

MIXING AUTOMORPHISMS OF COMPACT GROUPS AND A THEOREM BY KURT MAHLER

KLAUS SCHMIDT

Dedicated to the memory of Henry Abel Dye

We investigate the higher order mixing properties of \mathbb{Z}^d -actions by automorphisms of a compact, abelian group and exhibit a connection between certain mixing conditions and a result by Kurt Mahler.

1. Introduction. Let X be a compact, abelian group, and let $\text{Aut}(X)$ denote the group of continuous automorphisms of X . We investigate the mixing behaviour of \mathbb{Z}^d -actions $\alpha: \mathbf{n} \rightarrow \alpha_{\mathbf{n}}$ on X with the property that $\alpha_{\mathbf{n}} \in \text{Aut}(X)$ for every $\mathbf{n} \in \mathbb{Z}^d$ (such an action will be called a \mathbb{Z}^d -action by automorphisms). If (X, α) satisfies the *descending chain condition*, i.e. if every decreasing sequence of closed, α -invariant subgroups of X eventually becomes constant, then α is algebraically and topologically conjugate to the shift action on a closed, shift invariant subgroup of $(\mathbb{T}^k)^{\mathbb{Z}^d}$, where $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, and is automatically a *Markov shift* in d dimensions (cf. [KS] for a more general result). Furthermore it is easy to see that the dual group \hat{X} of X can naturally be viewed as a finitely generated R_d -module, where R_d is the ring of Laurent polynomials in d variables with integral coefficients (cf. [KS]). In view of this correspondence between finitely generated R_d -modules and \mathbb{Z}^d -actions by automorphisms of compact, abelian groups the question arises how the algebraic properties of the R_d -module $M = \hat{X}$ reflect the dynamical properties of the \mathbb{Z}^d -action α . In [S2] it was shown how to read off ergodicity, mixing, expansiveness, and certain facts about periodic orbits, from properties of the prime ideals associated with the R_d -module M . In this paper we continue this investigation and study the higher order mixing behaviour of such actions. This problem was raised by a paper of F. Ledrappier which contains examples of such actions which are (strongly) mixing, but which fail to be r -mixing for some $r \geq 2$. In these examples higher order mixing breaks down in a particularly interesting way: there exist a nonempty set $S \subset \mathbb{Z}^d$ and Borel sets $\{B_{\mathbf{n}} \subset X: \mathbf{n} \in S\}$ with positive Haar measure such that the sets $\{\alpha_{k\mathbf{n}}(B_{\mathbf{n}}): \mathbf{n} \in S\}$ fail to become asymptotically independent as $k \rightarrow \infty$. In order to simplify terminology we call the set S a *mixing*

shape if the sets $\{\alpha_{k\mathbf{n}}(B_{\mathbf{n}}) : \mathbf{n} \in S\}$ become asymptotically independent as $k \rightarrow \infty$, irrespective of the choice of $\{B_{\mathbf{n}} \subset X : \mathbf{n} \in S\}$.

If the action α is r -mixing for every $r \geq 1$, then every shape $S \subset \mathbb{Z}^d$ must obviously be mixing, but the converse is not at all clear. In §3 we prove the following results: if α is mixing and X is connected, then every shape $S \subset \mathbb{Z}^d$ is mixing. If X is zero dimensional, then there exist shapes which are not mixing, unless the prime ideals associated with the module $M = \hat{X}$ are all of the form $p_i = \pi_i R_d$, where $\pi_i \in \mathbb{Z}$ is a rational prime. Furthermore, if X is zero dimensional, then α is r -mixing for every $r \geq 1$ if and only if every shape $S \subset \mathbb{Z}^d$ is mixing. I was unable to prove the corresponding result for connected groups.

The statement about mixing shapes for connected groups turns out to be intimately linked with a result due to Kurt Mahler [Ma]: if c_1, \dots, c_m and a_1, \dots, a_m are nonzero algebraic numbers, and if $c_1 a_1^k + \dots + c_m a_m^k = 0$ for infinitely many $k \geq 1$, then there exists an arithmetic progression $P \subset \mathbb{N}$ such that $c_1 a_1^k + \dots + c_m a_m^k = 0$ for every $k \in P$. Since we need this result in a slightly strengthened form (with c_i, a_i in an arbitrary field of characteristic 0) we include a proof of Mahler's result, adapted to this case, §2.

