An Introduction to Commutative Algebraic Dynamics

Klaus Schmidt

Multiplication by 2

Let $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, and let $T_2 \colon \mathbb{T} \longrightarrow \mathbb{T}$ be the surjective group homomorphism given by $T_2 x = 2x \pmod 1$ for every $x \in \mathbb{T}$.

If λ is Lebesgue measure (= length) on $\mathbb{T} = [0,1)$, and if $I = [a,b) \subset \mathbb{T} = [0,1)$, then

$$T_2^{-1}(I) = [a/2, b/2) \cup [a/2 + 1/2, b/2 + 1, 2),$$

and $\lambda(T_2^{-1}(I)) = \lambda(I)$. Hence $\lambda(T_2^{-1}(B)) = \lambda(B)$ for every Borel set $B \subset \mathbb{T}$, i.e. T_2 *preserves* λ.

Define a map $\theta \colon Y = \{0,1\}^{\mathbb{N}} \longrightarrow [0,1]$ by

$$\theta(y) = \sum_{j \geq 1} 2^{-j} y_j$$

for every $y = (y_1, y_2, \dots) \in Y$. Then θ is surjective, injective on the complement of a countable set $D \subset Y$, and

$$\theta \circ \sigma = T_2 \circ \theta$$

for every $y \in Y \setminus D$, where σ is the shift $(\sigma y)_n = y_{n+1}$ on Y.

Let $Z \subset Y$ be the set consisting of all sequences $y = (y_n)$ with $y_j y_{j+1} = 0$ for all $j \geq 1$. Then $\sigma B \subset B$, and hence $C = \theta(B) \supset T_2 C$. Note that C is infinite, but $C \neq \mathbb{T}$.

By varying this construction we get infinitely many infinite closed sets $A \subset \mathbb{T}$ which are T_2-*invariant* in the sense that $T_2 A \subset A$.

We can also construct infinitely many T_2-invariant probability measures on $\mathbb{T}$: put $\nu_p(0) = p$, $\nu_p(1) = 1 - p$ with $p \in (0, 1)$, and put $m_p = \nu_p^{\mathbb{N}}$. Then $m_p \sigma^{-1} = m_p$ and m_p is nonatomic and ergodic under σ.

For every $p \in (0, 1)$, the probability measure $\mu_p = \theta_* m_p$ (defined by $\theta_* m_p(B) = m_p(\theta^{-1}(B))$ for all Borel sets $B \subset \mathbb{T}$) is T_2-invariant, ergodic and nonatomic. We obtain uncountably many T_2-invariant, ergodic, nonatomic probability measures on $\mathbb{T}$.

The map $T_3 = 3x \pmod 1$ on $\mathbb{T}$ has similar properties: it has infinitely many infinite closed invariant subsets and uncountably many invariant, ergodic and nonatomic probability measures.

Furstenberg's example (1967)

Let α be the $\mathbb{N}^2$-action on $\mathbb{T}$ defined by

$$\alpha^{(m,n)}x = T_2^m T_3^n x = 2^m 3^n x \pmod 1$$

for every $(m,n) \in \mathbb{N}^2$ and $x \in \mathbb{T}$.

Theorem. The only infinite closed subset $A \subset \mathbb{T}$ with $\alpha^{-\mathbf{n}}A \subset A$ for all $\mathbf{n} \in \mathbb{N}^2$ is $\mathbb{T}$ itself.

Conjecture. Let μ be a nonatomic α-invariant probability measure on $\mathbb{T}$. Then $\mu = \lambda$.

Rudolph (1990) proves the conjecture under the additional hypothesis that μ is ergodic under α and at least one of the maps T_2 or T_3 is noninvertible (mod μ). The general case remains open.

Furstenberg's example shows that the dynamical properties of several commuting group automorphisms (or, in this case, homomorphisms) can differ quite radically from those of single automorphisms (or homomorphisms).

In order to understand why this is so we have to take a closer look at group automorphisms.

Basic facts from harmonic analysis

Let X be a compact abelian group with Haar measure $\lambda = \lambda_X$, and let $\mathbb{S} = \{z \in \mathbb{C} : |z| = 1\} \cong \mathbb{T}$.

The *dual group* (or *character group*) $\hat{X} = \mathrm{Hom}(X, \mathbb{S})$ is the group of all continuous homomorphisms from X into $\mathbb{S}$. We view $\hat{X}$ as a discrete additive group and denote by $\langle a, x \rangle$ the value of the character $a \in \hat{X}$ at $x \in X$. *Pontryagin's duality theorem* implies that $\hat{X}$ separates the points of X, and that every homomorphism $\chi \colon \hat{X} \longrightarrow \mathbb{S}$ is therefore of the form $\chi(a) = \langle a, x \rangle$ for some unique $x \in X$ (i.e. $\hat{\hat{X}} = X$).

