be the S–integer dynamical system corresponding to $k = \mathbb{F}_p(t)$, $S = \{t\}$ and $\xi = t$ (so the corresponding dynamical system is the full p-shift). The covering space is the product $k_\infty \times k_v$ where v is the valuation corresponding to t and ∞ the valuation

corresponding to t^{-1}. The local hyperbolicity portrait in the covering space is shown in Figure 4.

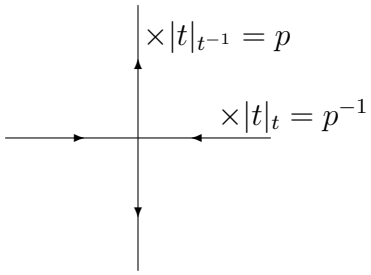

FIGURE 4. Multiplication by t is hyperbolic for $S = \{t\}$

The system is hyperbolic, which shows up in having extremely regular properties (for example, the dynamical zeta function is rational).

Example 2.9. A non-hyperbolic additive cellular automaton is given by choosing $k = \mathbb{F}_p(t)$, $S = \{t\}$ and $\xi = 1 + t$. This is the additive cellular automata with local rule given by

$$f(x_0, x_1) = x_0 + x_1.$$

If $p = 2$ this is 'rule 102' in the standard description of cellular automata with radius 1. The covering space is the same product. The local hyperbolicity portrait is shown in Figure 5, which indicates why this system is non–hyperbolic.

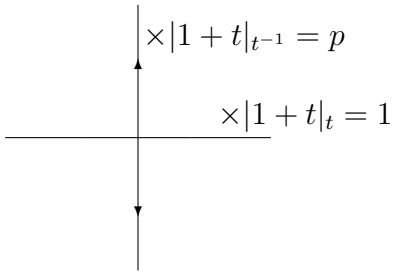

FIGURE 5. Local effect of multiplication by $1 + t$

The non-hyperbolicity makes the dynamics extremely complicated: the direction in which the map acts likes an isometry behaves like a sort of rotation, destroying some (but not all) periodic points.

The final example is a connected group automorphism.

Example 2.10. Let $k = \mathbb{Q}$, $S = \{2, 3\}$ and $\xi = 2$. This system is an isometric extension of the invertible extension of the circle doubling map. The covering space is $\mathbb{R} \times \mathbb{Q}_2 \times \mathbb{Q}_3$.

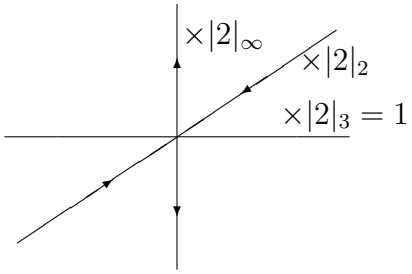

FIGURE 6. Local effect of multiplying by 2 on $\widehat{\mathbb{Z}[\frac{1}{6}]}$

2.4. **Topological entropy.** For any automorphism $\alpha : X \to X$ of a compact metrizable group X, the topological entropy $h(\alpha)$ may be defined in several different ways. The most convenient formulation is that of Bowen [5], where the topological entropy is expressed as a local rate of volume growth.

Definition 2.11. The topological entropy of the compact group automorphism $\alpha : X \to X$ is defined to be

$$h_{Bowen}(\alpha) = \lim_{\epsilon \searrow 0} \limsup_{n\to\infty} -\frac{1}{n} \log \mu \left(\bigcap_{k=0}^{n-1} \alpha^{-k} \left(B_\epsilon(\alpha^k x) \right) \right),$$

where x is any point, μ is Haar measure, and B_ϵ denotes the metric open ball around x.

Bowen [5, Prop. 7] is that

$$h(\alpha) = h_{Bowen}(\alpha).$$

This gives a very straightforward way to compute the entropy of automorphisms of solenoids (compact, connected, finite-dimensional groups) – this entropy was computed originally by Yuzvinskii [83], and then a much simpler proof using Bowen's formulation and the adelic covering space was given in [47] and [73] for the solenoid case. The geometric case, which includes certain cellular automata is similar (see [79]).

Theorem 2.12. *The topological entropy of an S–integer system is given by*

$$h(\alpha^{(k,S,\xi)}) = \sum_{w \in S \cup \mathbb{P}_\infty(k)} \log^+ |\xi|_w \tag{2.2}$$

Proof. The proof is sketched for a simple case. Assume that the field k has positive characteristic (so all the places are non-Archimedean) and

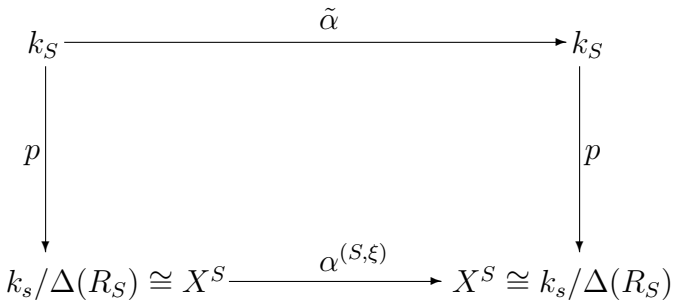

FIGURE 7. Adelic covering space

assume that the set S is finite (so the topology on the S-adele ring is simple the product topology).

Using Section 2.2 the group R_S embeds as a discrete subgroup of $\prod_{\nu\in S\cup\mathbb{P}_\infty} k_\nu$ with compact quotient, and there is a map $p : k_S \to k_s/\Delta(R_S)$; Theorem 2.6 means that there is a commutative diagram expressing the adelic covering space k_S, shown in Figure 7.

in which the map p is a local isometry and $\tilde{\alpha}$ denotes multiplication by ξ in each coordinate.

It follows by [5, Th. 9, 20] that

$$h(\alpha) = h(\tilde{\alpha}) = \lim_{\epsilon\searrow 0} \limsup_{n\to\infty} -\frac{1}{n} \log \mu \left(\bigcap_{j=0}^{n-1} \tilde{\alpha}^{-j}(B_\epsilon) \right) \tag{2.3}$$

where B_ϵ is the metric open ball of radius ϵ around the identity, μ is Haar measure on the locally compact group $\prod_{\nu\in S\cup\mathbb{P}_\infty} k_\nu$, and $\tilde{\alpha}$ is the lifted map $(x_\nu)_{\nu\in S\cup\mathbb{P}_\infty} \mapsto (\xi x_\nu)_{\nu\in S\cup\mathbb{P}_\infty}$ on the covering space $\prod_{\nu\in S\cup\mathbb{P}_\infty} k_\nu$.

Since S is finite, we may use the max metric on $\prod_{\nu\in S\cup\mathbb{P}_\infty} k_\nu$. It follows that

$$B_\epsilon = \{(x_\nu) : |x|_\nu < \epsilon \ \forall\ \nu \in S \cup \mathbb{P}_\infty\}.$$

Now the covering map from $\prod_{\nu\in S\cup\mathbb{P}_\infty} k_\nu$ onto X^S gives a local portrait of the hyperbolicity.

For example, if $S \cup \mathbb{P}_\infty = \{\nu_1, \nu_2, \nu_3\}$ say, and $|\xi|_{\nu_1} > 1$, $|\xi|_{\nu_2} > 1$, $|\xi|_{\nu_3} < 1$ then the local dynamics in a neighbourhood of the identity in X^S is illustrated in Figure 8. The box B_ϵ is transformed under $\tilde{\alpha}^{-1}$ (multiplication by ξ^{-1}) into a squashed box with sides of length $2\epsilon|\xi|_{\nu_1}^{-1}$, $2\epsilon|\xi|_{\nu_2}^{-1}$, $2\epsilon|\xi|_{\nu_3}^{-1}$ in the directions corresponding to ν_1, ν_2, ν_3 respectively. In the covering space the effect of multiplying the box B_ϵ by ξ^{-1} gives

$$\begin{aligned}\tilde{\alpha}^{-j}(B_\epsilon) &= \{(x_\nu) : |\xi^j x|_\nu < \epsilon \ \forall\ \nu \in S \cup \mathbb{P}_\infty\} \\ &= \{(x_\nu) : |x|_\nu < \epsilon/|\xi|_\nu^j \ \forall\ \nu \in S \cup \mathbb{P}_\infty\}.\end{aligned}$$

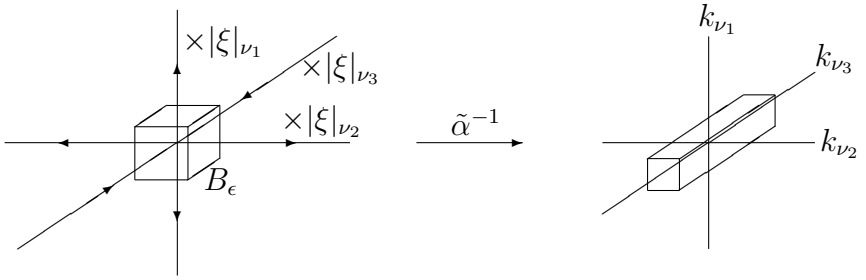

FIGURE 8. Multiplying B_ϵ by ξ^{-1} for $S \cup \mathbb{P}_\infty = \{\nu_1, \nu_2, \nu_3\}$

Thus the set

$$D(n,\epsilon) = \bigcap_{j=0}^{n-1} \tilde{\alpha}^{-j}(B_\epsilon)$$

is a 'box' with one side for each term $\nu \in S \cup \mathbb{P}_\infty$, and the 'length' of each side is

$$\min\{\epsilon, \epsilon/|\xi|_\nu, \epsilon/|\xi|_\nu^2, \ldots, \epsilon/|\xi|_\nu^{n-1}\} = \begin{cases} \epsilon & \text{if } |\xi|_\nu \leq 1, \\ \epsilon/|\xi|_\nu^{n-1} & \text{if } |\xi|_\nu > 1. \end{cases} \tag{2.4}$$

It follows that

$$\mu\left(D(n,\epsilon)\right) = \epsilon^{|S\cup\mathbb{P}_\infty|} \cdot \left(\prod_{\nu:|\xi|_\nu>1} |\xi|_\nu^{n-1} \right)^{-1},$$

which when substituted into (2.3) gives the formula (2.12). □

2.5. **Dynamical properties.** Recall the following standard criterion for ergodicity of compact group automorphisms.

Theorem 2.13. *If X is a compact metrizable abelian group and $\alpha : X \to X$ is a surjective continuous endomorphism then Haar measure is ergodic for T if and only if the trivial character $\gamma \equiv 1$ is the only $\gamma \in \hat{X}$ satisfying $\gamma \circ T^n = \gamma$ for some $n > 0$.*

Proof. See [29, Th. 1]. □

Corollary 2.14. *Let $(X, \alpha) = (X^{(k,S)}, \alpha^{(k,S,\xi)})$ be an S–integer dynamical system. Then α is ergodic if and only if ξ is not a root of unity.*

It follows that in the geometric case α is ergodic if and only if $\xi \notin \mathbb{F}_p^*$.

Proof. The map α is non–ergodic if and only if there is a $r \in R_S \backslash \{0\}$ with $\xi^m r = r$ for some $m \neq 0$. This is possible in a field if and only if ξ is a unit root. □

Recall that a continuous map $\alpha : (X, d) \to (X, d)$ is *forwardly expansive* if there is a constant $\delta > 0$ such that for each pair $x \neq y \in X$ there is some $n \in \mathbb{N}$ with $d(\alpha^n x, \alpha^n y) > \delta$. A homeomorphism $\beta : (X, d) \to (X, d)$ is *expansive* if there is a constant $\delta > 0$ such that for each pair $x \neq y \in X$ there is some $n \in \mathbb{Z}$ with $d(\beta^n x, \beta^n y) > \delta$. Homeomorphisms can only be forwardly expansive on finite metric spaces – this observation seems to have been first made in the Ph.D. thesis of Schwartzman; a proof is in [13].

Theorem 2.15. *Let K be a non–discrete field complete with respect to a valuation $|\cdot|$, and let $\bar{K}$ denote the algebraic closure of K with the uniquely extended absolute value from K. Let E be a finite dimensional vector space over K, and let u be an automorphism of E. Then u is expansive if and only if $|\lambda| \neq 1$ for each eigenvalue λ of u in $\bar{K}$.*

Proof. See Eisenberg's paper [23, Th. 3]. □

There is an infinite-dimensional analogue of Eisenberg's result – see [24].

Corollary 2.16. *Let $(X, \alpha) = (X^{(k,S)}, \alpha^{(k,S,\xi)})$ be an S–integer dynamical system. Then α is expansive if and only if $S \cup \mathbb{P}_\infty \subseteq \{\nu \leq \infty : |\xi|_\nu \neq 1\}$.*

Proof. Recall that there is a local isometry between $k_{\mathbb{A}}(S)$ and X, so it is enough to check expansiveness of the lifted map on $k_{\mathbb{A}}(S)$. Here Eisenberg's criterion in Theorem 2.15 applies to each of the (finitely many) indicated quasifactors. □

Remark 2.17. Corollary 2.16 is a generalisation of [65, Prop. 7.2] where Schmidt considers k to be a number field and $S = \{\nu < \infty : |\xi|_\nu \neq 1\}$.

2.6. **Periodic points.** One of the remarkable features of S-integer systems is that there is an exact formula for the number of periodic points. To see where this comes from, go back to the circle doubling map, $\alpha : \mathbb{T} \to \mathbb{T}$. Finding the points of period n under this map amounts to solving the equation $(2^n - 1)x = 0 \bmod 1$ on $\mathbb{T}$. One way to count solutions to this equation is to use the covering space $\pi : \mathbb{R} \to \mathbb{T}$ again: fix a fundamental domain F for π (this could be $[0, 1)$ say – but it does not really matter as long as it is a measurable set) and consider the image of F under $\times(2^n - 1)$ in the covering space: write $G = (2^n - 1)F$. I claim that the set G contains exactly $(2^n - 1)$ integers, and the pre-image of each of these under multiplication by $(2^n - 1)$ gives a unique point of period n. It follows that the number of points

of period n is equal to the amount by which the map $x \mapsto (2^n - 1)x$ scales Lebesgue measure on $\mathbb{R}$.

Let Γ be a discrete cocompact subgroup of a locally compact abelian group X. A *fundamental domain* F of X modulo Γ is a full (measurable) set of coset representatives of Γ in X. Denote by μ the Haar measure on X normalised to give $\mu(F) = 1$. Let $\tilde{A} : X \to X$ be a continuous surjective mapping with $\tilde{A}(\Gamma) \subset \Gamma$, and let $A : X/\Gamma \to X/\Gamma$ be the induced map on the quotient space.

Lemma 2.18. *If* $\ker A$ *is discrete, then*

$$\mathrm{mod}_X(\tilde{A}) = |\ker A|.$$

Proof. Since Γ is discrete in X, a fundamental domain F may be chosen so that there exists a neighbourhood $U(0_X)$ of the identity $0_X \in X$ with $U(0_X) \subset F$. The finiteness of $|\ker A|$ follows from the fact that X/Γ is compact. So for a sufficiently small neighbourhood $V(0_{X/\Gamma})$ of the identity $0_{X/\Gamma} \in X/\Gamma$,

$$A^{-1}V(0_{X/\Gamma}) = \bigcup_{i=1,\ldots,|\ker A|} V_i,$$

where each V_i is a neighbourhood of a point in the set $A^{-1}(0_{X/\Gamma})$ and their union is disjoint. Since A is measure–preserving, $\mu\left(A^{-1}V(0_{X/\Gamma})\right) = \mu\left(V(0_{X/\Gamma})\right)$. Once again using the discreteness of Γ in X we have that X is locally isomorphic to X/Γ. This means that, assuming the neighbourhoods $U(0_X)$ and $V(0_{X/\Gamma})$ are small enough, $\pi|_{U(0_X)}$ is a homeomorphism between $U(0_X)$ and $V(0_{X/\Gamma})$. Thus we have

$$\begin{aligned} \mu\left(\tilde{A}U(0_X)\right) &= \mu\left(AV(0_{X/\Gamma})\right) \\ &= |\ker A|\mu\left(V(0_{X/\Gamma})\right) \\ &= |\ker A|\mu\left(U(0_X)\right) \end{aligned}$$

which proves the Lemma. Furthermore, since $U(0_X) \subset F$, $\mu(\tilde{A}F) = |\ker A|$. □

Lemma 2.19. *Let* $(X, \alpha) = (X^{(k,S)}, \alpha^{(k,S,\xi)})$ *be an* S*–integer dynamical system. Then the number of points of period* $n \geq 1$ *is finite if* α *is ergodic, and*

$$|\mathrm{Per}_n(\alpha)| = \prod_{\nu \in S \cup \mathbb{P}_\infty} |\xi^n - 1|_\nu.$$

Proof. A fundamental domain of $k_{\mathbb{A}}(S)$ modulo k is a set

$$F = \begin{cases} [0,1)^d \times \prod_{\nu\in S} r_\nu & \text{if } k \text{ is a number field with } d = [k:\mathbb{Q}], \\ \text{Finite} \times \prod_{\nu\in S\cup\mathbb{P}_\infty} r_\nu & \text{otherwise.} \end{cases}$$

The set F is measurable. For each $\nu \in S \cup \mathbb{P}_\infty$, let μ_ν denote a Haar measure on k_ν normalised to have $\mu_\nu(r_\nu) = 1$ for all but finitely many ν. Then the product measure $\mu = \prod_{\nu\in S\cup\mathbb{P}_\infty} \mu_\nu$ is well defined and is a Haar measure on $k_{\mathbb{A}}(S)$. Set $A = \alpha^n - I, X = k_{\mathbb{A}}(S)$ and $\Gamma = \Delta(R_S)$, then ergodicity implies that $\ker A$ is discrete in $\hat{R}_S$ and by Lemma 2.18 we have

$$|\operatorname{Per}_n(\alpha)| = |\ker(\alpha^n - 1)| = \mu\left((\tilde{\alpha}^n - 1)F\right) = \prod_{\nu\in S\cup\mathbb{P}_\infty} |\xi^n - 1|_\nu.$$

□

2.7. **Growth rates.** Any expansive map α must have

$$\limsup_{n\to\infty} \frac{1}{n} \log \operatorname{Per}_n(\alpha) \le h(\alpha) \tag{2.5}$$

but many natural systems have a much stronger property.