Finally a remark about notation: $\mathbb{C}, \mathbb{N}, \mathbb{Q}, \mathbb{R}$ will denote the complex, natural, rational and real numbers, and $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. If R is a ring then R^\times will stand for the group of units in R , and $R[x_1, \dots, x_n]$ is the ring of polynomials in the variables x_1, \dots, x_n with coefficients in R . If $R = \mathbb{Z}$ or \mathbb{Q} , and if $I \subset R[x_1, \dots, x_n]$ is an ideal, we set $V(I) = \{(c_1, \dots, c_n) \in (\mathbb{Q}^-)^n : f(c_1, \dots, c_n) = 0 \text{ for every } f \in I\}$, where \mathbb{Q}^- is the algebraic closure of \mathbb{Q} .

Acknowledgment. I would like to thank the Institute for Advanced Study, Princeton, for hospitality and support during the Spring Term 1988, when this work was carried out. Special thanks are due to Enrico Bombieri for pointing out to me Mahler's paper [Ma] and for helpful discussions.

2. Mahler's theorem.

2.1. THEOREM([Ma]). *Let k be an algebraic number field of degree $(k : \mathbb{Q}) = d$, $q \geq 2$, and let $\alpha_1, \dots, \alpha_q$ be nonzero elements in k . Suppose that there exist an infinite sequence $m_1 < m_2 < \dots$ in \mathbb{N} and nonzero elements c_1, \dots, c_q in k such that*

$$(2.2) \quad c_1 \alpha_1^{m_j} + c_2 \alpha_2^{m_j} + \dots + c_q \alpha_q^{m_j} = 0$$

for every $j \geq 1$. Let $p \geq 2$ be a rational prime and let v be a valuation of k above p such that $|\alpha_i|_v = 1$ for $i = 1, \dots, q$. Then there exist integers a, b such that

$$(2.3) \quad 1 \leq a < p^{2d^2}, \quad 0 \leq b < a,$$

$$(2.4) \quad c_1 \alpha_1^{ja+b} + c_2 \alpha_2^{ja+b} + \dots + c_q \alpha_q^{ja+b} = 0 \quad \text{for every } j \geq 0,$$

and

$$(2.5) \quad \alpha_i^a = \alpha_{i'}^a \quad \text{for some } i, i' \text{ with } 1 \leq i < i' \leq q.$$

Proof. Denote by k_v , I_v , and r_v the completion of k with respect to v , the maximal compact subring of k_v , and the maximal ideal of I_v , respectively, and choose a prime element $\pi \in r_v$ (i.e. $|\pi|_v = \sup\{|\alpha|_v : \alpha \in k \text{ and } |\alpha|_v < 1\}$). Since $\text{card}(k_v/r_v^{2d}) \leq p^{2d^2}$ we can find an integer a with $1 \leq a < p^{2d^2}$ such that $\alpha^a \equiv 1 \pmod{r_v^{2d}}$ for every $\alpha \in k$ with $|\alpha|_v = 1$, and we set $\beta_i \pi^{2d} = \alpha_i^a - 1$, $1 \leq i \leq q$. Fix i for the moment and observe that, for every $z \in \mathbb{N}$,

$$(2.6) \quad \alpha_i^{az} = (1 + \beta_i \pi^{2d})^z = \sum_{j=0}^{\infty} \beta_i^j \pi^{2dj} \binom{z}{j}.$$

The polynomial

$$P_j(z) = \binom{z}{j} \cdot j! = z \cdot (z-1) \cdot \dots \cdot (z-j+1)$$

has integral coefficients. For every $j \geq 0$, the highest power $t \geq 0$ such that p^t divides $j!$ satisfies that $t < j/p + j/p^2 + \dots = j/(p-1) \leq j$, and we conclude that $|j!|_v > |p^j|_v \geq |\pi^{dj}|_v$ and $|\pi^{dj}/j!|_v < 1$. We can thus rearrange the sum in (2.6) as

$$(2.7) \quad \sum_{j=0}^{\infty} \beta_i^j \pi^{2dj} P_j(x)/j! = \sum_{j=0}^{\infty} \gamma_i(j) x^j = f_i(x),$$