Since distinct elements $a, a' \in \hat{X}$ are orthonormal in $L^2(X, \lambda)$, $\hat{X}$ is a complete orthonormal system in $L^2(X, \lambda)$ by Stone-Weierstrass.

If $Y \subset X$ is a closed subgroup then

$$Y^\perp = \{a \in \hat{X} : \langle a, x \rangle = 1 \text{ for all } x \in Y\}$$

is the *annihilator* of Y, $\hat{Y} = \hat{X}/Y^\perp$ and $\widehat{X/Y} = Y^\perp$.

Examples.

(1) $\widehat{\mathbb{Z}/n\mathbb{Z}} = \mathbb{Z}/n\mathbb{Z}$: every (continuous) homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{S}$ is of the form $m \mapsto e^{2\pi i m/n}$ for some $m \in \{0, \ldots, n-1\}$.

(2) $\hat{\mathbb{T}} = \mathbb{Z}$: every continuous homomorphism from $\mathbb{T}$ to $\mathbb{S}$ is of the form $t \mapsto e^{2\pi i k t}$ for some $k \in \mathbb{Z}$.

(3) Let $\mathbb{Z}_2$ be the group of *dyadic integers*: $\mathbb{Z}_2 = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ as a set, but we identify each $x = (x_n) \in \mathbb{Z}_2$ with the rather large integer $s(x) = \sum_{n \geq 1} x_n 2^{n-1}$. Addition is therefore component-wise, carrying to the right. For example,

$$\begin{aligned} & 1010100\ldots \\ + \ & 0111000\ldots \\ = \ & 1100010\ldots \end{aligned}$$

If $q = a/2^m$ is a dyadic rational number, then q defines an $a_q \in \widehat{\mathbb{Z}_2}$ by $\langle a_q, x \rangle = e^{2\pi i q s(x)}$ for every $x \in \mathbb{Z}_2$. Since these homomorphism separate the points of $\mathbb{Z}_2$, $\widehat{\mathbb{Z}_2} = \mathbb{Z}[\frac{1}{2}]/\mathbb{Z}$.

Group automorphisms

Let α be a continuous group automorphism of a compact abelian group X.

- For every $a \in \hat{X}$, the map $x \mapsto \langle \hat{\alpha}(a), x\rangle := \langle a, \alpha(x)\rangle$ defines an element $\hat{\alpha}(a)$ of $\hat{X}$, and the map $a \mapsto \hat{\alpha}(a)$ from $\hat{X}$ to $\hat{X}$ is the *dual automorphism* of α.
- α preserves the Haar measure of X.
- If $\hat{\alpha}$ has a finite nonzero orbit then α is nonergodic.
- If every nonzero orbit of $\hat{\alpha}$ is infinite then α is ergodic.
- If α is ergodic then it is mixing.

Exercise: Show that multiplication by 3 is an automorphism of $\mathbb{Z}[\frac{1}{2}]/\mathbb{Z}$. Hence the map $T_3 x = 3x$ is an automorphism of $\mathbb{Z}_2$. Is it ergodic?

Toral automorphisms

Let $A \in \mathrm{GL}(n, \mathbb{Z})$, and let α be the automorphism of $X = \mathbb{T}^n$ defined by the linear action of A on $\mathbb{R}^n$. Then $\hat{\alpha}$ is the linear action of $A^\top$ on $\hat{X} = \mathbb{Z}^n$.

Many dynamical properties of α can be expressed purely in terms of the eigenvalues of A.

- α is ergodic if and only if no eigenvalue of A is a root of unity ($\Leftrightarrow$ $A^\top$ has no finite nonzero orbit in $\mathbb{Z}^n$).
- The *entropy* of α is given by

$$h(\alpha) = \sum_{\gamma} \log \max(1, |\gamma|),$$

  where γ varies over the eigenvalues of A (with multiplicity).
- If α is ergodic it has positive entropy (Kronecker's Theorem). In fact, it is *Bernoulli*.

Expansiveness

The automorphism α is *expansive* if

$$\bigcap_{n\in\mathbb{Z}} \alpha^n(\mathcal{O}) = \{0\}.$$

for some open set $\mathcal{O}$ with $0 \in \mathcal{O} \subset \mathbb{T}^n$. α is expansive if and only if A has no eigenvalues of absolute value 1.