Theorem 2.20. *If $\alpha : X \to X$ is an expansive automorphism of a compact connected group, then*

$$\lim_{n\to\infty} \frac{1}{n} \log \operatorname{Per}_n(\alpha) = h(\alpha).$$

In fact the same is true of ergodic automorphisms under a finiteness condition, but this is much more subtle (see below).

It is clear from Lemma 2.19 and Theorem 2.12 that for S–integer dynamical systems we always have

$$\liminf_{n\to\infty} \frac{1}{n} \log \operatorname{Per}_n(\alpha) \le \limsup_{n\to\infty} \frac{1}{n} \log \operatorname{Per}_n(\alpha) \le h(\alpha) < \infty.$$

A useful measure of the regularity of periodic points is the dynamical zeta function of α,

$$\zeta_\alpha(z) = \exp \sum_{n=1}^{\infty} \operatorname{Per}_n(\alpha) \frac{z^n}{n}, \tag{2.6}$$

a (formal) power series defined whenever $\operatorname{Per}_n(\alpha)$ is finite for all $n \ge 1$. By Hadamard, if (2.5) holds then (2.6) actually defines a holomorphic function in the disk of radius $e^{-h(\alpha)}$ about the origin.

Several Diophantine issues come up in trying to extend Theorem 2.20. In order to see what is involved in finding the growth rate of periodic points for S-integer systems, consider the following examples.

Example 2.21. Let $\xi = \sqrt{2} - 1 + i\sqrt{2\sqrt{2} - 2}$, $k = \mathbb{Q}(\xi)$, $S = \emptyset$. Then $R_S = \mathbb{Z} + \xi\mathbb{Z} + \xi^2\mathbb{Z} + \xi^3\mathbb{Z} \cong \mathbb{Z}^4$, so $X^{(k,S)}$ is the 4-torus $\mathbb{T}^4$, and the action of $\alpha^{(k,\xi,S)}$ is isomorphic to the action of the matrix

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -4 & 2 & -4 \end{bmatrix}$$

with eigenvalues $\lambda_1 = \sqrt{2} - 1 + i\sqrt{2\sqrt{2} - 2} \approx .414 + .910i$, $\lambda_2 = \sqrt{2} - 1 - i\sqrt{2\sqrt{2} - 2} \approx .414 - .910i$, $\lambda_3 \approx -.217$ and $\lambda_4 \approx -4.612$. The formula for the periodic points gives

$$\mathrm{Per}_n(A) = \det(A^n - I) = \prod_{j=1}^{4} |\lambda_j^h - 1|.$$

The last two terms are fine: it is clear that

$$\lim_{n\to\infty} \frac{1}{n} \log\left(|\lambda_3^h - 1| \times |\lambda_4^h - 1|\right) = \log|\lambda_4| = h(\alpha).$$

The problem is with the first two terms: $|\lambda_1| = |\lambda_2| = 1$, but neither are unit roots. This means that, for example $|\lambda_1^n - 1|$ gets arbitrarily small for certain values of n (the argument of λ_1 is not a rational multiple of π, so multiplication by λ_1 behaves like an irrational circle rotation with dense orbits). This problem is discussed in [45], where it is shown to be equivalent to a problem solved by Gel′fond in [28]. Since it is better-known, we will use Baker's stronger result.

Lemma 2.22. [BAKER'S THEOREM] *If λ is an algebraic number that is not a root of unity, then there exist constants A and B for which*

$$|\lambda^n - 1| > \frac{A}{n^B}. \tag{2.7}$$

It follows at once that the other two terms do not contribute anything to the logarithmic growth rate:

$$\lim_{n\to\infty} \frac{1}{n} \log\left(|\lambda_1^h - 1| \times |\lambda_2^h - 1|\right) = 0.$$

We conclude that

$$\lim_{n\to\infty} \frac{1}{n} \log \mathrm{Per}_n(\alpha) = h(\alpha)$$

for this non-expansive toral automorphism.

Example 2.23. If $k = \mathbb{Q}$, $S = \{2, 3\}$ and $\xi = 2$, then

$$\mathrm{Per}_n = (2^n - 1) \times |2^n - 1|_3,$$

so the growth rate of periodic points presents a similar problem. The first term is fine: $(1/n)\log|2^n-1| \to \log 2$, but the second term is less clear. There certainly is a sequence (n_j) for which $|2^{n_j}-1|_3 \to 0$, the question is how fast must such a sequence grow?

Lemma 2.24. *Let k be a an $\mathbb{A}$-field of characteristic zero, fix ξ not a unit, and let T be any finite subset of the finite places of k. Then there are constants $A, B > 0$ for which*

$$1 \geq \prod_{v \in T} |\xi^n - 1|_v \geq \frac{A}{n^B}.$$

This is not a deep result at all, and implies for example that

$$\lim_{n\to\infty} \frac{1}{n} \log|2^n-1|_3 = 0,$$

which shows that for this system also

$$\lim_{n\to\infty} \frac{1}{n} \log \mathrm{Per}_n(\alpha) = h(\alpha).$$

Similar reasoning gives the following theorem.

Theorem 2.25. *Let $(X,\alpha) = (X^{(k,S)}, \alpha^{(k,S,\xi)})$ be an ergodic arithmetic S–integer dynamical system with S finite. Then the growth rate of the number of periodic points exists and is given by*

$$\lim_{n\to\infty} \frac{1}{n} \log \mathrm{Per}_n(\alpha) = h(\alpha). \tag{2.8}$$

On the other hand, for most S-integer systems the dynamical zeta function is not rational (or even algebraic).

Example 2.26. The geometric case is very different: it is clear that property (2.8) does not hold for non-hyperbolic linear cellular automata for example. Example 2.9 with $k = \mathbb{F}_2(t)$, $S = \{t\}$ and $\xi = 1+t$ already shows some of the difficulties. The entropy is $\log 2$, and Lemma 2.19 says that

$$\begin{aligned} |F_n(\alpha)| &= |(t+1)^n - 1|_\infty \, |(t+1)^n - 1|_t \\ &= p^n \left| t^n + \binom{n}{1} t^{n-1} + \ldots + \binom{n}{n-1} t \right|_t . \end{aligned}$$

We claim that the set of limit points of $\left\{\frac{1}{n}\log|F_n(\alpha)|\right\}_{n=1}^{\infty}$ is

$$\left\{ \left(1 - \frac{1}{q}\right) h(\alpha) : q \in \mathbb{N}, p \not| q \right\} \cup \{h(\alpha)\}.$$

This is seen as follows: write $n = qp^{\mathrm{ord}_p(n)}$ where $p \not| q$ then

$$\begin{aligned} |F_n(\alpha)| &= |(t+1)^n - 1|_\infty |(t+1)^q - 1|_t \\ &= p^n p^{-p^{\mathrm{ord}_p(n)}} \text{ since } p \not| q \\ &= p^{n\left(1-\frac{1}{q}\right)}. \end{aligned}$$

So for a sequence $n_j \to \infty$ with $n_j / p^{\mathrm{ord}_p(n_j)} = q$ for a fixed $q, p \not| q$,

$$\lim_{\mathrm{ord}_p(n_j)\to\infty} \frac{1}{n_j} \log |F_{n_j}(\alpha)| = \left(1 - \frac{1}{q}\right) \log p.$$

Also, $p^+(\alpha) = h(\alpha)$ is obtained by letting $n \to \infty$ through the numbers which are coprime to p.

Similar reasoning gives the following general result.

Theorem 2.27. *Let $(X, \alpha) = (X^{(k,S)}, \alpha^{(k,S,\xi)})$ be an ergodic geometric S–integer dynamical system with S finite. Then*

$$\limsup_{n\to\infty} \frac{1}{n} \log \mathrm{Per}_n(\alpha) = h(\alpha),$$

and (usually) the set $\left\{\frac{1}{n} \log \mathrm{Per}_n(\alpha)\right\}$ has infinitely many other limit points.

Given that elements of S destroy periodic points, an interesting question is to ask if S can be *infinite* while still having many periodic points. It turns out that this is so in a very strong sense – see Section 2.8. Before that, I will describe an example due to Chothi [12]. Let $k = \mathbb{Q}$ and suppose ξ is a non–zero integer. Recall that ξ is said to be a *primitive root* modulo a prime p if and only if the residue classes modulo p of $\xi, \xi^2, \ldots, \xi^{p-1} \equiv 1$ are all distinct. The number of primitive roots modulo p is $\phi(p-1)$, where ϕ is the Euler function. For example, 2 is not a primitive root modulo 7 since $2^3 \equiv 1 (\mathrm{mod}\ 7)$. In 1927 Artin made the following conjecture: if a is neither a square nor -1, then there exist infinitely many primes such that a is a primitive root modulo p. So, if we choose $\xi \in \mathbb{Z}$ to be neither a square nor -1 and define S to be the set of places $|.|_p$ for which ξ is a primitive root modulo p, then Artin's conjecture implies that S is infinite. Let α be the endomorphism of $\hat{R}_S$ dual to multiplication by ξ on R_S.

Theorem 2.28. *If Artin's conjecture holds for ξ then $p^+(\alpha) = h(\alpha)$.*

Proof. Since $|\xi^n - 1|_p = 1$ if and only if $p - 1 \not| n$ for each $p \in S$, we have

$$\frac{1}{n} \log |F_n(\alpha)| = \frac{1}{n} \log |\xi^n - 1|_\infty + \frac{1}{n} \sum_{p \in S : p-1 | n} \log |\xi^n - 1|_p.$$

So by letting $n \to \infty$ through all the prime numbers, we get

$$\limsup_{n\to\infty} \frac{1}{n} \log |F_n(\alpha)| = \log |\xi| = h(\alpha).$$

□

Theorem 2.29. [HEATH–BROWN] *There are infinitely many primes p with either 2 or 3 or 5 as a primitive root.*

Proof. Heath–Brown [30] proves that, with the exception of at most two primes the following is true: for each prime q there are infinitely many primes p with q a primitive root modulo p. □

Corollary 2.30. *There exist non–expansive systems $(\hat{R}_S, \alpha)$ with S infinite such that*

$$\limsup_{n\to\infty} \frac{1}{n} \log \mathrm{Per}_n(\alpha) = h(\alpha) > 0.$$

These dynamical systems have the remarkable property that on the one hand they mimic hyperbolic behaviour ($\limsup_{n\to\infty} \frac{1}{n} \log \mathrm{Per}_n(\alpha) = h(\alpha)$), while on the other they have infinitely many directions in which they behave as isometries.

Theorem 2.29 will appear again in connection with *geometric* systems (cf. Theorem 2.35).

2.8. **Typical group automorphisms.** It is not clear whether it makes sense to speak of a 'typical' or 'generic' compact group automorphism. For one thing, it is not known what values the most obvious global invariant, the topological entropy, takes on. In order to explain this first difficulty, recall that the *Mahler measure* of a polynomial $f \in \mathbb{Z}[x]$ is defined to be

$$m(f) = \int_0^1 \log |f(e^{2\pi i s})| \mathrm{d}s.$$

An application of Jensen's formula shows that if ξ is an algebraic number with minimal polynomial f, and $S = \emptyset$, then the entropy of the associated S-integer system is $m(f)$. This appearance of Mahler measures as entropies also arises for higher-rank actions, which we will see again later.

Problem 2.31. [LEHMER'S PROBLEM] Is 0 a cluster point of

$$\{m(f) \mid f \in \mathbb{Z}[x]\}?$$

This problem arose in Lehmer's paper [40] of 1933 and seems to be very deep. For an extended discussion of what is know about it, see [7] and [26]. Mahler measures (for polynomials in several variable) have arisen in several areas of mathematics, including ergodic theory [49], number theory [50], probability [9], syntomic cohomology [16] and knot theory [67], [68].

The connection between Lehmer's problem and the problem of describing all compact group automorphisms is provided by a result due to Lind [45] (the same result holds in higher-rank also: see [49]).

Theorem 2.32. *The set of possible entropies of compact group automorphisms is all of* $[0,\infty]$ *if the answer to Lehmer's problem is 'yes', and is the countable set* $\{m(f) \mid f \in \mathbb{Z}[x]\}$ *if the answer is 'no'.*

Even after choosing a fixed entropy, it is not clear how to describe all the group automorphisms with that entropy. So we focus on a much simpler setting: for fixed k and ξ, can anything be said about the dynamics of $\alpha^{(k,S,\xi)}$ for a 'typical' set S? What (little) is known is described in the papers [75], [77] and [78]. Here we simply examine two examples that illustrate some of the difficulties. For the first example, we make the unwarranted assumption that there are infinitely many Mersenne primes.

Example 2.33. Let $k = \mathbb{Q}$, $\xi = 2$, and parametrize the possible sets S as follows: identify $S \subset \{3,5,7,11,\dots\}$ with a unique point in $\{0,1\}^{\mathbb{N}}$ in the obvious way, and place the iid $(1/2,1/2)$-measure on this set. Assume that $n_1 < n_2 < \dots$ is a sequence of primes for which $p_j = 2^{n_j} - 1$ is prime. Now for almost every S, there is a sequence $j_1 < j_2 < \dots$ of primes with $p_{j_k} \in S$ for all k. Now for any such S,

$$\mathrm{Per}_{j_k}(\alpha^{(\mathbb{Q},2,S)}) = |2^{j_k} - 1| \times |2^{j_k} - 1|_{p_{j_k}} = 1,$$

so

$$\liminf_{n\to\infty} \frac{1}{n} \log \mathrm{Per}(\alpha^{(\mathbb{Q},2,S)}) = 0$$

almost surely. On the other hand, for almost every S there is a sequence $\ell_1 < \ell_2 < \dots$ with $p_{\ell_k} \notin S$ for all k. Now for any such S,

$$\mathrm{Per}_{\ell_k}(\alpha^{(\mathbb{Q},2,S)}) = |2^{\ell_k} - 1|,$$

so

$$\limsup_{n\to\infty} \frac{1}{n} \log \mathrm{Per}(\alpha^{(\mathbb{Q},2,S)}) = \log 2$$

almost surely.

In fact the full Mersenne prime conjecture is not needed to reach the conclusions of Example 2.33: all that is needed is the weaker assumption that $\sum_{n=1}^{\infty} 2^{-\omega(2^n-1)} = \infty$, where $\omega(N)$ is the number of primes dividing N.

What can be said without making any assumptions?

Theorem 2.34. *Let $k = \mathbb{Q}$, $\xi = 2$. Then for almost every S*

$$\limsup_{n\to\infty} \frac{1}{n} \log \mathrm{Per}_n(\alpha) \geq \frac{1}{2} \log 2.$$

Proof. This is proved in three steps: the first is to show that the set of S for which the upper limit is positive must have positive measure. The second is to show that there is an ergodic transformation on the set of S's that preserves the upper limit, so that there must be a set of full measure on which it is constant (and positive by the first part). The third is to use an involution on the set of S's and the Artin-Whaples product formula to see that this upper limit must be at least half the entropy.