where $x \in I_v$, $\gamma_i(j) \in k_v$ and $|\gamma_i(j)|_v \leq |\pi^{dj}|_v$ for every $j \geq 0$, and obtain a well defined function $f_i: I_v \rightarrow I_v$ with $f_i(x) = \alpha_i^{ax}$ whenever $x \in \mathbb{N}$. Assume without loss in generality that $|c_i|_v \leq 1$ for $i = 1, \dots, q$, choose an integer b with $0 \leq b < a$ and $m_j \equiv b \pmod{a}$ for infinitely many $j \geq 1$, and define $g: I_v \rightarrow I_v$ by

$$(2.8) \quad \begin{aligned} g(x) &= c_1 \alpha_1^b f_1(x) + \dots + c_q \alpha_q^b f_q(x) \\ &= \sum_{j=0}^{\infty} (c_1 \alpha_1^b \gamma_1(j) + \dots + c_q \alpha_q^b \gamma_q(j)) x^j. \end{aligned}$$

Note that g is a power series which converges for every $x \in I_v$, and that there exists an infinite set $S \subset I_v$ such that $g(x) = 0$ for every $x \in S$. Since I_v is compact, S has a limit point y , and $g(y) = 0$. Exactly as in the case of a complex power series one concludes that $g(x) = 0$ for every $x \in I_v$. In particular

$$g(z) = c_1 \alpha_1^b f_1(z) + \cdots + c_q \alpha_q^b f_q(z) = c_1 \alpha_1^{az+b} + \cdots + c_q \alpha_q^{az+b} = 0$$

for every $z \in \mathbb{N}$, which proves (2.4). Condition (2.5) follows from the fact that

$$\det \begin{pmatrix} 1 & \cdots & 1 \\ \alpha_1^a & \cdots & \alpha_q^a \\ \vdots & \ddots & \vdots \\ \alpha_1^{a(q-1)} & \cdots & \alpha_q^{a(q-1)} \end{pmatrix} = 0. \quad \square$$

2.2. COROLLARY. *Let $m_1 < m_2 < \cdots$ be an infinite sequence in \mathbb{N} , and let $n \geq 2$. For every $1 \leq j_1 < j_2 < \cdots < j_n$ we define a polynomial*

$$(2.9) \quad P_{(j_1, \dots, j_n)}(x_1, \dots, x_n) = \det \begin{pmatrix} x_1^{m_{j_1}} & \cdots & x_n^{m_{j_1}} \\ \vdots & \ddots & \vdots \\ x_1^{m_{j_n}} & \cdots & x_n^{m_{j_n}} \end{pmatrix}$$

with integral coefficients, and we denote by $I \subset \mathbf{R} = \mathbb{Q}[x_1, \dots, x_n]$ the ideal generated by $\{P_{(j_1, \dots, j_n)} : 1 \leq j_1 < \cdots < j_n\}$. Then there exists an integer $a \geq 1$ such that

$$(2.10) \quad V(I) \subset V(\Delta(x_1^a, \dots, x_n^a)),$$

where

$$(2.11) \quad \Delta(x_1^a, \dots, x_n^a) = \prod_{1 \leq i < j \leq n} (x_j^a - x_i^a).$$

Proof. Since we can find prime ideals $\{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ in \mathbf{R} such that $V(I) = \bigcup_{i=1}^s V(\mathfrak{p}_i)$ it will be sufficient to prove that there exists, for every prime ideal \mathfrak{p} in \mathbf{R} with $\mathfrak{p} \supset I$, an integer $a \geq 1$ with $V(\Delta(x_1^a, \dots, x_n^a)) \supset V(\mathfrak{p})$.

Indeed, let $I \subset \mathfrak{p} \subset \mathbf{R}$ be a prime ideal. If $V(\mathfrak{p})$ is finite, our assertion follows from Theorem 2.1. Assume therefore that $V(\mathfrak{p})$ is infinite and set $R' = \mathbf{R}/\mathfrak{p}$. For every polynomial $f \in \mathbf{R}$ we denote by $f = f + \mathfrak{p}$ the corresponding element in R' and we put $y_i = x'_i$, $i = 1, \dots, n$. The Noether normalization lemma [AM] allows us to find an integer $1 \leq m \leq n$ and linear functions z_1, \dots, z_m of the elements y_1, \dots, y_n in R' such that the z_1, \dots, z_m are algebraically independent and each