Let $\mathbb{R}^n = W^{(u)} \oplus W^{(s)} \oplus W^{(0)}$ be the decomposition of $\mathbb{R}^n$ into the *unstable* (= expanding), *stable* (= contracting) and *central* subspaces (corresponding to the eigenvalues of A with absolute values > 1, < 1 and $= 1$). If $\pi\colon \mathbb{R}^n \longrightarrow \mathbb{T}^n$ is the quotient map, then $X^{(u)} = \pi(W^{(u)})$, $X^{(s)} = \pi(W^{(s)})$ and $X^{(0)} = \pi(W^{(0)})$ are the *stable*, *unstable* and *central* subgroups of $\mathbb{T}^n$. The automorphism α is expansive (or *hyperbolic*) if and only if $W^{(0)} = \{0\}$.

A class of examples

The *shift* $(\sigma x)_n = x_{n+1}$ is an automorphism of the compact abelian group $\mathbb{T}^{\mathbb{Z}}$. For every polynomial $f(u) = f_0 + f_1 u + \cdots + f_m u^m$ with integer coefficients we set $f(\sigma) = f_0 + f_1\sigma + \cdots + f_m\sigma^m$ and define a closed, shift-invariant subgroup

$$X_f = \{(x_n) \in \mathbb{T}^{\mathbb{Z}} : f_0 x_k + \cdots + f_m x_{k+m} = 0 \text{ for all } k\} = \ker f(\sigma)$$

and denote by $\alpha_f = \sigma|_{X_f}$ the restriction of σ to X_f.

We write $R_1 = \mathbb{Z}[u^{\pm 1}]$ for the ring of Laurent polynomials with integer coefficients and identify $\widehat{\mathbb{T}^{\mathbb{Z}}} = \sum_{\mathbb{Z}} \mathbb{Z}$ with R_1 by setting

$$\langle h, x\rangle = e^{2\pi i \sum_{n\in\mathbb{Z}} h_n x_n}$$

for every $h = \sum_{n\in\mathbb{Z}} h_n u^n \in R_1$ and $x = (x_n) \in \mathbb{T}^{\mathbb{Z}}$. Under this identification

$$\widehat{X}_f = \widehat{\mathbb{T}^{\mathbb{Z}}}/X_f^{\perp} = R_1/(f),$$

where $(f) = fR_1$, and $\widehat{\alpha}_f$ is multiplication by u on $R_1/(f)$.

Dynamical properties of these examples

We assume for simplicity that the polynomial f is irreducible.

- α_f is ergodic if and only if f is not cyclotomic (i.e. f does not divide $u^m - 1$ for any $m \geq 1$ or, equivalently, no root of f is a root of unity). Reason: if α_f is nonergodic, then $\hat{\alpha}_f^n a = u^n a = a$ for some $n > 0$ and $0 \neq a \in R_1/(f)$, and hence $(u^n - 1)h \in (f)$ for some $h \notin (f)$. As f is irreducible this implies that it is cyclotomic.
- α_f is expansive if and only if f has no roots of absolute value 1. Reason: if α_f is nonexpansive, then there exist distinct points $x = (x_n)$ and $y = (y_n)$ in X_f such that

$$|x_n - y_n| < 1/3\|f\|_1 = \left(3 \sum_{n \in \mathbb{Z}} |f_n|\right)^{-1}$$

for every $n \in \mathbb{Z}$. But $z = x - y \in X_f$, and hence, for every $n \in \mathbb{Z}$, $\sum_{m \in \mathbb{Z}} f_m z_{m+n} = 0$ *in* $\mathbb{R}$, *not just in* $\mathbb{T}$. But this implies that z is a linear combination of bounded vectors of the form $w = (w_n) = (\gamma^n)$ with $f(\gamma) = 0$, i.e. that f must have roots of absolute value 1.

(1) If $f_0 f_m = \pm 1$, then the map $x = (x_n) \mapsto \phi(x) = \begin{bmatrix} x_0 \\ \vdots \\ x_{m-1} \end{bmatrix}$ is a group isomorphism from X_f to $\mathbb{T}^m$ with $\beta \circ \phi = \phi \circ \alpha_f$, where β is the toral automorphism defined by the companion matrix

$$B = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & & \cdots & 0 & 1 \\ -f_m & & & -f_2 & -f_1 \end{bmatrix}$$

of f. The eigenvalues of B are the roots of f, and α_f is ergodic (or expansive) if and only if f has no unit roots (or roots of absolute value 1).

Let us try this with $f = 1 + u - u^2$: then $B = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right]$.