Step 1: Let

$$E = \left\{ S \mid \limsup_{n\to\infty} \frac{1}{n} \log \mathrm{Per}_n\left(\alpha^{(\mathbb{Q},S,2)}\right) > 0 \right\};$$

I claim that E has positive measure. Let $\bar{S} = S \cup \{\infty\}$, and assume that E has zero measure. Then for almost every S,

$$\lim_{n\to\infty} \frac{1}{n} \log \prod_{v\in\bar{S}} |2^n - 1|_v = 0. \tag{2.9}$$

On the other hand, we know that

$$\lim_{n\to\infty} \frac{1}{n} \log \prod_{v=2,\infty} |2^n - 1| = \log 2 > 0. \tag{2.10}$$

Now let $\bar{S}^* = \{v \mid v \notin S\} \cup \{2, \infty\}$. By the product formula,

$$\prod_{v\in\bar{S}} |\eta|_v \times \prod_{v\in\bar{S}*} |\eta|_v = |2^n - 1| \times |2^n - 1|_2 = |2^n - 1|. \tag{2.11}$$

The three equations (2.9), (2.10), (2.11) together imply that for almost every S,

$$\lim_{n\to\infty} \frac{1}{n} \log \prod_{v\in\bar{S}} |2^n - 1|_v = \log 2 > 0, \tag{2.12}$$

which contradicts (2.9). We deduce that E must have positive measure.

Step 2: Notice that the set E certainly does not contain the set $S = \{2, 3, 5, 7, \dots\}$ of all primes (corresponding to the point $(1, 1, 1, \dots) \in$

$\{0,1\}^{\mathbb{N}}$). So if we write the primes as $\{p_1, p_2, \dots\}$, any member of E looks like

$$S = \{p_{n(1)}, p_{n(2)}, p_{n(3)}, \dots\};$$

with $n(1) < n(2) < n(3) < \dots$ and $n(j) = j$ only finitely often: for $j = 1, \dots, r$ say. Then define a map V on the set of all S by

$$V(S) = \{\nu_{m(1)}, \nu_{m(2)}, \nu_{m(3)}, \dots\};$$

where $m(1) = n(r) + 1, m(\ell) = n(r + \ell - 1)$ for $\ell \geq 2$ if $n(1) = 1$, and $m(1) = 1, m(\ell) = n(\ell - 1)$ for $\ell \geq 2$ if $n(1) > 1$. If sets S are thought of as sequences of 0's and 1's, then V is the add-and-carry odometer, ergodic with respect to the $(1/2, 1/2)$ iid measure. By Step 1, for any $S \in E$ there is a sequence $n_j \to \infty$ for which

$$\frac{1}{n_j} \log \prod_{p \in S \cup \{\infty\}} |2^{n_j} - 1| \to h_0 > 0$$

say. Now the difference between S and $V(S)$ is only finitely many primes, and we have already seen in Lemma 2.24 that the product over finitely many terms has zero logarithmic growth rate. It follows that

$$\frac{1}{n_j} \log \prod_{p \in S^* \cup \{\infty\}} |2^{n_j} - 1| \to h_0 > 0$$

also. Thus the actual value of the upper limit must be positive and almost everywhere constant by the ergodic theorem.

Step 3: Finally, we want to show that the common value is not too small. To do this we use the involution from Step 1 again. Let h_0 denote the almost everywhere value of the upper limit. If $h_0 < \frac{1}{2} \log 2$, then by (2.11) we must have the upper limit $> \frac{1}{2} \log 2$ on the image of that set of S's under the map $S \to S^*$. This is clearly impossible, so the upper limit is at least $\frac{1}{2} \log 2$. □

Of course the upper limit is expected to be exactly $\log 2$ almost everywhere.

As is often the case, the geometric (positive characteristic) case turns out to be more tractable, and in some cases one can simply prove the basic expected result.

Theorem 2.35. *Let $k = \mathbb{F}_p(t)$, $\xi = t$. Then for almost every S and for some p,*

$$\limsup_{n \to \infty} \frac{1}{n} \log \mathrm{Per}_n(\alpha) = \log p.$$

What this means is that there is a probability space of isometric extensions of the full p-shift, and for almost every member of that space the extended system still has many periodic points. The positive characteristic analogue of the Mersenne prime conjecture appears here again, with the difference that it is (almost) solved. The proof therefore follows Example 2.33 rather than Theorem 2.34.

Proof. Using Lemma 2.19, we have that

$$\mathrm{Per}_n(\alpha) = |t^n - 1|_\infty \times \prod_{v \in S} |t^n - 1|_v = p^n \times \prod_{v \in S} |t^n - 1|_v.$$

Now assume that n is prime (we are only after an upper limit). A standard fact from finite fields – see [41, Th. 2.47] – gives the factorization of $t^n - 1$ over $\mathbb{F}_p$ (this is analogous to having a 'formula' for the prime factors of $2^n - 1$):

$$t^n - 1 = (t-1)(1 + t + t^2 + \cdots + t^{n-1}) = (t-1) \prod_{i=1}^{(n-1)/f} \zeta_i(t),$$

where each $\zeta_i(t)$ is irreducible and f is the least positive integer for which $p^f \equiv 1 \bmod n$. Using Theorem 2.29 we may choose the characteristic p in such a way that there are infinitely many prime values of n for which the corresponding f is $(n-1)$. That is: after eliminating (at most) two values of p, the polynomial $(1 + t + t^2 + \cdots + t^{n-1})$ is irreducible for infinitely many primes n. By Borel-Cantelli, we may assume that for almost every S infinitely many of those irreducibles are *not* in S; along that sequence we have

$$\mathrm{Per}_n(\alpha) = p^n \times e_n$$

(where e_n is 1 if the place corresponding to $(t-1)$ is not in S and is p if it is in S), so

$$\limsup_{n \to \infty} \frac{1}{n} \log \mathrm{Per}_n(\alpha) = \log p = h(\alpha).$$

Similarly, for almost every S there are infinitely many of those irreducible polynomials *in* S, giving a sequence along which

$$\mathrm{Per}_n(\alpha) = p^n \times e_n \times p^{-(n-1)},$$

so

$$\liminf_{n \to \infty} \frac{1}{n} \log \mathrm{Per}_n(\alpha) = 0.$$

□

In summary: asking for the dynamical behaviour of a typical compact group automorphism turns out to involve a network of questions in arithmetic of some subtlety.

3. Bernoullicity and recurrence

In the last section we saw some topological properties of compact group automorphisms. However the first way in which compact group automorphisms entered ergodic theory was as measurable systems: if $\alpha : X \to X$ is a compact group automorphism, then α preserves the Haar measure λ on X. Theorem 2.13 gives a characterization of ergodicity for group automorphisms. Rokhlin showed that ergodicity implied positive entropy for such systems in [58], and later showed that ergodicity implies completely positive entropy in [59] (this was extended to the non-abelian setting by Yuzvinskii in [82]). Katznelson [35] introduced an approach to these systems that used Fourier analysis and Diophantine approximation arguments to show that an ergodic automorphism of the k-torus is isomorphic to a Bernoulli shift. This argument was extended to automorphisms of the infinite-dimensional torus by Lind [42] and Aoki and Totoki [1] using algebraic reduction steps. The general result, that an ergodic automorphism of a compact group is isomorphic to a Bernoulli shift was eventually shown independently by Lind [43] and Miles and Thomas [51]. The shape of these proofs proceeds via several steps, and our purpose here is to isolate one of these steps, where the Diophantine problems arise, and describe a recent observation of Lind and Schmidt [48] that uses the product formula for number fields to obtain the desired estimate.

Recall that an invertible measure-preserving transformation T of a probability space $(X, \mathcal{B}, \mu)$ is isomorphic to a Bernoulli shift if there is a measurable partition $\mathfrak{P}$ of X with the following properties.

(1) $\mathfrak{P}$ is *independent*: for any $k \geq 1$, sets $A_0, A_1, \ldots, A_k \in \mathfrak{P}$ and distinct $n_1, n_2, \ldots, n_k \in \mathbb{Z}\backslash\{0\}$,

$$\mu\left(A_0 \cap T^{-n_1}(A_1) \cap \cdots \cap T^{-n_k}(A_k)\right) = \mu(A_0)\ldots\mu(A_k).$$

(2) $\mathfrak{P}$ *generates*: the smallest σ-algebra containing $\bigcup_{n\in\mathbb{Z}} T^{-n}(\mathfrak{P})$ is (modulo null sets) equal to $\mathcal{B}$.

The claim is therefore that if $\alpha : X \to X$ is an ergodic automorphism of a compact group, then a partition with those properties can be found.

(1) *Algebra:* using methods from group theory and commutative algebra, it is sufficient to prove this when X is a *solenoid* (a group whose dual group is a subgroup of $\mathbb{Q}^k$ for some k). These

reduction steps are implicit in several of the papers mentioned above; they are neatly summarized in Lind [46].

(2) *Measure theory:* using methods from Ornstein theory, it is enough to find a sequence of partitions $\mathfrak{P}_n$ that become independent and generate in the limit.

(3) *Fourier analysis:* using Fourier series to approximate the characteristic functions of the sets in the partitions, it is enough to show that trigonometric polynomials on X become independent under the action of α.

The last two steps require much technical attention: in particular, if the *rate* at which either of them happens is not fast enough, then they do not guarantee Bernoullicity.

3.1. **Automorphisms of solenoids.** Finally, one is reduced to the following question. Let ξ be an algebraic number that is not a root of unity. Is it possible that two expressions of the form

$$\sum_{j=-n^2}^{-n} c_j \xi^j \text{ and } \sum_{j=n}^{N} c_j \xi^j \tag{3.1}$$

can coincide with bounded coefficients $c_j \in \mathbb{Z}$ and large $N \geq n$?

How this question comes about is roughly as follows. The algebraic number ξ determines an automorphism of a solenoid as we have seen (the group is dual to $\mathbb{Q}(\xi)$, the automorphism is dual to multiplication by ξ). An expression of the form $\sum_A^B c_j \xi^j$, $|A|, |B| \leq f(N)$, $|c_j| \leq N$ is a trigonometric polynomial that may be used to approximate the characteristic function of an element of a partition. Multiplying by a high power of ξ corresponds to applying the automorphism many times (that is, moving apart in time). Finally, the only way for characters on a group to fail to be independent is if they coincide.

The following result and proof are taken directly from the note of Lind and Schmidt [48].

Theorem 3.1. *There exists an $n_0 \geq 0$ with the property that*

$$\beta = \sum_{j=-n^2}^{-n} c_j \xi^j = \sum_{j=n}^{N} c_j \xi^j \tag{3.2}$$

for some $N \geq n \geq n_0$ and $|c_j| \leq |j|^{20}$ implies that $\beta = 0$.

Proof. Let k be the number field $\mathbb{Q}(\xi)$, and let

$$S = \{v \in \mathbb{P}(k) \mid v \in \mathbb{P}_\infty(k) \text{ or } |\xi|_v \neq 1\}.$$

For any place $v \notin S$, $|\beta|_v \leq \max\{|c_j \xi^j|_v\} \leq 1$. The set S is finite; write the places in S as $v_1, v_2, \ldots, v_q$ with $|\xi|_{v_i} < \rho < 1$ for $i \leq p$ and $|\xi|_{v_i} \geq 1$ for $i \geq p+1$. Notice that there must be a place with $|\xi| < 1$ since ξ is not a root of unity.

Fix $i \leq p$. If v_i is finite, then the ultrametric inequality and the last term in (3.2) shows that

$$|\beta|_{v_i} \leq \max_{j=n,\ldots,N} \left\{|c_j|_{v_i} |\xi|_{v_i}^j\right\} \leq \rho^n,$$

while if v_i is infinite

$$|\beta|_{v_i} \leq \sum_{j=n}^{N} |c_j|_{v_i} |\xi|_{v_i}^j \leq \rho^n \sum_{j=n}^{\infty} j^{20} \rho^{j-n} = C\rho^n$$

for some constant C independent of n.

Now fix $i \geq p+1$ and use the second term in (3.2). If v_i is finite, then

$$|\beta|_{v_i} \leq \max_{j=-n^2,\ldots,-n} \left\{|c_j|_{v_i} |\xi|_{v_i}^j\right\} \leq 1,$$

while if v_i is infinite,

$$|\beta|_{v_i} \leq \sum_{j=-n^2}^{n} |j|^{20} \leq n^{42}.$$

Now assume that $\beta \neq 0$, and recall that $|\beta|_v \leq 1$ for all $v \notin S$. By the product formula,

$$\prod_{v \in S} |\beta|_v = \left(\prod_{v \notin S} |\beta|_v\right)^{-1} \geq 1.$$

Using the estimates above this gives

$$1 \leq \prod_{v \in S} |\beta|_v = \prod_{i=1}^{p} |\beta|_{v_i} \times \prod_{i=p+1}^{q} |\beta|_{v_i} \leq (C\rho^n)^p \left(n^{42}\right)^q \to 0$$

as $n \to \infty$. It follows that β must be zero if n is large enough. □

Here valuations have given a hyperbolic behaviour (witnessed by the number $\rho < 1$) even in a non-hyperbolic setting (for example, ξ could have been the number from Example 2.3(5), corresponding to a quasihyperbolic automorphism of the 4-torus).

3.2. **Exponential recurrence.** One of the outstanding problems in the metrical theory of compact group automorphisms is the question of whether an ergodic group automorphism is *finitarily* isomorphic to a Bernoulli shift. That is, can an isomorphism be found to a Bernoulli shift that is continuous off an invariant null set? A *necessary* condition for this property is exponential recurrence.

Definition 3.2. Let T be a homeomorphism of a compact metric space X, preserving a nonatomic Borel measure μ that is positive on open set. For U any Borel set of positive measure, let $r_U(x) = \min\{j > 0 \mid T^j(x) \in U\}$; by Poincaré recurrence r_U is finite almost everywhere. The map T is called *exponentially recurrent* if $\mu\{x \in U \mid r_U(x) = n\} \to 0$ exponentially for any open set U.

Lind proves in [46] that ergodic group automorphisms are exponentially recurrent. The proof uses reduction steps as above, which leave the case of an irreducible automorphism of the solenoid. If this automorphism has a complex eigenvalue with modulus not equal to 1, then the resulting hyperbolic growth gives the result. Just as in the last section, the case in which all the complex eigenvalues have modulus 1 requires new ideas, and these come from the finite valuations. Using this hidden hyperbolicity in a finite valuation, Lind shows the exponential recurrence.

The next example shows how this can come about.

Example 3.3. Let $\xi = \frac{3}{5} + \frac{4}{5}i$, and consider the S-integer system with $k = \mathbb{Q}(\xi)$ and $S = \emptyset$. There are two complex places, ∞_1 and ∞_2, with

$$|\xi|_{\infty_1} = |\xi| = 1$$

and

$$|\xi|_{\infty_2} = |\bar{\xi}| = 1.$$

This means there will be no hyperbolicity in the complex component of the covering space. However, the two places of k that lie above $\mathbb{Q}_5$ give ξ norm 5 and $1/5$, showing that there is hyperbolicity there.

3.3. **Commuting automorphisms.** The structure of $\mathbb{Z}^d$-actions by automorphisms of compact abelian groups will be described in more detail later. We will see later that there are ergodic $\mathbb{Z}^2$-actions that have zero entropy and therefore cannot be Bernoulli. The natural conjecture is that when there are no entropy constraints, ergodicity does still imply Bernoullicity. A major result – the higher-rank analogue of the Bernoullicity result – is the following.

Theorem 3.4. [RUDOLPH AND SCHMIDT] *If α is a completely positive entropy $\mathbb{Z}^d$-action by automorphisms of a compact abelian group, then α is measurably isomorphic to a d-dimensional Bernoulli shift.*

This is proved in [60]; a feature of the proof is that the same idea appears again. A form of asymptotic independence is needed, and this comes from the estimate [60, Lem. 3.6] in which the product formula for global fields is used.

4. Mixing

In Section 3 we saw that for a compact group automorphism a whole hierarchy of mixing properties,

$$\text{Bernoulli} \Rightarrow \text{c.p.e.} \Rightarrow \text{mixing of all orders} \Rightarrow$$

$$\text{mixing} \Rightarrow \text{mild mixing} \Rightarrow \text{weak mixing} \Rightarrow \text{ergodic}$$

collapses into one. It is well-known that for measure-preserving transformations each of the implications shown above *except for mixing of all orders $\Rightarrow$ mixing* is known to be strict. In this section the analogue of this remark for $\mathbb{Z}^d$-actions will be described. Here the picture is much more complicated, and a whole hierarchy of mixing properties between mixing of all orders and mixing emerges. Most of the material in this section is taken from [19], [65], [66] and [76]. The structure of non-mixing shapes and related problems to do with finding measurable invariants is not dealt with here in any detail but may be found in the papers [37] and [63].

Let T be an action of some countable group Γ by measure-preserving transformations of a probability space $(X, \mathcal{B}, \mu)$. In the group Γ, write $g \to \infty$ for the statement: for any finite set $F \subset \Gamma$, g is eventually not in F. For example, if $\Gamma = \mathbb{Z}$, then $g \to \infty$ means $|g| \to \infty$ in the usual sense. The mixing notions introduced below will be phrased for a general group Γ, but all the examples later will be for abelian groups.

Definition 4.1. Let T be a measure-preserving Γ-action.

(1) T is *ergodic* if any $A \in \mathcal{B}$ that is invariant under T (that is, $A = T_{-g}(A)$ up to null sets for all $g \in \Gamma$) must have $\mu(A) = 0$ or 1.

(2) T is *rigid* if there is a sequence $g \to \infty$ with the property that

$$\mu\left(T_{-g}(A) \Delta A\right) \to 0 \text{ for all } A \in \mathcal{B}.$$

(3) T is *mixing* if for any $A, B \in \mathcal{B}$

$$\lim_{g \to \infty} \mu(A \cap T_{-g}(B)) \to \mu(A)\mu(B).$$

(4) T is *k-fold mixing*, or *mixing on k sets*, if for any $A_1, \dots, A_k \in \mathcal{B}$,

$$\lim_{g_i g_j^{-1} \to \infty; i \neq j} \mu\left(T_{-g_1}(A_1) \cap \cdots \cap T_{-g_k}(A_k)\right) \to \prod_{i=1}^{k} \mu(A_i).$$

(5) T is *mixing of all orders* if it is mixing on k sets for all k.
(6) A finite set $F \subset \Gamma$ is a *mixing shape* for T if for any sets $A_f, f \in F$ in $\mathcal{B}$

$$\lim_{n \to \infty} \mu\left(\bigcap_{f \in F} T_{-f^n}(A_f)\right) \to \bigcap_{f \in F} \mu(A_f).$$

One of the central problems in ergodic theory is whether for $\mathbb{Z}$-actions mixing implies mixing of all orders. A very interesting recent result in [61] shows that amenable group actions with completely positive entropy are mixing of all orders.

The first examples show that ergodicity does not imply mixing, and that mixing does not imply mixing of all orders, for $\mathbb{Z}^d$-actions with $d \geq 2$.

Example 4.2. Let $S : X \to X$ be an ergodic measure-preserving transformation. Define a $\mathbb{Z}^2$-action T on X by $T_{(a,b)} = S^a$. Then T is certainly ergodic because $T_{(1,0)}$ is, but is not mixing because, for example, $T_{(0,1)}$ is the identity.

A more subtle phenomena, the full ramifications of which are not entirely understood, comes from Ledrappier's example [39].

Example 4.3. [LEDRAPPIER] Let

$$X = \{x \in \{0,1\}^{\mathbb{Z}^2} \mid x_{(n,m)} + x_{(n+1,m)} + x_{(n,m+1)} = 0 \bmod 2 \ \forall\ n, m\},$$

and define a $\mathbb{Z}^2$-action α on X by the shift: $(\alpha_{(a,b)}(x))_{(n,m)} = x_{(a+n,b+m)}$. We shall see later that α is mixing. However, it is not mixing on 3 sets: notice that if $x \in X$ then for any n,

$$x_{(0,0)} + x_{(2^n,0)} + x_{(0,2^n)} = 0 \bmod 2 \tag{4.1}$$

(this is simply a consequence of the shape of Pascal's triangle mod 2). The relation (4.1) makes it impossible for α to be mixing on 3 sets. If $A = \{x \in X \mid x_{(0,0)} = 1\}$, then $\mu(A) = \frac{1}{2}$ (since X is the disjoint union of A and $A + y$, where y is any point in X with $y_{(0,0)} = 1$). On the other hand, (4.1) shows that

$$A \cap \alpha_{(0,-2^n)}(A) \cap \alpha_{(-2^n,0)} = \emptyset,$$

so α is not mixing on 3 sets.

The abelian alphabet $\{0,1\}$ makes the mixing break down; some examples with a non-abelian alphabet that are more mixing are discussed in [74].

An important difference between the general case and the algebraic case is shown up by the following, taken from [76].

Theorem 4.4. *An algebraic $\mathbb{Z}^d$-action by automorphisms of a compact abelian group is mixing of all orders if and only if it has no non-mixing shapes. In contrast, there are measure-preserving $\mathbb{Z}^d$-actions for $d \geq 2$ that are rigid and have all shapes mixing.*

The first part of this theorem is surprisingly deep. The second part is a Gaussian measure-space construction due to Ferenczi and Kaminski [27].

4.1. **Background from algebra.** In order to try and understand the mixing properties of an algebraic $\mathbb{Z}^d$-action, some background ideas are needed. These can all be found for example in the book [65] and were first used systematically in this context in the paper [36] . The basic idea is to use Fourier analysis to translate a mixing property into a statement in commutative algebra, and then use algebra to study that statement. This has been implicit in much of what has already been discussed, and will be used again in Section 5.

Let α be a $\mathbb{Z}^d$-action by automorphisms of the compact metrizable abelian group X. Dual to α is a natural $\mathbb{Z}^d$-action on the countable dual $M = \widehat{X}$. If the action of $\widehat{\alpha_{\mathbf{e}_i}}$ is identified with multiplication by a variable u_i, then the additive group M acquires the structure of a module over the ring $\mathfrak{R}_d = \mathbb{Z}[u_1^{\pm 1}, \ldots, u_d^{\pm 1}]$. The same construction works in reverse: if M is any countable $\mathfrak{R}_d$-module, then it defines a corresponding $\mathbb{Z}^d$-action α^M on the group $\widehat{M}$. It will be convenient to write $\mathbf{u}^{\mathbf{n}}$ for the monomial $u_1^{n_1} \ldots u_d^{n_d}$.

Example 4.5. If $M = \mathfrak{R}_2/\langle 2, 1 + u_1 + u_2 \rangle$ then the corresponding system is Ledrappier's example (cf. Example 4.3).

As we have seen in several situations, the algebraic structure allows for mixing problems to be reduced to a simple case. To describe this, we examine Definition 4.1 in more detail for a $\mathbb{Z}^d$-action α on a non-trivial compact group

$$(X, \mathcal{B} = \text{Borel sets}, \mu = \text{Haar measure}).$$

A sequence $(\mathbf{n}_1^{(j)}, \mathbf{n}_2^{(j)}, \ldots, \mathbf{n}_r^{(j)})$ of r-tuples of elements of $\mathbb{Z}^d$ is *mixing for* α if for any sets $A_1, \ldots, A_r \in \mathcal{B}$,

$$\lim_{j \to \infty} \mu \left(\alpha_{-\mathbf{n}_1^{(j)}}(A_1) \cap \cdots \cap \alpha_{-\mathbf{n}_r^{(j)}}(A_r) \right) \to \mu(A_1) \cdots \mu(A_r). \tag{4.2}$$

This certainly requires that

$$\mathbf{n}_s^{(j)} - \mathbf{n}_t^{(j)} \to \infty \text{ as } j \to \infty \text{ for every } s \neq t. \tag{4.3}$$

If this condition is also sufficient (that is, if (4.3) implies (4.2)) then α is *mixing of order* r. A finite set $\{\mathbf{n}_1, \ldots, \mathbf{n}_r\}$ of integer vectors is a *mixing shape* for α if

$$\lim_{k\to\infty} \mu\left(\alpha_{-k\mathbf{n}_1}(A_1) \cap \cdots \cap \alpha_{-k\mathbf{n}_r}(A_r)\right) \to \mu(A_1)\cdots\mu(A_r). \tag{4.4}$$

As in Section 3, the question of whether a given sequence is mixing for a given system can be translated into another form and then simplified.

(1) *Approximation:* The mixing property (4.2) holds if and only if the *a priori* stronger property that for any $L^\infty(\mu)$ functions $f_1, \ldots, f_r$,

$$\int_X f_1(\alpha_{\mathbf{n}_1^{(j)}}(x)) \ldots f_r(\alpha_{\mathbf{n}_r^{(j)}}(x)) \mathrm{d}\mu(x) \longrightarrow \prod_{i=1}^r \int_X f_i \mathrm{d}\mu \text{ as } j \to \infty \tag{4.5}$$

holds. In one direction this equivalence is trivial, for the other direction approximate the functions by linear combinations of indicator functions of measurable sets.

(2) *Fourier analysis:* Property (4.5) holds if and only if for any elements $m_1, \ldots, m_r$, not all zero, of $M = \widehat{X}$, the equation

$$\mathbf{u}^{\mathbf{n}_1^{(j)}} m_1 + \cdots + \mathbf{u}^{\mathbf{n}_1^{(j)}} m_r = 0 \tag{4.6}$$

has only finitely many solutions in j. This may be seen by approximating the functions with trigonometric polynomials.

(3) *Algebra:* Call a prime ideal $\mathfrak{p} \subset \mathfrak{R}_d$ an *associated prime* of the module M if there is an element $m \in M$ for which $\mathfrak{p} = \{f \in \mathfrak{R}_d \mid f \cdot m = 0 \in M\}$. Then an algebraic argument in the module M (see [37] for the details) shows that equation (4.6) has only finitely many solutions in j if and only if for every prime ideal $\mathfrak{p}$ associated to M, and any elements $a_1, \ldots, a_r$, not all zero, of $\mathfrak{R}_d/\mathfrak{p}$, the equation

$$\mathbf{u}^{\mathbf{n}_1^{(j)}} a_1 + \cdots + \mathbf{u}^{\mathbf{n}_1^{(j)}} a_r = 0 \tag{4.7}$$

has only finitely many solutions in j.

Thus the mixing problem for $\mathbb{Z}^d$-actions by automorphisms of compact abelian groups is reduced to the following problem: describe the solutions of equations like (4.7) in rings like $\mathfrak{R}_d/\mathfrak{p}$.

4.2. **Order of mixing – connected case.** First let us assume that X is a connected group. This is equivalent to assuming that for any prime ideal $\mathfrak{p}$ associated to the corresponding module, $\mathfrak{p} \cap \mathbb{Z} = \{0\}$. By the remarks in the last section, it is enough to consider cyclic modules.

Example 4.6. Let $M = \mathfrak{R}_2/\langle u_1 - 2, u_2 - 3\rangle$; the corresponding dynamical system α is the invertible extension of the semi-group action generated by $x \mapsto 2x$ and $x \mapsto 3x$ mod 1 on the additive circle. Assume that α is *not* mixing on r sets for some r. Notice that there is an isomorphism $\mathfrak{R}_2/\langle u_1 - 2, u_2 - 3\rangle \to \mathbb{Z}[\frac{1}{6}]$ of additive groups, and under this isomorphism multiplication by u_1 (resp. u_2) is sent to multiplication by 2 (resp. 3). So the non-mixing sequence on r sets is witnessed as follows: there are rationals $a_1, \ldots, a_r \in \mathbb{Z}[\frac{1}{6}]$, not all zero, and a sequence $(\mathbf{n}_1^{(j)}, \mathbf{n}_2^{(j)}, \ldots, \mathbf{n}_r^{(j)})$ with

$$\mathbf{n}_s^{(j)} - \mathbf{n}_t^{(j)} \to \infty \text{ as } j \to \infty \text{ for every } s \neq t$$

such that

$$2^{n_{1,1}^{(j)}} 3^{n_{1,2}^{(j)}} a_1 + \cdots + 2^{n_{r,1}^{(j)}} 3^{n_{r,2}^{(j)}} a_r = 0 \text{ for all } j \geq 1. \tag{4.8}$$

This equation is a simple example of an *S-unit equation*; a deep result by Schlickewei (see [62] for example) says that (4.8) has only *finitely many* solutions in different values of the vector $(\mathbf{n}_1^{(j)}, \mathbf{n}_2^{(j)}, \ldots, \mathbf{n}_r^{(j)})$ (and hence of the index j) unless some subsum of the left-hand side vanishes infinitely often. By the characterization of mixing given above, this forces the action α to be non-mixing for some order $\ell < r$. On the other hand, α is clearly mixing on 2 sets, so we deduce that α is mixing of all orders.

Thus the $\times 2, \times 3$ system is a mixing of all orders, zero entropy, Markov shift. Using entirely different methods Mozes constructed another example of this phenomena (see [54]).

Roughly the same method may be used in general. There is a substantial obstacle to be overcome when the underlying group is not finite-dimensional, in which case the corresponding field has positive transcendance degree, and for this case one needs not just the *qualitative* theorem that S-unit equations have only finitely many solutions, but the *quantitative* S-unit theorem that gives a uniform bound for the number of solutions in terms of r and the field. Using this gives the following theorem from [66].

Theorem 4.7. [SCHMIDT AND WARD] *A mixing $\mathbb{Z}^d$-action by automorphisms of a compact connected abelian group is mixing of all orders.*

4.3. **Order of mixing – disconnected case.** Now assume that X is a totally disconnected group carrying a $\mathbb{Z}^d$-action α. This is equivalent to assuming that for each prime ideal $\mathfrak{p}$ associated to the module corresponding to α, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime p. Thus we may assume that equation (4.7) takes place in a ring of the form $\mathfrak{R}_d^{(p)}/\mathfrak{p}$, where $\mathfrak{R}_d^{(p)} = \mathbb{F}_p[u_1^{\pm 1}, \dots, u_d^{\pm 1}]$. The first observation is that something like Example 4.3 must happen unless the ideal $\mathfrak{p}$ is trivial.

Theorem 4.8. *If $\mathfrak{p} \neq \{0\}$, then the system corresponding to the module $\mathfrak{R}_d^{(p)}/\mathfrak{p}$ has non-mixing shapes.*

Proof. By assumption, there is a polynomial $f \in \mathfrak{p}$ that is not a monomial. Let $S = S(f)$ be the support of f; this is a finite subset of $\mathbb{Z}^d$ with at least two elements. Then exactly the same argument as that used in Example 4.3 shows that S is a non-mixing shape. □

A simple consequence of this is that a $\mathbb{Z}^d$ action by automorphisms of a zero-dimensional group is mixing of all orders if and only if it is isomorphic to a d-dimensional Bernoulli shift. Put another way, this means that the only way such an action can fail to be mixing of all orders is to have a factor that looks like the system corresponding to $\mathfrak{R}_d^{(p)}/\mathfrak{p}$ for some non-trivial prime ideal $\mathfrak{p}$.

Theorem 4.8 is the starting point for an intricate puzzle: given $\mathfrak{p}$, find all the non-mixing shapes for the system corresponding to the module $\mathfrak{R}_d^{(p)}/\mathfrak{p}$. The importance of this problem comes from the fact that non-mixing shapes are a new kind of measurable invariant specific to the higher-rank setting. For a complete discussion of this, see [65, Chap. VIII]. The problem of finding non-mixing *shapes* is in principle *algebraic*.

In this section I want to discuss a slightly different problem: finding the exact *order* of mixing, which is closer to a *Diophantine* problem. The basic conjecture states that there is no obstacle to mixing that does not come about from non-mixing shapes. We take the following from [19].

Conjecture 4.9. *An algebraic dynamical system for which all shapes of cardinality r are mixing is mixing of order r.*

That is, we conjecture that it is never possible to exhibit failure to mix of a certain order with some exotically shaped sequence unless there is a simple shape that witnesses failure to mix of that order. A degenerate case is when all shapes are mixing: then Theorems 4.7 and 4.8 show that Conjecture 4.9 holds. It also holds for Ledrappier's

example, because that is mixing on 2 sets but not on 3 sets, which is witnessed by a non-mixing shape.

The result that may be proved using the methods of [19] proves Conjecture 4.9 for some more cases.

Theorem 4.10. *If $\mathfrak{p} = \langle f \rangle$ is a principal $\mathfrak{R}_d^{(p)}$-module, and the support of f comprises the vertices of a tight polyhedra, then Conjecture 4.9 holds for $\alpha^{\mathfrak{R}_d^{(p)}/\mathfrak{p}}$.*

In the remainder of this section we will explain what this means and how it comes about by proving it for $d = 2$.

The type of polyhedra we are interested in are convex hulls of finite sets of points in $\mathbb{Z}^d$.

Definition 4.11. A *parallel redrawing* of a polyhedron P is another polyhedron P' with the property that each edge e of P is parallel to a single edge of P'. A polyhedron is *tight* if any parallel redrawing must be homothetic to the original polyhedron.

The terminology is taken from the slightly different setting of [14] and [81].

Example 4.12. To make sense of Definition 4.11, consider the following examples.