Which matrices B can we get in this way? More generally, if we call $B, B' \in \mathrm{GL}(n, \mathbb{Z})$ *algebraically conjugate* if there exists a $C \in \mathrm{GL}(n, \mathbb{Z})$ with $BC = CB'$, can we get all $B \in \mathrm{GL}(n, \mathbb{Z})$ up to algebraic conjugacy?

Exercise: You can get $\left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right]$, but not $\left[\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right]$. Why not?

(2) Let $f = 2 - u$. Then

$$X_f = \widehat{R_1/(f)} = \{(x_n) \in \mathbb{T}^{\mathbb{Z}} : x_{n+1} = 2x_n \text{ for all } n\},$$

and the surjective group homomorphism $\phi(x) = x_0$ from X_f to $\mathbb{T}$ satisfies that $\phi \circ \alpha_f = T_2 \circ \phi$, where α_f is the shift on X_f. Note that α_f is expansive, since f has no roots of absolute value 1.

What is X_f?

(a) X_f a projective limit of tori $\cdots \xrightarrow{T_2} \mathbb{T} \xrightarrow{T_2} \mathbb{T} \xrightarrow{T_2} \mathbb{T}$, and α_f acts as multiplication by 2 on each component,

(b) $X_f = (\mathbb{R} \times \mathbb{Z}_2)/\mathbb{Z}[\frac{1}{2}]$, where $\mathbb{Z}_2$ is the dyadic integers, $\mathbb{Z}[\frac{1}{2}]$ is diagonally embedded in $\mathbb{R} \times \mathbb{Z}_2$, and α_f is multiplication by 2 on each component of $\mathbb{R} \times \mathbb{Z}_2$.

In (b) you can see explicitly the expanding and contracting subgroups $(\mathbb{R} \times \{0\})/\mathbb{Z}$ and $(\{0\} \times \mathbb{Z}_2)/\mathbb{Z}$ of the 'hyperbolic' automorphism α_f.

(3) Let $f = 3 - 2u$. Then

$$X_f = \widehat{R_1/(f)} = \{(x_n) \in \mathbb{T}^{\mathbb{Z}} : 2x_{n+1} = 3x_n \text{ for all } n\}$$
$$\cong (\mathbb{R} \times \mathbb{Z}_2 \times \mathbb{Z}_3)/\mathbb{Z}[\tfrac{1}{6}],$$

where $\mathbb{Z}_3$ denotes the tri-adic integers, $\mathbb{Z}[\frac{1}{6}]$ is again embedded diagonally (where we are using that multiplication by 2 and 3 are automorphisms of $\mathbb{Z}_3$ and $\mathbb{Z}_2$, respectively), and the shift α_f on X_f corresponds to multiplication by 3/2 on each component of $\mathbb{R} \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

Note that multiplication by 3/2 expands $(\mathbb{R} \times \mathbb{Z}_2 \times \{0\})/\mathbb{Z}[\frac{1}{6}]$ and contracts $(\{0\} \times \{0\} \times \mathbb{Z}_3)/\mathbb{Z}[\frac{1}{6}]$ and is thus again 'hyperbolic'.

Commuting group automorphisms

The last examples show that certain automorphisms of compact abelian groups are dual to multiplication by the variable u on the R_1-module $R_1/(f)$, where $f \in R_1$ is a Laurent polynomial.

More generally, if α is *any* continuous automorphism of a compact abelian group X, then $M = \widehat{X}$ is a module over the ring R_1 with module operation

$$h \cdot a = \sum_{n \in \mathbb{Z}} h_n \widehat{\alpha}^n(a)$$

for every $a \in \widehat{X}$ and $h = \sum_{n \in \mathbb{Z}} h_n u^n \in R_1$, and $\widehat{\alpha}(a) = u \cdot a$.

Conversely, every R_1-module M defines an automorphism α_M of the compact abelian group $X_M = \widehat{M}$ dual to multiplication by u on M.

This also works if we replace R_1 by the ring $R_d = \mathbb{Z}[u_1^{\pm 1}, \ldots, u_d^{\pm 1}]$ of Laurent polynomials in d variables: if M is a module over R_d, then we obtain d commuting automorphisms $\alpha_1, \ldots, \alpha_d$ of $X_M = \widehat{M}$ dual to multiplication by $u_1, \ldots, u_d$, and hence a $\mathbb{Z}^d$-action $\mathbf{n} = (n_1, \ldots, n_d) \mapsto \alpha^{\mathbf{n}} = \alpha_1^{n_1} \cdots \alpha_d^{n_d}$ by automorphisms of X_M.

Conversely, if $\alpha_1, \ldots, \alpha_d$ are commuting automorphisms of a compact abelian group X, then the dual group $M = \hat{X}$ is a module over the ring R_d with module operation

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

for every $a \in \hat{X}$ and $h = \sum_{\mathbf{n} \in \mathbb{Z}^d} h_{\mathbf{n}} u^{\mathbf{n}}$, where $\alpha^{\mathbf{n}} = \alpha_1^{n_1} \cdots \alpha_d^{n_d}$ and $u^{\mathbf{n}} = u_1^{n_1} \cdots u_d^{n_d}$ for all $\mathbf{n} = (n_1, \ldots, n_d) \in \mathbb{Z}^d$. This module $M = \hat{X}$ is the *dual module* of the $\mathbb{Z}^d$-action $\alpha \colon \mathbf{n} \mapsto \alpha^{\mathbf{n}}$.

The simplest R_d-modules are those of the form R_d/I, where $I \subset R_d$ is an ideal. We denote by σ the shift-action $(\sigma^{\mathbf{m}} x)_{\mathbf{n}} = x_{\mathbf{m}+\mathbf{n}}$ of $\mathbb{Z}^d$ on $\mathbb{T}^{\mathbb{Z}^d}$ and set $f(\sigma) = \sum_{\mathbf{n} \in \mathbb{Z}^d} f_{\mathbf{n}} \sigma^{\mathbf{n}}$ for every $f = \sum_{\mathbf{n} \in \mathbb{Z}^d} f_{\mathbf{n}} u^{\mathbf{n}}$. As before we see that

$$X_{R_d/I} = \{x \in \mathbb{T}^{\mathbb{Z}^d} : f(\sigma) = 0 \text{ for all } f \in I\} = \bigcap_{f \in I} \ker f(\sigma),$$

and that $\alpha_{R_d/I} = \sigma|_{X_{R_d/I}}$ is the restriction of σ to $X_{R_d/I}$.

(1) Let $I = (2-u_1, 3-u_2) = (2-u_1)R_2 + (3-u_2)R_2 \subset R_2$. Then

$$\widehat{R_2/I} = X_{R_2/I} = \{x = (x_{k,l}) \in \mathbb{T}^{\mathbb{Z}^2} : \\ x_{k+1,l} = 2x_{k,l} \text{ and } x_{k,l+1} = 3x_{k,l} \text{ for all } k, l\}.$$

The group homomorphism $\phi(x) = x_{0,0}$ from $X_{R_2/I}$ to $\mathbb{T}$ satisfies that $\phi \circ \alpha^{(1,0)}_{R_2/I} = T_2 \circ \phi$ and $\phi \circ \alpha^{(0,1)}_{R_2/I} = T_3 \circ \phi$ (Furstenberg's example).

(2) Let α be the $\mathbb{Z}^2$-action on $\mathbb{T}^3$ given by $\alpha^{\mathbf{n}} = A^{n_1}B^{n_2}$ for every $\mathbf{n} = (n_1, n_2) \in \mathbb{Z}^2$, where

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

We know that $\alpha = \alpha_M$ for some R_2-module M. Is $M = R_2/I$ for some ideal I? If so, what is I?

Hint: A is the companion matrix of the irreducible polynomial

$$g = x^3 + 3x^2 - 6x + 1,$$

and $B = 2I - 4A - A^2$.

The dictionary

We have established a one-to-one correspondence between R_d-modules and algebraic $\mathbb{Z}^d$-actions α_M (i.e. $\mathbb{Z}^d$-actions by automorphisms of compact abelian groups) and R_d-modules M. This correspondence should enable us to translate dynamical properties of α_M into algebraic properties of M and to 'design' $\mathbb{Z}^d$-actions by using commutative algebra.

It turns out that many properties of α_M can be expressed in terms of the *associated prime ideals* of M, i.e. in terms of the prime ideals $\mathfrak{p} \subset R_d$ of the form

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

for some $a \in M$. The set of prime ideals associated with M is denoted by asc(M); if M is Noetherian then asc(M) is finite.