(1) For $d = 2$ there is only one tight shape, and that is the triangle.
(2) For $d = 3$ there are many tight polyhedra. Roughly speaking, a polyhedron with many triangular faces will be tight.

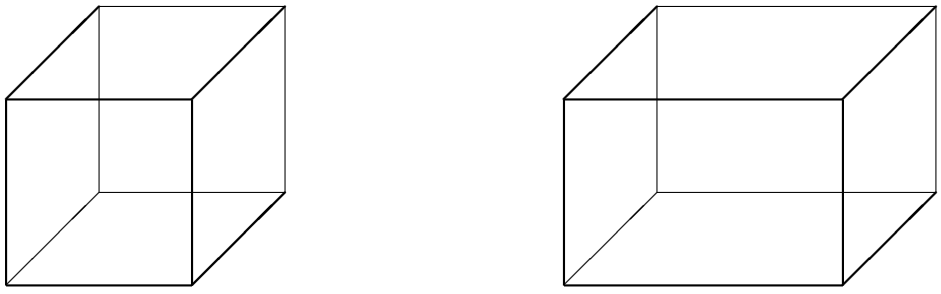

FIGURE 9. A parallel redrawing of the cube

(3) Of the platonic solids, the tetrahedron, octahedron and icosahedron are tight, while the cube and dodecahedron are loose.
(4) All the geodesates are tight. This gives many easy examples of very complex tight polyhedra.

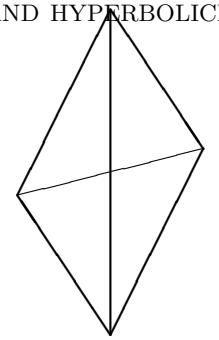

FIGURE 10. The tetrahedron is tight

Let $\mathcal{M}(\alpha^{\mathfrak{R}_d^{(p)}/\langle f\rangle})$ denote the order of mixing – the largest value of r for which (4.3) implies (4.2) – of $\alpha^{\mathfrak{R}_d^{(p)}/\langle f\rangle}$, where f is an irreducible polynomial in $\mathbb{F}_p[u_1^{\pm 1}, u_2^{\pm 2}]$. Finding $\mathcal{M}(\alpha^{\mathfrak{R}_d^{(p)}/\langle f\rangle})$ is difficult (see [65, Sect. 28]) even for this special class of systems. Let $S(f)$ denote the support of f, and $\mathcal{N}(f)$ the convex hull of $S(f)$.

Theorem 4.13. *Assume that $\mathcal{N}(f)$ is an R-gon and f is irreducible. Then*

$$R - 1 \leq \mathcal{M}(\alpha^{\mathfrak{R}_d^{(p)}/\langle f\rangle}) < |S(f)|.$$

Theorem 4.14. *Conjecture 4.9 holds when $r = 3$.*

The method of proof of Theorem 4.13 is to show that an arbitrary non-mixing sequence for $\alpha^{R_2/\mathfrak{p}}$ must asymptotically reflect part of the structure of $\mathcal{N}(f)$ (the slopes of the faces). Proving Conjecture 4.9 would involve showing that the exact structure of $\mathcal{N}(f)$ appears, and the reason Theorem 4.14 holds is that a triangle is the only tight polyhedron in 2 dimensions. Thus Theorem 4.14 is a special case of Theorem 4.10.

The key step in the proof is to construct valuations that reflect the geometry of $\mathcal{N}(f)$. To clarify this, an example is described in detail.

Example 4.15. Let $f(u_1, u_2) = u_2 + u_1 + u_1^3 u_2$, and view f as an element of $\mathbb{F}_p(u_2)[u_1]$. Choose a norm $|\cdot|$ on $\mathbb{F}_p(u_2)$ with $|u_2| = \frac{1}{p}$. This norm extends in two ways to the field $K = \mathbb{F}_p(u_2)[u_1]/\langle f\rangle$, determined by the Newton polygon of f viewed as a polynomial for u_1 with coefficients in $\mathbb{F}_p(u_2)$. The four points that define the Newton polygon are $(0, -\log_p |u_2|)$, $(1, -\log_p |1|)$, $(2, \infty)$ and $(3, -\log_p |u_2|)$. From Figure 12 it follows that the two extended norms $|\cdot|_1$, $|\cdot|_2$ have $|u_1|_1 = \frac{1}{p}$ (from the line segment with slope -1) and $|u_1|_2 = \sqrt{p}$ (from the line segment with slope $1/2$).

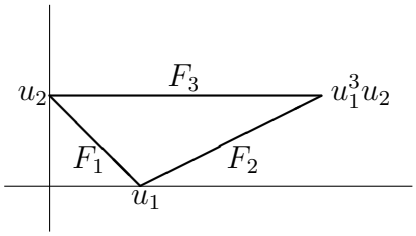

FIGURE 11. The faces of $\mathcal{N}(u_2 + u_1 + u_1^3u_2)$

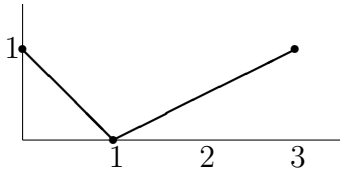

FIGURE 12. The Newton polygon of $f \in \mathbb{F}_p(u_2)[u_1]$

Thus the vector $\begin{pmatrix} \log_p |u_1|_1 \\ \log_p |u_2|_1 \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \end{pmatrix}$ is normal to the face F_1 and points out from $\mathcal{N}(f)$. The same expression using $|\cdot|_2$ gives an outward normal to the face F_2.

Finally, if the initial norm on $\mathbb{F}_p(u_2)$ is chosen with $|u_2| = p$, then the corresponding Newton polygon shows only one extension, and the resulting norm gives an outward normal to the face F_3.

Proposition 4.16. *Assume that* $\left(A^{(j)}\right) = (\mathbf{n}_1^{(j)}, \mathbf{n}_2^{(j)}, \ldots, \mathbf{n}_r^{(j)})$ *is a sequence with the property that*

$$m_1\mathbf{u}^{\mathbf{n}_1^{(j)}} + m_2\mathbf{u}^{\mathbf{n}_2^{(j)}} + \cdots + m_r\mathbf{u}^{\mathbf{n}_r^{(j)}} = 0 \tag{4.9}$$

for all j, *where* $m_1, \ldots, m_r \in R/\mathfrak{p}\backslash\{0\}$. *Write* $\mathcal{N}(A^{(j)})$ *for the convex hull of* $A^{(j)}$. *Then there is a constant* $K > 0$ *such that for each face* F *of* $\mathcal{N}(f)$ *there is a face of* $\mathcal{N}(A^{(j)})$ *spanned (without loss of generality) by* $\mathbf{n}_1^{(j)}, \mathbf{n}_2^{(j)}$, *and there is a vector* $\mathbf{m}^{(j)}$ *with the property that the line through* $\mathbf{n}_1^{(j)}, \mathbf{m}^{(j)}$ *is parallel to* F *and* $\|\mathbf{m}^{(j)} - \mathbf{n}_1^{(j)}\| \leq K$.

Proof. Pick a face F of $\mathcal{N}(f)$. Using the irreducibility of f, construct as in Example 4.15 a norm $|\cdot|$ on $R_2/\langle f\rangle$ so that $\begin{pmatrix} \log_p |u_1| \\ \log_p |u_2| \end{pmatrix}$ is an outward normal to $\mathcal{N}(f)$ through F.

Choose K so that $K \geq 2\max_{i=1,\dots,r}\{\big|\log_p|m_i|\big|\}$.

Find an F-exposed vertex $\mathbf{p}_j = \mathbf{n}_t^{(j)}$ in $A^{(j)}$, let ℓ be the line through $\mathbf{p}_j$ parallel to F, and assume that no other point in $A^{(j)}$ is within distance K of ℓ. Then for $\mathbf{n}_i^{(j)} \neq \mathbf{p}_j$, $\log_p|\mathbf{u}^{\mathbf{n}_i^{(j)}}m_i| < \log_p|\mathbf{u}^{\mathbf{p}_j}m_t|$, which contradicts (4.9). It follows that there is another vertex of $A^{(j)}$ within the strip as required. □

Proof. (of Theorem 4.13) First recall that $S(f)$ is automatically a non-mixing shape for $\alpha^{\mathfrak{R}_d^{(p)}/\langle f\rangle}$ by the method of proof of Theorem 4.8, so $\mathcal{M}(\alpha^{\mathfrak{R}_d^{(p)}/\langle f\rangle}) < |S(f)|$. On the other hand, each of the R faces of $\mathcal{N}(f)$ must asymptotically appear in $\mathcal{N}(A^{(j)})$ for a non-mixing sequence $(A^{(j)})$ by Proposition 4.16. It follows that $R-1 \leq \mathcal{M}(\alpha^{R_2/\mathfrak{p}})$. □

Proof. (of Theorem 4.14) If $\mathcal{N}(f)$ lies on a line, then $\alpha^{\mathfrak{R}_d^{(p)}/\langle f\rangle}$ cannot be mixing. If $\mathcal{N}(f)$ is an R-gon with $R > 3$ then Theorem 4.13 shows that $\mathcal{M}(\alpha^{\mathfrak{R}_d^{(p)}/\langle f\rangle}) \geq 3$. So assume that $\mathcal{N}(f)$ is a triangle, that $\alpha^{\mathfrak{R}_d^{(p)}/\langle f\rangle}$ is not mixing on 3 sets, and that all triangles are mixing shapes for $\alpha^{\mathfrak{R}_d^{(p)}/\langle f\rangle}$. This means that there are non-zero polynomials a, b, c with

$$a\mathbf{u}^{\mathbf{n}_1^{(j)}} + b\mathbf{u}^{\mathbf{n}_2^{(j)}} + c\mathbf{u}^{\mathbf{n}_r^{(j)}} = 0$$

for all j. By Proposition 4.16 each of $\mathbf{n}_1^{(j)}, \mathbf{n}_2^{(j)}, \mathbf{n}_3^{(j)}$ lie within a bounded distance of the vertices of some dilate of $\mathcal{N}(f)$. Multiplying a, b, c by monomials chosen to shift the vertices a bounded distance onto the vertices of an integer dilate of $S(f)$, produces an equation

$$a'\mathbf{u}^{\mathbf{m}_1^{(j)}} + b'\mathbf{u}^{\mathbf{m}_2^{(j)}} + c'\mathbf{u}^{\mathbf{m}_r^{(j)}} = 0$$

that witnesses a non-mixing shape of order 3. This contradicts the assumption. □

Example 4.17. Theorem 4.13 shows that if f is an irreducible polynomial for which the support $S(f)$ coincides with the extreme points of the Newton polygon $\mathcal{N}(f)$, then $\mathcal{M}(\alpha^{\mathfrak{R}_d^{(p)}/\langle f\rangle}) = |S(f)| - 1$. In order to produce an example with prescribed order of mixing $\mathcal{M}(\alpha^{\mathfrak{R}_d^{(p)}/\langle f\rangle}) = k$, it is therefore sufficient to exhibit such an irreducible polynomial with $|S(f)| = k+1$. This may be done using Eisenstein's irreducibility criterion (see [10] for a general valuation-theoretic treatment of the Eisenstein criterion). Two simple examples will illustrate the method; it is clear from these how to build an example for any order of mixing.

(1) To find an example with order of mixing 3, consider $f(u_1, u_2) = u_1^2 + u_1u_2^2 + u_2^3 + u_2 \in \mathbb{F}[u_2][u_1]$; the prime $u_2 \in \mathbb{F}[u_2]$ divides the

coefficients u_2^2 and $u_2^3+u_2$ but u_2^2 does not divide the coefficient $u_2^3+u_2$. The support of the polynomial is shown in Figure 13.

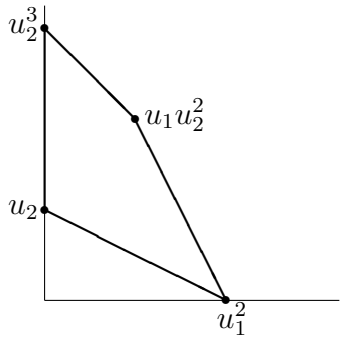

FIGURE 13. The support of a polynomial giving 3-fold mixing

(2) To find an example with order of mixing 4, let $f(u_1,u_2) = u_1^6+u_1^5u_2+u_1^3u_2^2+u_2+u_2^3$. As before, this is seen to be irreducible by viewing it as a polynomial in u_1 with coefficients in $\mathbb{F}[u_2]$. The support of the polynomial is shown in Figure 14.

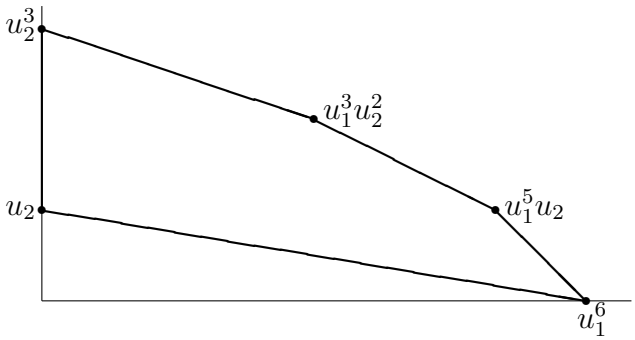

FIGURE 14. The support of a polynomial giving 4-fold mixing

Notice that in these examples we are choosing the shape of the support freely; it is also possible to find examples for which any prescribed shape is the minimal non-mixing shape by [76], though not in a constructive fashion.

Example 4.18. Theorem 4.14 shows that the system corresponding to the ideal $\mathfrak{p} = \langle 2, 1+u_1+u_2+u_2^2\rangle$ is 3-mixing, answering a question in [65, p. 283].

Example 4.19. In the previous example, we used the fact from [65] that no shape with cardinality 3 is non-mixing. An alternative method to show this is to use a result of Voloch on solutions to $ax+by=1$ in

functions fields. Consider again $\mathfrak{p} = \langle 2, 1+u_1+u_2+u_2^2\rangle$; then Theorem 4.13 says that

$$2 \le \mathcal{M}(\alpha^{R_2/\mathfrak{p}}) < 4,$$

and we wish to show that $\mathcal{M}(\alpha^{R_2/\mathfrak{p}}) = 3$. To see this, assume that

$$\left(\mathbf{n}_1^{(j)}, \mathbf{n}_2^{(j)}, \mathbf{n}_3^{(j)} = 0\right)$$

is a non-mixing sequence for $\alpha^{R_2/\mathfrak{p}}$ with $\mathbf{n}_s^{(j)} - \mathbf{n}_t^{(j)} \to \infty$ as $j \to \infty$ for $s \ne t$. Then there are elements m_1, m_2, m_3 of $\mathfrak{R}_2/\mathfrak{p}$, not all zero, with

$$m_1\mathbf{u}^{\mathbf{n}_1^{(j)}} + m_2\mathbf{u}^{\mathbf{n}_2^{(j)}} = -m_3 \tag{4.10}$$

for infinitely many j. The field of fractions of $\mathfrak{R}_2/\mathfrak{p}$ may be identified with $\mathbb{F}_2(t)$ by the map $u_1 \mapsto t$, $u_2 \mapsto 1+t+t^2$, and in this field (4.10) becomes

$$ax + by = 1 \tag{4.11}$$

with infinitely many solutions for x, y in the finitely generated multiplicative subgroup $G = \langle\langle t, 1+t+t^2\rangle\rangle$ of $\mathbb{F}_2(t)^*$. By [72], it follows that (4.11) is a *G-trivial* equation: there is an $n \ge 1$ for which $a^n, b^n \in G$. Since G is generated by irreducible polynomials, this can only be true if $a, b \in G$. So there is an infinite family of equations

$$\mathbf{u}^{\mathbf{m}_1^{(j)}} + \mathbf{u}^{\mathbf{m}_2^{(j)}} = 1 \tag{4.12}$$

with $\mathbf{m}_1^{(j)}$, $\mathbf{m}_2^{(j)}$, and $\mathbf{m}_1^{(j)} - \mathbf{m}_2^{(j)} \to \infty$ as $j \to \infty$. By considering the shape of $\mathcal{N}(1+u_1+u_1^2+u_2)$, this shows that the polynomial in (4.12) has the same shape as $\mathcal{N}(1+u_1+u_1^2+u_2)$, so (without loss of generality), $\mathbf{m}_1^{(j)} = (0, m(j))$ and $\mathbf{m}_2^{(j)} = (2m(j), 0)$ for some $m(j) \to \infty$. Thus the equation reduces to

$$(1+t+t^2)^{m(j)} = 1 + t^{2m(j)}. \tag{4.13}$$

Write $m(j) = 2^e\ell$, ℓ odd, for some $e \ge 0$. Then the left-hand side of (4.13) is

$$\begin{aligned}(1+t+t^2)^{2^e\ell} &= (1+t+O(t^2))^{2^e}\\ &= 1+t^{2^e}+O(t^2)^{2^e}\\ &= 1+t^{2^{e+1}\ell},\end{aligned}$$

which is impossible. It follows that $\mathcal{M}(\alpha^{R_2/\mathfrak{p}}) = 3$.