	Property	$\alpha = \alpha_{R_d/\mathfrak{p}}$	$\alpha = \alpha_M$
1	Expansive-ness	$V_{\mathbb{C}}(\mathfrak{p}) \cap \mathbb{S}^d = \varnothing$	M is Noetherian and $\alpha_{R_d/\mathfrak{p}}$ is expansive for every $\mathfrak{p} \in \mathrm{asc}(M)$
2	Ergodicity	$\{u^{k\mathbf{n}} - 1 : \mathbf{n} \in \mathbb{Z}^d\} \not\subset \mathfrak{p}$ for every $k \geq 1$	$\alpha_{R_d/\mathfrak{p}}$ is ergodic for every $\mathfrak{p} \in \mathrm{asc}(M)$
3	Mixing	$u^{\mathbf{n}} - 1 \notin \mathfrak{p}$ for every $\mathbf{n} \in \mathbb{Z}^d$, $\mathbf{n} \neq \mathbf{0}$	$\alpha_{R_d/\mathfrak{p}}$ is mixing for every $\mathfrak{p} \in \mathrm{asc}(M)$
4	Mixing of every order	$\mathfrak{p} = pR_d$ for some $p \in \mathbb{Z}$, or $\mathfrak{p} \cap \mathbb{Z} = \{0\}$ and $\alpha_{R_d/\mathfrak{p}}$ is mixing	For every $\mathfrak{p} \in \mathrm{asc}(M)$, $\alpha_{R_d/\mathfrak{p}}$ is mixing of every order
5	$h(\alpha) > 0$	$\mathfrak{p}$ is principal and $\alpha_{R_d/\mathfrak{p}}$ is mixing	$h(\alpha_{R_d/\mathfrak{p}}) > 0$ for some $\mathfrak{p} \in \mathrm{asc}(M)$
6	$h(\alpha) < \infty$	$\mathfrak{p} \neq \{0\}$	If M is Noetherian: $\{0\} \notin \mathrm{asc}(M)$
7	Bernoulli	$h(\alpha^{R_d/\mathfrak{p}}) > 0$	$h(\alpha_{R_d/\mathfrak{p}}) > 0$ for every $\mathfrak{p} \in \mathrm{asc}(M)$

The correspondence between 'algebra' and 'dynamics' goes quite deep. Let us pursue this connection in the case of mixing.

Higher order mixing

Let α be an algebraic $\mathbb{Z}^d$-action with dual module $M = \widehat{X}$. If α is not mixing, then there exist Borel sets $B_1, B_2 \subset X$, a sequence $(\mathbf{n}_k,\, k \geq 1)$ in $\mathbb{Z}^d$ with $\lim_{k\to\infty} \mathbf{n}_k = \infty$, and a $c \geq 0$ with

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

Fourier expansion yields $a_1, a_2 \in M \setminus \{0\}$ such that

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

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

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

for some nonzero $\mathbf{m} \in \mathbb{Z}^d$.

More generally, α is not mixing of order $r \geq 2$ (or r-mixing) if and only if there exist Borel sets $B_1, \ldots, B_r$ in X and a sequence $((\mathbf{n}_k^{(1)}, \ldots, \mathbf{n}_k^{(r)}), k \geq 1)$ in $(\mathbb{Z}^d)^r$ such that

$$\lim_{k\to\infty} \mathbf{n}_k^{(i)} - \mathbf{n}_k^{(j)} = \infty$$

for $i \neq j$ and

$$c = \lim_{k\to\infty} \lambda_X\left(\bigcap_{i=1}^{r} \alpha^{-\mathbf{n}_k^{(i)}} B_i\right) \neq \prod_{i=1}^{r} \lambda_X(B_i),$$

and hence elements $a_1, \ldots, a_r$ in M, not all equal to zero, with

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

for every $k \geq 1$.

It is a famous open problem whether a single mixing (= 2-mixing) transformation can fail to be r-mixing for some $r \geq 3$, but every mixing group automorphism is certainly mixing of all orders.

For algebraic $\mathbb{Z}^d$-actions with $d > 1$, higher order mixing may fail, and it may even fail in a particularly regular way, as the following example shows.

Example (Ledrappier). Let $\mathfrak{p} = (2, 1 + u_1 + u_2) = 2R_2 + (1 + u_1 + u_2)R_2$, $M = R_2/\mathfrak{p}$, and let $\alpha = \alpha_M$ be the corresponding algebraic $\mathbb{Z}^2$-action on $X = X_M = \widehat{M}$. Then α is mixing, but not three-mixing, and

$$\lambda_X(B \cap \alpha^{-(n,0)}(B) \cap \alpha^{-(0,n)}(B)) \not\to \lambda_X(B)^3$$

for some Borel set $B \subset X$, as $n \to \infty$.

Remember that

$$X = \{(x_{\mathbf{n}}) \in \mathbb{T}^{\mathbb{Z}^2} : x_{(n_1,n_2)} \in \{0, 1/2\} \text{ and}$$
$$x_{(n_1,n_2)} + x_{(n_1+1,n_2)} + x_{(n_1,n_2)} = 0 \text{ for all } (n_1, n_2)\}.$$

Since $(1 + u_1 + u_2)^{2^n} - (1 + u_1^{2^n} + u_2^{2^n}) \in \mathfrak{p}$ for every $n \geq 1$, we get that $1 + u_1^{2^n} + u_2^{2^n} \in \mathfrak{p}$ and

$$x_{(n_1,n_2)} + x_{(n_1+2^n,n_2)} + x_{(n_1,n_2+2^n)} = 0 \pmod 1.$$

for every $n \geq 1$. For $B = \{x \in X : x_{(0,0)} = 0\}$ it follows that

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

and

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

for every $n \geq 0$.

This example suggests the following definition:

A nonempty finite subset $S \subset \mathbb{Z}^d$ is *mixing* under α if

$$\lim_{k\to\infty} \lambda_X\left(\bigcap_{\mathbf{n}\in S} \alpha^{-k\mathbf{n}} B_{\mathbf{n}}\right) = \prod_{\mathbf{n}\in S} \lambda_X(B_{\mathbf{n}})$$

for all Borel sets $B_{\mathbf{n}} \subset X$, $\mathbf{n} \in S$, and *nonmixing* otherwise.

In the last example, the set $S = \{(0,0),(1,0),(0,1)\}$ turned out to be nonmixing.

If α is r-mixing, then every set $S \subset \mathbb{Z}^d$ with cardinality $|S| = r$ is obviously mixing. The reverse implication for algebraic $\mathbb{Z}^d$-actions is a much more complicated problem.

As in (1) one sees that a nonempty finite set $S \subset \mathbb{Z}^d$ is nonmixing if and only if there exist elements $a_{\mathbf{n}} \in M$, $\mathbf{n} \in S$, not all equal to zero, such that

$$\sum_{\mathbf{n}\in S} u^{k\mathbf{n}} \cdot a_{\mathbf{n}} = 0 \tag{2}$$

for infinitely many $k \geq 1$.

The higher order mixing behaviour of an algebraic $\mathbb{Z}^d$-action α with dual module M is again completely determined by that of the actions $\alpha_{R_d/\mathfrak{p}}$ with $\mathfrak{p} \in \mathrm{asc}(M)$.

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

(1) For every $r \geq 2$, α is r-mixing if and only if $\alpha_{R_d/\mathfrak{p}}$ is r-mixing for every $\mathfrak{p} \in \mathrm{asc}(M)$.

(2) For every nonempty finite set $S \subset \mathbb{Z}^d$, S is α-mixing if and only if S is $\alpha_{R_d/\mathfrak{p}}$-mixing for every $\mathfrak{p} \in \mathrm{asc}(M)$.

In order to exhibit the connection between mixing properties and additive relations in fields we need a simple observation:

Let $\mathfrak{p} \subset R_d$ be a prime ideal, and let $K = Q(R_d/\mathfrak{p})$ be the field of fractions of the integral domain $R_d/\mathfrak{p}$. Then the following are equivalent:

(1) $X_{R_d/\mathfrak{p}}$ is connected,

(2) $\mathfrak{p}$ contains no nonzero constant,

(3) $\mathrm{char}(K) = 0$.

We begin with the connected case and recall a famous result by Mahler.

Theorem. Let K be a field of characteristic 0 and let $a_1, \ldots, a_r$ be nonzero elements of K. If we can find nonzero elements $c_1, \ldots, c_r$ such that the equation

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

has infinitely many solutions $k \geq 0$, then there exist integers $s \geq 1$ and i, j with $1 \leq i < j \leq r$ such that $a_i^s = a_j^s$.

We set $K = Q(R_d/\mathfrak{p}) \supset R_d/\mathfrak{p}$, choose a finite set $S = \{\mathbf{n}_1, \ldots, \mathbf{n}_r\} \subset \mathbb{Z}^d$ and set $a_i = u^{\mathbf{n}_i}$ for $i = 1, \ldots, r$. Mahler's Theorem is equivalent to the following statement:

Theorem. Let α be a mixing algebraic $\mathbb{Z}^d$-action on a compact connected abelian group. Then every finite subset $S \subset \mathbb{Z}^d$ is mixing.

If an algebraic $\mathbb{Z}^d$-action α is not mixing of every order, then there exists a smallest integer $r \geq 2$ such that α is not r-mixing. We set $K = Q(R_d/\mathfrak{p})$ and write $G \subset K^\times$ for the subgroup $\{u^{\mathbf{n}} : \mathbf{n} \in \mathbb{Z}^d\}$. The assumption that $\alpha_{R_d/\mathfrak{p}}$ is mixing is equivalent to the condition that $G \cong \mathbb{Z}^d$. The following results are again equivalent.