4.4. **Typical actions.** The analogue of Section 2.8 is even less accessible for commuting automorphisms. The entropy has been computed in terms of the prime ideals associated to the module – see [49, Th. 4.4] – and is built up from the cyclic case.

Theorem 4.20. *The topological entropy of the $\mathbb{Z}^d$-action $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ is 0 if $\mathfrak{p}$ is non-principal, and is given by*

$$h(\alpha^{\mathfrak{R}_d/\mathfrak{p}}) = m(f) = \int_0^1 \dots \int_0^1 \log|f(e^{2\pi i s_1}, \dots, e^{2\pi i s_d})| ds_1 \dots ds_d$$

if $\mathfrak{p} = \langle f \rangle$.

It turns out that Lehmer's Problem 2.31 is not changed by passing to more variables: 0 is a cluster point of $\{m(f) \mid f \in \mathbb{Z}[x]\}$ if and only if 0 is a cluster point of $\{m(f) \mid f \in \mathfrak{R}_d\}$ for some $d \geq 1$. This is a consequence of a non-trivial approximation result due to Lawton [38] (see [26] for a simple treatment). It follows that it is not known what the possible entropies of algebraic $\mathbb{Z}^d$-actions are.

Beyond that, the algebra of higher-rank S-integer systems is quite subtle, and there are real difficulties associated with formulating the analogue of S-integer dynamical systems in higher rank. For some results see [52] and [53].

5. Subdynamics

As we have seen, the problem of understanding the dynamics of algebraic $\mathbb{Z}^d$-actions can always be reduced to statements in commutative algebra, and for these valuations are a powerful tool. The last dynamical property we will discuss is the geometric notion of *subdynamics*: for a given $\mathbb{Z}^d$-action, what properties do lower-rank subactions have? The material here is taken from the papers [8], [20], and [21].

Let β be a $\mathbb{Z}^d$-action by homeomorphisms of a compact metric space (X, ρ). For a subset F of $\mathbb{R}^d$ define a new (pseudo-)metric by

$$\rho_\beta^F(x, y) = \sup\{\rho\big(\beta^{\mathbf{n}}(x), \beta^{\mathbf{n}}(y)\big) : \mathbf{n} \in F \cap \mathbb{Z}^d\},$$

and if $F \cap \mathbb{Z}^d = \emptyset$ define $\rho_\beta^F(x, y) = 0$.

Definition 5.1. The $\mathbb{Z}^d$-action β on (X, ρ) is said to be *expansive* if there is a $\delta > 0$ with the property that

$$\rho_\beta^{\mathbb{R}^d}(x, y) \leq \delta \Rightarrow x = y. \tag{5.1}$$

Any $\delta > 0$ satisfying (5.1) is called an *expansive constant* for β.

For $t > 0$, let

$$F^t = \{\mathbf{x} \in \mathbb{R}^d : \mathrm{dist}(\mathbf{x}, F) \leq t\},$$

where dist denotes the usual Euclidean distance. Thus F^t is the result of *thickening* F by t. This device of considering thickened subsets comes from [8] and is an implicit way of passing from the countable collection of rational subspaces of $\mathbb{Q}^d$ to the compact Grassmanian. An alternative way to compactify the space of directions is to replace the original $\mathbb{Z}^d$-action with a $\mathbb{R}^d$-flow on a suspension – see [32], [33].

Definition 5.2. A subset $F \subset \mathbb{R}^d$ is *expansive for* β if there are $\varepsilon > 0$ and $t > 0$ such that

$$\rho_\beta^{F^t}(x, y) \leq \varepsilon \Rightarrow x = y.$$

Every subset of a nonexpansive set for β is nonexpansive for β. Every translate of an expansive set is expansive by [8, p. 57]. In Definition 5.2 ε can be fixed for β [8, Lemma 2.3].

Let $\mathsf{G}_k = \mathsf{G}_{d,k}$ denote the Grassmann manifold of k-dimensional subspaces (or k-planes) of $\mathbb{R}^d$; G_k is a compact manifold of dimension $k(d-k)$ whose topology is given by declaring two subspaces to be close if their intersections with the unit sphere are close in the Hausdorff metric.

Definition 5.3. For a $\mathbb{Z}^d$-action β define

$$\mathsf{E}_k(\beta) = \{V \in \mathsf{G}_k : V \text{ is expansive for } \beta\},$$
$$\mathsf{N}_k(\beta) = \{V \in \mathsf{G}_k : V \text{ is nonexpansive for } \beta\}.$$

An *expansive component of k-planes for* β is a connected component of $\mathsf{E}_k(\beta)$.

Example 5.4. [LEDRAPPIER'S EXAMPLE] Take $d = 2$,

$$X = \{x \in (\mathbb{Z}/2\mathbb{Z})^{\mathbb{Z}^2} : x_{i,j} + x_{i+1,j} + x_{i,j+1} \equiv 0 \pmod 2 \text{ for all } i, j\},$$

and let β be the $\mathbb{Z}^2$-action generated by the horizontal and vertical shifts. If L is a line that is not parallel to one of the sides of the unit simplex in $\mathbb{R}^2$ and $t \geq 2$, then for each $x \in X$ the coordinates of x within L^t determine all of x, so that $L \in \mathsf{E}_1(\beta)$. On the other hand, the three lines parallel to the sides of the simplex do not have this property, and they comprise $\mathsf{N}_1(\beta)$ (see [8, Example 2.7] for details).

Coding arguments [8, Lemma 3.4] show that each $\mathsf{E}_k(\beta)$ is an open subset of G_k, so that each $\mathsf{N}_k(\beta)$ is compact. Hence expansive components of k-planes for β are open subsets of G_k. If W is nonexpansive for β and V is a subspace of W, then V is also nonexpansive for β.

A basic result [8, Theorem 3.6] is a sort of converse to this: If V is a nonexpansive subspace for β of dimension $\leq d-2$, then there is a nonexpansive subspace for β containing V of one higher dimension. If X is infinite, then the zero subspace is nonexpansive, and hence each $\mathsf{N}_k(\beta) \neq \emptyset$ for $1 \leq k \leq d-1$. Hence $\mathsf{N}_k(\beta)$ consists of exactly all k-dimensional subspaces of the subspaces in $\mathsf{N}_{d-1}(\beta)$. Thus $\mathsf{N}_{d-1}(\beta)$ determines the entire expansive subdynamics of β.

In order to treat algebraic $\mathbb{Z}^d$-actions, it is convenient to shift our viewpoint slightly and use half-spaces in $\mathbb{R}^d$ rather than $(d-1)$-planes. Let $\mathbb{S}^{d-1} = \{\mathbf{v} \in \mathbb{R}^d : \|\mathbf{v}\| = 1\}$ be the unit $(d-1)$-sphere. For $\mathbf{v} \in \mathbb{S}^{d-1}$ define $H_{\mathbf{v}} = \{\mathbf{x} \in \mathbb{R}^d : \mathbf{x} \cdot \mathbf{v} \leq 0\}$ to be the half-space with outward unit normal $\mathbf{v}$. Let H_d be the set of half-spaces in $\mathbb{R}^d$, which we identify with $\mathbb{S}^{d-1}$ via the parameterization $\mathbf{v} \leftrightarrow H_{\mathbf{v}}$. For $H \in \mathsf{H}_d$ we denote its outward unit normal vector by $\mathbf{v}_H$.

Expansiveness along a half-space H is defined using Definition 5.3 with $F = H$. Observe that thickening $H_{\mathbf{v}}$ by $t > 0$ results merely in the translation $H_{\mathbf{v}} + t\mathbf{v}$ of $H_{\mathbf{v}}$. Hence there is no need to thicken half-spaces in the definition, and a $\mathbb{Z}^d$-action β is therefore expansive along H if and only if there is an $\varepsilon > 0$ such that $\rho_\beta^H(x, y) \leq \varepsilon$ implies that $x = y$.

Definition 5.5. For a $\mathbb{Z}^d$-action β define

$$\mathsf{E}(\beta) = \{H \in \mathsf{H}_d : H \text{ is expansive for } \beta\},$$
$$\mathsf{N}(\beta) = \{H \in \mathsf{H}_d : H \text{ is nonexpansive for } \beta\}.$$

An *expansive component of half-spaces for* β is a connected component of $\mathsf{E}(\beta)$.

Remark 5.6. A coding argument analogous to [8, Lemma 3.4] shows that $\mathsf{E}(\beta)$ is an open set and so $\mathsf{N}(\beta)$ is a compact set.

The following lemma shows that a $(d-1)$-plane is nonexpansive for β if and only if at least one of the two bounding half-spaces is also nonexpansive for β. Thus if we define $\pi \colon \mathsf{H}_d \to \mathsf{G}_{d-1}$ by $\pi(H) = \partial H$, then $\pi(\mathsf{N}(\beta)) = \mathsf{N}_{d-1}(\beta)$. This shows that the half-space behavior $\mathsf{N}(\beta)$ determines the expansive subdynamics of β.

The following key definition is taken from [8, Definition 3.1].

Definition 5.7. Let β be an expansive $\mathbb{Z}^d$-action with expansive constant δ. For subsets E, F of $\mathbb{R}^d$ we say that E *codes* F provided that, for every $\mathbf{x} \in \mathbb{R}^d$, if $\rho_\beta^{E+\mathbf{x}}(x, y) \leq \delta$ then $\rho_\beta^{F+\mathbf{x}}(x, y) \leq \delta$.

Lemma 5.8. *Let β be a $\mathbb{Z}^d$-action and $V \in \mathsf{G}_{d-1}$. Then $V \in \mathsf{N}_{d-1}(\beta)$ if and only if there is an $H \in \mathsf{N}(\beta)$ with $\partial H = V$.*

Proof. If $H \in \mathsf{N}(\beta)$, then $V = \partial H \subset H$ is also nonexpansive.

Conversely, let $V \in \mathsf{G}_{d-1}$ and $H = H_{\mathbf{v}}$, $H' = H_{-\mathbf{v}}$ be the two half-spaces with boundary V. Suppose that both H and H' are expansive for β. We prove that V is also expansive for β, which will complete the proof.

Since β has an expansive half-space, it is an expansive action. Let $\delta > 0$ be an expansive constant for β. Let $B(r)$ denote the ball of radius r in $\mathbb{R}^d$, and $[\mathbf{0}, \mathbf{v}]$ be the line segment joining $\mathbf{0}$ to $\mathbf{v}$. A "finite" version of the expansiveness of H, entirely analogous to [8, Lemma 3.2], is that there is an $r > 0$ such that $H \cap B(r)$ codes $[\mathbf{0}, \mathbf{v}]$. Similarly, there is an $s > 0$ such that $H' \cap B(s)$ codes $[\mathbf{0}, -\mathbf{v}]$. Hence if $t = \max\{r, s\}$, then V^t codes V^{t+1}, which by the same argument codes V^{t+2}, and so on. Thus V^t codes $\mathbb{R}^d$, which means that V is expansive. □

As a starting point, Schmidt [64] gave the following characterization of expansiveness for α^M. For an ideal $\mathfrak{p} \subset \mathfrak{R}_d$, let

$$\mathsf{V}(\mathfrak{p}) = \big\{ \mathbf{z} = (z_1, \dots, z_d) \in (\mathbb{C}^\times)^d : f(z_1, \dots, z_d) = 0 \text{ for all } f \in \mathfrak{p} \big\}.$$

Let $\mathbb{S}^d = \{(z_1, \dots, z_d) \in \mathbb{C}^d : |z_1| = \cdots = |z_d| = 1\}$ be the multiplicative d-torus.

Theorem 5.9. *The $\mathbb{Z}^d$-action α^M is expansive if and only if both*

1. *M is a Noetherian $\mathfrak{R}_d$-module, and*
2. *for each prime ideal $\mathfrak{p} \subset \mathfrak{R}_d$ associated to M, $V(\mathfrak{p}) \cap \mathbb{S}^d = \emptyset$.*

The first condition – *algebraic* in nature – is necessary for the following reason. If M is not Noetherian, then there is an infinite ascending chain of submodules $\{0\} \subset M_1 \subset M_2 \subset \dots$ inside M; their annihilators form an infinite descending chain of closed α^M-invariant subgroups $\{0\}^\perp = X_M \supset M_1^\perp \supset M_2^\perp \supset \dots$ with $\bigcap_{j \geq 1} M_j^\perp = \{0\}$, showing that α^M is not expansive. The second condition – which is *geometric* – is necessary because from a point in $V(\mathfrak{p}) \cap \mathbb{S}^d$ a point may be constructed whose orbit under the action of α^M stays close to 0.

The main result in [20] is a directional version of this theorem. There are several steps involved in this, and the two different requirements for expansiveness each have their own analogues. For $H \in \mathsf{H}_d$, define the ring $\mathfrak{R}_H = \mathbb{Z}[u^{\mathbf{n}} : \mathbf{n} \in H \cap \mathbb{Z}^d]$, which is a subring of $\mathfrak{R}_d$. In general $\mathfrak{R}_H$ is *not* Noetherian; indeed, $\mathfrak{R}_H$ is Noetherian exactly when $\mathbf{v}_H$ is a rational direction in the sense that $\mathbb{R}\mathbf{v}_H \cap \mathbb{Z}^d \neq \{\mathbf{0}\}$, so that $\mathfrak{R}_H$ is Noetherian for only countably many H.

Theorem 5.10. *Let M be a Noetherian $\mathfrak{R}_d$-module, α^M be the corresponding algebraic $\mathbb{Z}^d$-action, and $H \in \mathsf{H}_d$. Then the following are equivalent.*

(1) α^M *is expansive along* H.
(2) $\alpha^{\mathfrak{R}_d/\mathfrak{p}}$ *is expansive along* H *for every prime ideal* $\mathfrak{p}$ *associated to* M.
(3) $\mathfrak{R}_d/\mathfrak{p}$ *is* $\mathfrak{R}_H$*-Noetherian and* $[0,\infty)\mathbf{v}_H \cap \log|\mathsf{V}(\mathfrak{p})| = \emptyset$ *for every* $\mathfrak{p} \in \operatorname{asc}(M)$.

In order to work with this result, it is important to give a more computable version of the $\mathfrak{R}_H$-Noetherian property. This is discussed in detail in [20] and [21]. From [20] we take the following theorem.

Theorem 5.11. *Let* M *be a Noetherian* $\mathfrak{R}_d$*-module,* $H \in \mathsf{H}_d$*, and* $\mathbf{k} \in \mathbb{Z}^d \setminus H$*. Then* M *is* R_H*-Noetherian if and only if there is a polynomial of the form* $u^{\mathbf{k}} - f(u)$ *with* $f(u) \in R_H$ *that annihilates* M*. It follows that there is an algorithm that describes the set of those* H *for which a given module* M *is* $\mathfrak{R}_H$*-Noetherian.*

The last part of this theorem relates to a slightly different kind of problem than those we have mentioned. That is, given a presentation of a module, how does one set about actually computing some of the dynamical properties of the associated system? In particular, for which properties are complex syzygy computations required? See [22] and [20, Sect. 6] for some discussion of this.

5.1. **Examples.** Using the correspondence $\mathsf{H}_d \leftrightarrow \mathbb{S}^{d-1}$ given by $H \leftrightarrow \mathbf{v}_H$, subsets of H_d may be identified with the corresponding subsets of $\mathbb{S}^{d-1}$. Using this convention, for an ideal $\mathfrak{a} \in \mathfrak{R}_d$ define

$$\mathsf{N}^{\mathsf{n}}(\alpha^{\mathfrak{R}_d/\mathfrak{a}}) = \{\mathbf{v} \in \mathbb{S}^{d-1} : \mathfrak{R}_d/\mathfrak{a} \text{ is not } R_{H_{\mathbf{v}}}\text{-Noetherian}\},$$
$$\mathsf{N}^{\mathsf{v}}(\alpha^{\mathfrak{R}_d/\mathfrak{a}}) = \{\mathbf{v} \in \mathbb{S}^{d-1} : [0,\infty)\mathbf{v} \cap \log|\mathsf{V}(\mathfrak{a})| \neq \emptyset\}.$$

Observe that $\mathsf{N}^{\mathsf{v}}(\alpha^{\mathfrak{R}_d/\mathfrak{a}})$ is the radial projection of $\log|\mathsf{V}(\mathfrak{a})|$ to $\mathbb{S}^{d-1}$. By Theorem 5.10,

$$\mathsf{N}(\alpha^{\mathfrak{R}_d/\mathfrak{a}}) = \mathsf{N}^{\mathsf{n}}(\alpha^{\mathfrak{R}_d/\mathfrak{a}}) \cup \mathsf{N}^{\mathsf{v}}(\alpha^{\mathfrak{R}_d/\mathfrak{a}}).$$

In the case of a principal ideal $\langle f\rangle$ in $\mathfrak{R}_d$ we abbreviate $\mathsf{V}(\langle f\rangle)$ to $\mathsf{V}(f)$.

Example 5.12. Consider Example 4.6 again. As we saw, this has a surprisingly mixing property, despite having zero entropy. Here $M = \mathfrak{R}_2/\langle u_1 - 2, u_2 - 3\rangle$; the corresponding dynamical system α is the invertible extension of the semi-group action generated by $x \mapsto 2x$ and $x \mapsto 3x \bmod 1$ on the additive circle. Write $\mathfrak{p} = \langle u_1 - 2, u_2 - 3\rangle$. To use Theorem 5.10, notice that $V(\mathfrak{p}) = \{(2,3)\}$, so the variety condition $[0,\infty)\mathbf{v}_H \cap \log|\mathsf{V}(\mathfrak{p})| = \emptyset$ will fail only in the direction $\mathbf{v}_H = (\log 2, \log 3)$. The module M is $\mathfrak{R}_H$-Noetherian except when

$\mathbf{v}_H = (0,-1)$ or $(-1,0)$. A sample of these arguments is the following: if $\mathbf{v}_H = (-1,0)$, then $\mathfrak{R}_H$ is the ring $\mathfrak{R}_H = \mathbb{Z}[u_1, u_2^{\pm 1}]$, and so

$$\mathfrak{R}_2/\mathfrak{p} \supset \cdots \supset \tfrac{1}{4}\mathfrak{R}_H/\mathfrak{p} \supset \tfrac{1}{2}\mathfrak{R}_H/\mathfrak{p} \supset \mathfrak{R}_H/\mathfrak{p} \supset$$

is an infinite ascending chain of $\mathfrak{R}_H$-submodules, showing this direction to be non-Noetherian. The non-expansive set is shown in Figure 15, using the convention above associating subsets of the Grassmanian to subsets of the $(d-1)$-sphere.

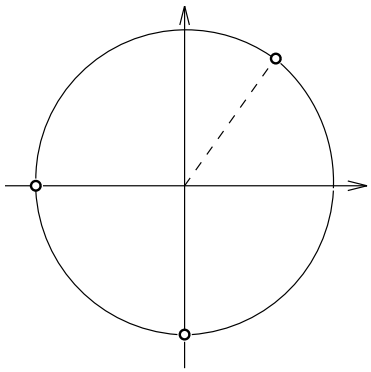

FIGURE 15. Non-expansive directions for $\times 2, \times 3$.

Ledrappier's example will have a similar picture, and these are representative of the possible type of phenomena in $\mathbb{Z}^2$-actions. For $\mathbb{Z}^3$-actions, there are many new possible phenomena.

Example 5.13. The following example is taken from Miles' thesis [52, Example 4.3.7], which constructs the systems in a different way. If X is the dual of the ring of integers in $\mathbb{Q}(\sqrt{2}+\sqrt{5})$, with a $\mathbb{Z}^3$-action α induced by the automorphisms dual to multiplication by $1+\sqrt{2}$, $2+\sqrt{5}$, and $3+\sqrt{2}\sqrt{5}$. Here there are four non-expansive planes in general position, leaving seven expansive cones shown in Figure 16.

Understanding the next example exhibits several new phenomena that arise in $\mathbb{Z}^d$-actions for $d \geq 3$. First, there may be no expansive lines at all. Second, a set of expansive directions may have curved sides. Finally, the set of non-expansive behaviour may have interior. It is not possible to draw the corresponding set of non-expansive planes, so the figure just shows the set of non-expansive vectors on the 2-sphere that are outward normals to non-expansive half-planes.

Example 5.14. Let $d = 3$ and $\mathfrak{p} = \langle 1 + u_1 + u_2, u_3 - 2\rangle$. This is a prime ideal (see [20] for the details of this argument). Since $\mathsf{V}(\mathfrak{p}) = \{(z, -z-1, 2) : z \in \mathbb{C}\}$, $\log|\mathsf{V}(\mathfrak{p})|$ lies in a plane at height $\log\ 2$ above

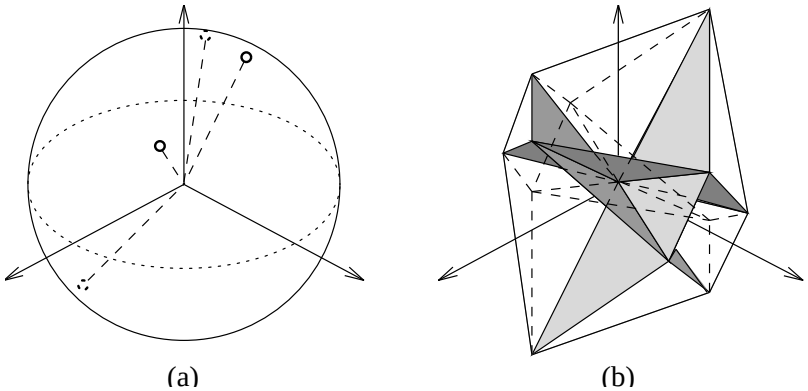

FIGURE 16. Non-expansive directions on the sphere and the corresponding planes.

the origin, and in this plane it has the shape shown in Figure 17(a), where the boundary curves are parameterized by $(\log r, \log|r \pm 1|)$ for $0 < r < \infty$. When projected onto $\mathbb{S}_2$, the set in the upper hemisphere shown in Figure 17(b) results, with three cusps on the equator.

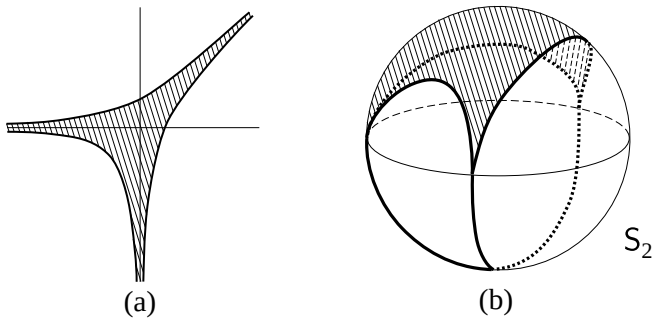

FIGURE 17. A nonexpansive set with interior.

Using Theorem 5.11, the polynomial $u_3 - 2 \in \mathfrak{p}$ witnesses that the open upper hemisphere in $\mathbb{S}_2$ is disjoint from $\mathsf{N}^{\mathsf{n}}(\alpha^{R_3/\mathfrak{p}})$. Moreover, $1 + u_1 + u_2 \in \mathfrak{p}$ shows that no points in the lower hemisphere are in $\mathsf{N}^{\mathsf{n}}(\alpha^{R_3/\mathfrak{p}})$ either, with the possible exceptions of those on the three quarter meridians shown in Figure 17(b). We will show that each of these quarter meridians is contained in $\mathsf{N}^{\mathsf{n}}(\alpha^{R_3/\mathfrak{p}})$, so that they, combined with $\mathsf{N}^{\mathsf{v}}(\alpha^{R_3/\mathfrak{p}})$ in the upper hemisphere, comprise all of $\mathsf{N}(\alpha^{R_3/\mathfrak{p}})$.

We will treat the meridian from $(0, -1, 0)$ to $(0, 0, -1)$, the other two being similar. It is enough to show that unit vectors in the directions $(0, -a, -b)$ are non-Noetherian, where a and b are positive integers (an argument in [20] shows that $\mathsf{N}^{\mathsf{n}}(\alpha^{R_3/\mathfrak{p}})$ is itself closed). Let $H \in \mathsf{H}_3$

be $\{\mathbf{x} \in \mathbb{R}^3 : \mathbf{x} \cdot (0, a, b) \geq 0\}$. The isomorphism $\phi : f \mapsto f(t, -t - 1, 2)$, $\phi\colon R_3/\mathfrak{p} \to \mathbb{Z}[t, 1/2t(t+1)]$ sends the subring R_H to $\mathbb{Z}[t^{\pm 1}, (-t - 1)^m 2^n : am + bn \geq 0]$. Then $\mathfrak{R}_3/\mathfrak{p}$ is Noetherian over R_H if and only if $\mathbb{Z}[t, 1/2t(t+1)]$ is finitely generated over $\mathbb{Z}[t^{\pm 1}, (-t-1)^m 2^n : am + bn \geq 0]$. Using the characterisation from Theorem 5.11 again, this is equivalent to whether we can write 1 as a combination, using coefficients in $\mathbb{Z}[t^{\pm 1}]$, of expressions of the form $(-t-1)^m 2^n$, where $am + bn > 0$. Suppose this to be the case, so that

$$1 = \sum_{(m,n)\in F} f_{mn}(t)(-t-1)^m\, 2^n, \tag{5.2}$$

where $f_{mn}(t) \in \mathbb{Z}[t^{\pm 1}]$ and F is a finite set of $(m, n) \in \mathbb{Z}^2$ for which $am + bn > 0$. Let $|\cdot|_2$ denote the extension of the 2-adic norm on $\mathbb{Q}$ to $\mathbb{Q}(2^{1/b})$. Substitute $t = 2^{a/b} - 1$ in (5.2). Since $|2^{a/b} - 1|_2 = 1$, it follows that $|f_{mn}(2^{a/b} - 1)|_2 \leq 1$. Hence

$$\begin{aligned} 1 = |1|_2 &= \left| \sum_{(m,n)\in F} f_{mn}(2^{a/b} - 1)(-2^{a/b})^m\, 2^n \right|_2 \\ &\leq \max_{(m,n)\in F} \left|f_{mn}(2^{a/b} - 1)\right|_2 \left|-2^{a/b}\right|_2^m \left|2\right|_2^n \\ &\leq \max_{(m,n)\in F} 2^{-(am+bn)/b} < 1. \end{aligned}$$

This contradiction shows that (5.2) is impossible, so that each rational direction $(0, -a, -b)$ is non-Noetherian.

5.2. **Adelic amoebas.** In Theorem 5.10 two entirely different kinds of reasons for non-expansiveness were presented: the module may fail to be Noetherian along the half-space H, or it may fail the variety condition. It turns out that this distinction in kind is not really necessary, and a valuation-theoretic approach gives a cleaner picture. This section is taken from Miles's thesis [52] and recent work of Einsiedler, Lind and Ward [21].

Example 5.15. To understand this, start with the very simple Example 5.12. There were three points in N, one coming from N^{v} as a result of the point $(2, 3)$ in the variety, and two coming from N^{n} corresponding to the two non-Noetherian directions. Now consider the logarithmic image of the same variety *over* $\mathbb{Q}_2$: the point $(2, 3) \in \mathbb{Q}_2^2$ has $(\log|2|_2 \log|3|_2) = (-\log 2, 0)$, giving the direction $(-1, 0)$. Similarly, the logarithmic image of the variety over $\mathbb{Q}_3$ gives the direction $(0, -1)$. Of course it is not really legitimate to select the primes 2 and 3 after we knew the answer: however, for any other prime p, the logarithmic image of the variety over $\mathbb{Q}_p$ comprises the point $(0, 0)$,

which does not project to anything more on the circle. So the union of the projections of the p-adic amoebas over all $p \leq \infty$ describes the non-expansive set.

The same thing holds in general, though it is a quite subtle and lengthy proof. With Theorem 5.10 taking care of the $p = \infty$ part, it amounts to proving a statement purely in commutative algebra. Namely: the directional Noetherian property is governed by the p-adic amoebas. A key step is to relate Theorem 5.11, an integrality condition, to the existence of a valuation that witnesses non-integrality.

Definition 5.16. For a prime ideal $\mathfrak{p} \in \mathfrak{R}_d$, define the usual amoeba to be

$$\mathrm{Am}(\mathfrak{p}) = \mathrm{Am}_\infty(\mathfrak{p}) = \{(\log|z_1|, \ldots, \log|z_d| \mid \mathbf{z} \in V_{\mathbb{C}}(\mathfrak{p})\},$$

where $V_{\mathbb{C}}$ denotes the variety over $\mathbb{C}^{ast}$. Similarly, for each prime p denote the p-adic amoeba by

$$\mathrm{Am}_p(\mathfrak{p}) = \{(\log|z_1|_p, \ldots, \log|z_d|_p \mid \mathbf{z} \in V_{\mathbb{C}_p}(\mathfrak{p})\}.$$

Finally define the *adelic amoeba* to be $\mathrm{Am}_{\mathbb{A}}(\mathfrak{p}) = \bigcup_{p \leq \infty} \mathrm{Am}_p(\mathfrak{p})$.

Theorem 5.17. *The non-expansive set* $\mathsf{N}(\alpha^{\mathfrak{R}_d/\mathfrak{p}})$ *is equal to the projection of* $\mathrm{Am}_{\mathbb{A}}(\mathfrak{p})$ *onto* $\mathbb{S}^{d-1}$.

Example 5.18. Consider Example 5.14 again. Here $d = 3$ and $\mathfrak{p} = \langle 1 + u_1 + u_2, u_3 - 2\rangle$. The usual amoeba of $\mathfrak{p}$ is that subset of $\mathbb{R}^3$ defined by

$$\mathrm{Am}_\infty(\mathfrak{p}) = \{(a, b, \log 2) \mid (a, b) \in V_{\mathbb{C}}(\langle 1 + x + y\rangle)\},$$

which looks like a copy of Figure 17(a) parallel to the (x, y)-plane at the level $z = \log 2$.

To compute the p-adic amoebas, first let k be any ultrametric field with valuation $|\cdot|$ and consider the (x, y) part. Then

$$(x, y) \in V_k(\langle 1 + x + y\rangle) \Rightarrow |x| = |1 + y|,$$

so

$$\log|y| < 0 \Rightarrow |y| < 1 \Rightarrow |x| = 1$$

by the ultrametric inequality. This means the negative y-axis is part of the amoeba. By symmetry, the negative x-axis is also in the amoeba. On the other hand,

$$\log|y| > 0 \Rightarrow |y| > 1 \Rightarrow |x| = |y|$$

by the ultrametric inequality again.

Now let $p = 2$. By the argument above, the 2-adic amoeba is the shape shown in Figure 18 since it lies at level $z = \log|2|_2 = -\log 2$.

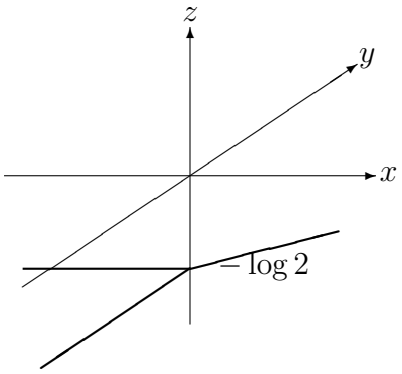

FIGURE 18. The 2-adic amoeba of $\langle 1 + u_1 + u_2, u_3 - 2\rangle$

For primes $p \neq 2$, the amoeba has the same shape in the (x, y)-plane, but at the level $z = \log |2|_{p\neq 2} = 0$, as shown in Figure 19. Projecting

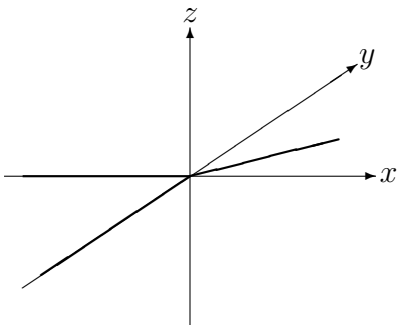

FIGURE 19. The 2-adic amoeba of $\langle 1 + u_1 + u_2, u_3 - 2\rangle$

these shapes onto the unit sphere gives the shape in Figure 17(b).

The p-adic amoebas also arise in the Biere-Strebel invariant in group theory – see [4], [3] and [21] for more details.

6. Some directions for future research

6.1. **Typical group automorphisms.** As we saw in Section 2.8, the complete picture of how many periodic points a 'typical' group automorphism has is still unknown.