Theorem (S-unit theorem). Let K be a field of characteristic 0 and G a finitely generated multiplicative subgroup of $K^\times = K \setminus \{0\}$. If $r \geq 2$ and $(c_1, \ldots, c_r) \in (K^\times)^r$, then the equation

$$\sum_{i=1}^{r-1} c_i a_i = 1 \tag{3}$$

has only finitely many solutions $(a_1, \ldots, a_{r-1}) \in G^{r-1}$ such that no sub-sum on the left-hand side of (3) vanishes.

Theorem. Let α be a mixing algebraic $\mathbb{Z}^d$-action on a compact connected abelian group X. Then α is mixing of every order.

For algebraic $\mathbb{Z}^d$-actions on disconnected groups the situation is considerably more complicated due to the possible presence of nonmixing sets.

The following result by Masser (already translated into our dynamical setting) allows one to determine the nonmixing sets of $\alpha_{R_d/\mathfrak{p}}$:

Theorem. Let $\mathfrak{p} \subset R_d$ be a prime ideal containing a rational prime $p > 1$, and let $\alpha = \alpha_{R_d/\mathfrak{p}}$ on $X = X_{R_d/\mathfrak{p}}$. Let $\bar{K}$ be the algebraic closure of the quotient field $K = Q(R_d/\mathfrak{p}) \supset R_d/\mathfrak{p}$. For every nonempty finite set $S \subset \mathbb{Z}^d$ the following conditions are equivalent:

(1) S is not α-mixing;

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

The 'order of mixing' problem is solved by another recent result by Masser:

Theorem. If $\alpha_{R_d/\mathfrak{p}}$ is not r-mixing, then there exists a nonmixing set of size r.

Isomorphism rigidity

Two measure-preserving $\mathbb{Z}^d$-actions α_1 and α_2 on probability spaces $(X_i, \mathcal{S}_i, \mu_i)$ are *measurably conjugate* if there exists a measure-preserving isomorphism $\phi\colon X_1 \longrightarrow X_2$ which is *equivariant*, i.e. which satisfies that $\phi \circ \alpha_1^{\mathbf{n}} = \alpha_2^{\mathbf{n}} \circ \phi$ μ_1-*a.e.*, for every $\mathbf{n} \in \mathbb{Z}^d$.

For a single ergodic toral automorphism α, entropy is a complete invariant of measurable conjugacy, since α is Bernoulli. In particular, α is conjugate to α^{-1}, α^2 is conjugate to $\alpha \times \alpha$, etc.

The same is true for algebraic $\mathbb{Z}^d$-actions which have completely positive entropy (and are therefore Bernoulli).

For algebraic $\mathbb{Z}^d$-actions with zero entropy (like commuting toral automorphisms) the picture changes.

Theorem. Let $d > 1$, and let $\mathfrak{p}_i$, $i = 1, 2$, be prime ideals in R_d such that $\alpha_{R_d/\mathfrak{p}_i}$ is mixing and has entropy zero. Then every measurable equivariant map $\phi\colon X_{R_d/\mathfrak{p}_1} = \widehat{R_d/\mathfrak{p}_1} \longrightarrow X_{R_d/\mathfrak{p}_2} = \widehat{R_d/\mathfrak{p}_2}$ coincides *a.e.* with an affine map.

Example.

Let α be the $\mathbb{Z}^2$-action on $\mathbb{T}^3$ given by $\alpha^{\mathbf{n}} = A^{n_1}B^{n_2}$ for every $\mathbf{n} = (n_1, n_2) \in \mathbb{Z}^2$, where

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

The matrices A and B have the same irreducible characteristic polynomial

$$g = x^3 + 3x^2 - 6x + 1,$$

and α is expansive and mixing.

Let $V = \begin{bmatrix} -2 & 2 & 1 \\ 0 & 3 & 0 \\ -1 & 4 & 2 \end{bmatrix}$, put

$$A' = V^{-1}AV = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 6 & -3 \end{bmatrix}, \qquad B' = V^{-1}BV = \begin{bmatrix} -2 & 4 & 1 \\ -1 & 4 & 1 \\ -1 & 5 & 1 \end{bmatrix},$$

and denote by α' the $\mathbb{Z}^2$-action $\mathbf{n} \mapsto A'^{n_1}B'^{n_2}$. It is clear that $\alpha^{\mathbf{n}}$ and $\alpha'^{\mathbf{n}}$ are measurably conjugate for every $\mathbf{n} \in \mathbb{Z}^2$. However, A and A' are not algebraically conjugate (why not?), and hence α and α' are not algebraically — and therefore also not measurably — conjugate.