6.2. **Periodic points.** How many periodic points can a compact group endomorphism have? There are some surprising examples here: in [25] a compact group automorphism T is constructed with the property that

$\mathrm{Per}_n(T)$ is the denominator of B_{2n} (the Bernoulli numbers). Specifically, if $(u_n)_{n\geq 1}$ is a sequence of positive integers with the properties

$$\sum_{d|n} \mu(n/d)u_d \equiv 0 \bmod n \text{ for all } n \geq 1 \text{ (Congruence)},$$

$$\sum_{d|n} \mu(n/d)u_d \geq 0 \text{ for all } n \geq 1 \text{ (Positivity), and}$$

$$m|n \Rightarrow u_m|u_n \text{ for all } n \geq 1 \text{ (Divisibility)}$$

is there a compact group automorphism T with $u_n = \mathrm{Per}_n(T)$ for all $n \geq 1$? For more on this, see [55] and [56].

6.3. **Mixing problem.** Is there a dynamical proof of Theorem 4.7? Even a dynamical proof that Example 4.6 is mixing of all orders seems difficult.

Is Conjecture 4.9 true? The results known suggest that there are two obstacles even for the case of principal ideals. First, the Newton polygon may be loose, opening up the possibility of a non-mixing sequence that approximates the wrong shape. Secondly, the polynomial itself may have non-zero coefficients deep inside its support.

6.4. **Entropy.** The outstanding problem here is Lehmer's problem of course.

6.5. **Entropy and Deligne periods.** A very interesting problem has been raised by Deninger in the course of his work on Mahler measures. In [16] he showed – roughly speaking – that $m(f)$ is the Deligne period of a certain mixed motive associated in a canonical way to f. Using a p-adic analogue of Deligne cohomology gives an analogous p-adic *valued* Mahler measure, m_p, described in [2]. The question raised there is whether there is a p-adic valued notion of entropy that gives entropy $m_p(f)$ to the dynamical system associated to f. A specific form of this general question is the following. Define $\log_p : \mathbb{C}_p^* \to \mathbb{C}_p$ to be the branch of the p-adic logarithm with $\log_p(p) = 0$, and consider the map $T_\lambda : x \mapsto \lambda x$ on (say) $\mathbb{Q}_p$. Is there a meaningful entropy-like invariant h_p (invariant under topological conjugacy, for example) with $h_p(T_\lambda) = \log_p \lambda$? For more background on the theory behind this question, see [2, Sect. 1.8]; for background on these questions and mixed motives, see [15], [18], [17].

References

[1] Nobuo Aoki and Haruo Totoki, *Ergodic automorphisms of $\mathbb{T}^\infty$ are Bernoulli transformations*, Publ. Res. Inst. Math. Sci. **10** (1974/75), 535–544. MR 52 #701

[2] Amnon Besser and Christopher Deninger, *p-adic Mahler measures*, J. Reine Angew. Math. **517** (1999), 19–50. MR **2001d:**11070

[3] Robert Bieri, Walter D. Neumann, and Ralph Strebel, *A geometric invariant of discrete groups*, Invent. Math. **90** (1987), no. 3, 451–477. MR **89b:**20108

[4] Robert Bieri and Ralph Strebel, *A geometric invariant for modules over an abelian group*, J. Reine Angew. Math. **322** (1981), 170–189. MR **82f:**20017

[5] Rufus Bowen, *Entropy for group endomorphisms and homogeneous spaces*, Trans. Amer. Math. Soc. **153** (1971), 401–414. MR 43 #469

[6] ———, *On Axiom A diffeomorphisms*, American Mathematical Society, Providence, R.I., 1978, Regional Conference Series in Mathematics, No. 35. MR 58 #2888

[7] David W. Boyd, *Speculations concerning the range of Mahler's measure*, Canad. Math. Bull. **24** (1981), no. 4, 453–469. MR **83h:**12002

[8] Mike Boyle and Douglas Lind, *Expansive subdynamics*, Trans. Amer. Math. Soc. **349** (1997), no. 1, 55–102. MR **97d:**58115

[9] Robert Burton and Robin Pemantle, *Local characteristics, entropy and limit theorems for spanning trees and domino tilings via transfer-impedances*, Ann. Probab. **21** (1993), no. 3, 1329–1371. MR **94m:**60019

[10] J. W. S. Cassels, *Local fields*, Cambridge University Press, Cambridge, 1986. MR **87i:**11172

[11] V. Chothi, G. Everest, and T. Ward, *S-integer dynamical systems: periodic points*, J. Reine Angew. Math. **489** (1997), 99–132. MR **99b:**11089

[12] Vijay Chothi, *Periodic Points in S-integer Dynamical Systems*, Ph.D. thesis, Univ. of East Anglia, 1996.

[13] Jean-Pierre Conze, *Points périodiques et entropie topologique*, C. R. Acad. Sci. Paris Sér. A-B **267** (1968), A149–A152. MR 37 #6920

[14] Henry Crapo and Walter Whiteley, *Spaces of stresses, projections and parallel drawings for spherical polyhedra*, Beiträge Algebra Geom. **35** (1994), no. 2, 259–281. MR **96b:**52036

[15] Christopher Deninger, *L-functions of mixed motives*, Motives (Seattle, WA, 1991), Amer. Math. Soc., Providence, RI, 1994, pp. 517–525. MR **95a:**11058

[16] ———, *Deligne periods of mixed motives, K-theory and the entropy of certain $\mathbb{Z}^n$-actions*, J. Amer. Math. Soc. **10** (1997), no. 2, 259–281. MR **97k:**11101

[17] ———, *On extensions of mixed motives*, Collect. Math. **48** (1997), no. 1-2, 97–113, Journées Arithmétiques (Barcelona, 1995). MR **98f:**11069

[18] ———, *Some analogies between number theory and dynamical systems on foliated spaces*, Proceedings of the International Congress of Mathematicians, Vol. I (Berlin, 1998), no. Extra Vol. I, 1998, pp. 163–186 (electronic). MR **99g:**11084

[19] M. Einsiedler and T. Ward, *Asymptotic geometry of non-mixing shapes*, Preprint (2000).

[20] Manfred Einsiedler, Douglas Lind, Richard Miles, and Thomas Ward, *Expansive subdynamics for algebraic $\mathbb{Z}^d$-actions*, Ergodic Theory Dynamical Systems (to appear).

[21] Manfred Einsiedler, Douglas Lind, and Thomas Ward, *p-adic amoebas and the Bieri-Strebel invariant*, Preprint.

[22] Manfred Einsiedler and Thomas Ward, *Fitting ideals for finitely presented algebraic dynamical systems*, Aequationes Math. **60** (2000), no. 1-2, 57–71. MR 1 777 892

[23] Murray Eisenberg, *Expansive automorphisms of finite-dimensional vector spaces*, Fund. Math. **59** (1966), 307–312. MR 34 #3279

[24] Murray Eisenberg and James H. Hedlund, *Expansive automorphisms of Banach spaces*, Pacific J. Math. **34** (1970), 647–656. MR 42 #5067

[25] Graham Everest, Yash Puri, and Thomas Ward, *Integer sequences counting periodic points*, Preprint.

[26] Graham Everest and Thomas Ward, *Heights of polynomials and entropy in algebraic dynamics*, Springer-Verlag London Ltd., London, 1999. MR **2000e:**11087

[27] S. Ferenczi and B. Kamiński, *Zero entropy and directional Bernoullicity of a Gaussian $\mathbb{Z}^2$-action*, Proc. Amer. Math. Soc. **123** (1995), no. 10, 3079–3083. MR **95m:**28024

[28] A. O. Gel′fond, *Transcendental and algebraic numbers*, Dover Publications Inc., New York, 1960. MR 22 #2598

[29] Paul R. Halmos, *On automorphisms of compact groups*, Bull. Amer. Math. Soc. **49** (1943), 619–624. MR 5,40c

[30] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 145, 27–38. MR **88a:**11004

[31] Erik Hemmingsen and William Reddy, *Expansive homeomorphisms on homogeneous spaces*, Fund. Math. **64** (1969), 203–207. MR 39 #3524

[32] A. Katok and R. J. Spatzier, *Invariant measures for higher-rank hyperbolic abelian actions*, Ergodic Theory Dynam. Systems **16** (1996), no. 4, 751–778. MR **97d:**58116

[33] ———, *Corrections to: "Invariant measures for higher-rank hyperbolic abelian actions" [Ergodic Theory Dynam. Systems **16** (1996), no. 4, 751–778; MR 97d:58116]*, Ergodic Theory Dynam. Systems **18** (1998), no. 2, 503–507. MR **99c:**58093

[34] Anatole Katok and Boris Hasselblatt, *Introduction to the modern theory of dynamical systems*, Cambridge University Press, Cambridge, 1995, With a supplementary chapter by Katok and Leonardo Mendoza. MR **96c:**58055

[35] Yitzhak Katznelson, *Ergodic automorphisms of $\mathbb{T}^n$ are Bernoulli shifts*, Israel J. Math. **10** (1971), 186–195. MR 45 #3672

[36] Bruce Kitchens and Klaus Schmidt, *Automorphisms of compact groups*, Ergodic Theory Dynam. Systems **9** (1989), no. 4, 691–735. MR **91g:**22008

[37] ———, *Mixing sets and relative entropies for higher-dimensional Markov shifts*, Ergodic Theory Dynam. Systems **13** (1993), no. 4, 705–735. MR **95f:**28022

[38] Wayne M. Lawton, *A problem of Boyd concerning geometric means of polynomials*, J. Number Theory **16** (1983), no. 3, 356–362. MR **84i:**10056

[39] François Ledrappier, *Un champ markovien peut être d'entropie nulle et mélangeant*, C. R. Acad. Sci. Paris Sér. A-B **287** (1978), no. 7, A561–A563. MR **80b:**28030

[40] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Annals of Math. **34** (1933), 461–479.
[41] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, Cambridge, 1986. MR **88c:**11073
[42] D. A. Lind, *Ergodic automorphisms of the infinite torus are Bernoulli*, Israel J. Math. **17** (1974), 162–168. MR 49 #10856
[43] ———, *The structure of skew products with ergodic group automorphisms*, Israel J. Math. **28** (1977), no. 3, 205–248. MR 57 #586
[44] ———, *Ergodic group automorphisms and specification*, Ergodic theory (Proc. Conf., Math. Forschungsinst., Oberwolfach, 1978), Springer, Berlin, 1979, pp. 93–104. MR **80j:**28024
[45] ———, *Dynamical properties of quasihyperbolic toral automorphisms*, Ergodic Theory Dynamical Systems **2** (1982), no. 1, 49–68. MR **84g:**28017
[46] ———, *Ergodic group automorphisms are exponentially recurrent*, Israel J. Math. **41** (1982), no. 4, 313–320. MR **83i:**28022
[47] D. A. Lind and T. Ward, *Automorphisms of solenoids and p-adic entropy*, Ergodic Theory Dynam. Systems **8** (1988), no. 3, 411–419. MR **90a:**28031
[48] Douglas Lind and Klaus Schmidt, *Bernoullicity of solenoidal automorphisms and global fields*, Israel J. Math. **87** (1994), no. 1-3, 33–35. MR **95e:**28013
[49] Douglas Lind, Klaus Schmidt, and Tom Ward, *Mahler measure and entropy for commuting automorphisms of compact groups*, Invent. Math. **101** (1990), no. 3, 593–629. MR **92j:**22013
[50] K. Mahler, *On some inequalities for polynomials in several variables*, J. London Math. Soc. **37** (1962), 341–344. MR 25 #2036
[51] G. Miles and R. K. Thomas, *Generalized torus automorphisms are Bernoullian*, Studies in probability and ergodic theory, Academic Press, New York, 1978, pp. 231–249. MR **80c:**22011
[52] Richard Miles, *Arithmetic Dynamical Systems*, Ph.D. thesis, Univ. of East Anglia, 2000.
[53] ———, *Dynamical systems arising from units in Krull rings*, Aequationes Math. **61** (2001), 113–127.
[54] Shahar Mozes, *A zero entropy, mixing of all orders tiling system*, Symbolic dynamics and its applications (New Haven, CT, 1991), Amer. Math. Soc., Providence, RI, 1992, pp. 319–325. MR **93j:**28032
[55] Yash Puri, *Arithmetic of Numbers of Periodic Points*, Ph.D. thesis, Univ. of East Anglia, 2001.
[56] Yash Puri and Thomas Ward, *Arithmetic of periodic orbits*, J. Integer Sequences (to appear).
[57] Dinakar Ramakrishnan and Robert J. Valenza, *Fourier analysis on number fields*, Springer-Verlag, New York, 1999. MR **2000d:**11002
[58] V. A. Rohlin, *The entropy of an automorphism of a compact commutative group*, Teor. Verojatnost. i Primenen. **6** (1961), 351–352. MR 27 #2605
[59] ———, *Metric properties of endomorphisms of compact commutative groups*, Izv. Akad. Nauk SSSR Ser. Mat. **28** (1964), 867–874. MR 29 #5955
[60] Daniel J. Rudolph and Klaus Schmidt, *Almost block independence and Bernoullicity of $\mathbb{Z}^d$-actions by automorphisms of compact abelian groups*, Invent. Math. **120** (1995), no. 3, 455–488. MR **96d:**22004

[61] Daniel J. Rudolph and Benjamin Weiss, *Entropy and mixing for amenable group actions*, Ann. of Math. (2) **151** (2000), no. 3, 1119–1150. MR **2001g:**37001

[62] Hans Peter Schlickewei, *S-unit equations over number fields*, Invent. Math. **102** (1990), no. 1, 95–107. MR **92c:**11028

[63] Klaus Schmidt, *Mixing automorphisms of compact groups and a theorem by Kurt Mahler*, Pacific J. Math. **137** (1989), no. 2, 371–385. MR **90c:**28031

[64] ———, *Automorphisms of compact abelian groups and affine varieties*, Proc. London Math. Soc. (3) **61** (1990), no. 3, 480–496. MR **91j:**28015

[65] ———, *Dynamical systems of algebraic origin*, Birkhäuser Verlag, Basel, 1995. MR **97c:**28041

[66] Klaus Schmidt and Tom Ward, *Mixing automorphisms of compact groups and a theorem of Schlickewei*, Invent. Math. **111** (1993), no. 1, 69–76. MR **95c:**22011

[67] Daniel S. Silver and Susan G. Williams, *Coloring link diagrams with a continuous palette*, Topology **39** (2000), no. 6, 1225–1237. MR 1 783 855

[68] ———, *A generalized Burau representation for string links*, Pacific J. Math. **197** (2001), no. 1, 241–255. MR 1 810 218

[69] S. Smale, *Differentiable dynamical systems*, Bull. Amer. Math. Soc. **73** (1967), 747–817. MR 37 #3598

[70] J. T. Tate, *Fourier analysis in number fields, and Hecke's zeta-functions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 305–347. MR 36 #121

[71] Olga Taussky, *On a theorem of Latimer and MacDuffee*, Canadian J. Math. **1** (1949), 300–302. MR 11,3k

[72] José Felipe Voloch, *The equation $ax + by = 1$ in characteristic p*, J. Number Theory **73** (1998), no. 2, 195–200. MR **2000b:**11029

[73] T. Ward, *Entropy of automorphisms of the solenoid*, Master's thesis, University of Warwick, 1986.

[74] ———, *An algebraic obstruction to isomorphism of Markov shifts with group alphabets*, Bull. London Math. Soc. **25** (1993), no. 3, 240–246. MR **94g:**22013

[75] ———, *An uncountable family of group automorphisms, and a typical member*, Bull. London Math. Soc. **29** (1997), no. 5, 577–584. MR **98k:**22028

[76] ———, *Three results on mixing shapes*, New York J. Math. **3A** (1997/98), no. Proceedings of the New York Journal of Mathematics Conference, June 9–13, 1997, 1–10 (electronic). MR **99e:**28031

[77] ———, *Almost all S-integer dynamical systems have many periodic points*, Ergodic Theory Dynam. Systems **18** (1998), no. 2, 471–486. MR **99k:**58152

[78] ———, *Dynamical zeta functions for typical extensions of full shifts*, Finite Fields Appl. **5** (1999), no. 3, 232–239. MR **2000m:**11067

[79] ———, *Additive cellular automata and volume growth*, Entropy **2** (2000), 142–167.

[80] André Weil, *Basic number theory*, Springer-Verlag, Berlin, 1995, Reprint of the second (1973) edition. MR **96c:**11002

[81] Walter Whiteley, *A matroid on hypergraphs, with applications in scene analysis and geometry*, Discrete Comput. Geom. **4** (1989), no. 1, 75–95. MR **89k:**05027

[82] S. A. Yuzvinskiĭ, *Metric properties of the endomorphisms of compact groups*, Izv. Akad. Nauk SSSR Ser. Mat. **29** (1965), 1295–1328. MR 33 #2798

[83] ———, *Calculation of the entropy of a group-endomorphism*, Sibirsk. Mat. Ž. **8** (1967), 230–239. MR 35 #5575

E-mail address: t.ward@uea.ac.uk

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, U.K.