y_i is algebraic and integral over $\mathbb{Q}[z_1, \dots, z_m] \subset R'$. Choose and fix monic polynomials $Q_i \in \mathbb{Q}[z_1, \dots, z_m][y]$ such that $Q_i(y_i) = 0$ for $i = 1, \dots, n$. We regard each Q_i either as a polynomial in y with coefficients in $\mathbb{Q}[z_1, \dots, z_m]$ or as an element of $\mathbb{Q}[z_1, \dots, z_m, y]$, and (ab)use the notation $Q_i = Q_i(y) = Q_i(z_1, \dots, z_m, y)$, $i = 1, \dots, n$, depending on our point of view. Let $\eta: V(\mathfrak{p}) \rightarrow (\mathbb{Q}^-)^m$ be the surjective map

$$\eta(\alpha_1, \dots, \alpha_n) = (z_1(\alpha_1, \dots, \alpha_n), \dots, z_m(\alpha_1, \dots, \alpha_n)),$$

$(\alpha_1, \dots, \alpha_n) \in V(\mathfrak{p}) \subset (\mathbb{Q}^-)^n$. Then $\eta^{-1}(\beta_1, \dots, \beta_m)$ is finite for every $(\beta_1, \dots, \beta_m) \in (\mathbb{Q}^-)^m$, and $Q_i(\beta_1, \dots, \beta_m, \alpha_i) = 0$ for every $(\alpha_1, \dots, \alpha_n) \in \eta^{-1}(\beta_1, \dots, \beta_m)$ and $i = 1, \dots, n$. Put $K = \{u + v\sqrt{-1} : u, v \in \mathbb{Q}\} \subset \mathbb{C}$. We denote by $\{P_s(z_1, \dots, z_m) : 0 \leq s \leq t\}$ the set of coefficients of the polynomials $Q_i \in \mathbb{Q}[z_1, \dots, z_m][y]$, $i = 1, \dots, n$, and claim that there exists a valuation w of K such that

$$\Sigma = \{(\beta_1, \dots, \beta_m) \in K^m : |P_s(\beta_1, \dots, \beta_m)|_w = 1 \text{ for every } s = 0, \dots, t\}$$

is dense in \mathbb{C}^m . Indeed, choose w so that, for every $s = 0, \dots, t$, the coefficients $c_{i,s}$ of the polynomial $P_s \in \mathbb{Q}[z_1, \dots, z_m]$ all satisfy $|c_{i,s}|_w = 1$, and such that $|P_s(1, \dots, 1)|_w = 1$. If $r_w = \{\beta \in K : |\beta|_w < 1\}$, then $q_w = 1 + r_w \subset K$ is dense in \mathbb{C} , and $|P_s(\beta_1, \dots, \beta_m)|_w = 1$ for all $(\beta_1, \dots, \beta_m) \in q_w^m$ and $s = 0, \dots, t$. Hence $q_w^m \subset \Sigma$, and Σ is dense in \mathbb{C}^m .

There exists an integer $d \geq 1$ such that, for every $(\beta_1, \dots, \beta_m) \in K^m$ and $(\alpha_1, \dots, \alpha_n) \in \eta^{-1}(\beta_1, \dots, \beta_m)$, the algebraic number field $K(\alpha_1, \dots, \alpha_n)$ generated by K and $(\alpha_1, \dots, \alpha_n)$ has degree $(K(\alpha_1, \dots, \alpha_n) : \mathbb{Q}) \leq d$. Now consider elements $(\beta_1, \dots, \beta_m) \in \Sigma$ and $(\alpha_1, \dots, \alpha_n) \in \eta^{-1}(\beta_1, \dots, \beta_m) \subset V(I)$. If v is a valuation of $K(\alpha_1, \dots, \alpha_n)$ above w , then $|\alpha_i|_v = 1$ for $i = 1, \dots, n$, and there exist constants c_1, \dots, c_n in $K(\alpha_1, \dots, \alpha_n)$ such that $c_i \neq 0$ for some $i \in \{1, \dots, n\}$ and

$$c_1 \alpha_1^{m_j} + c_2 \alpha_2^{m_j} + \dots + c_q \alpha_q^{m_j} = 0$$

for every $j \geq 1$. After renumbering the α_i we may assume that $c_1 \neq 0, \dots, c_q \neq 0$, and $c_{q+1} = \dots = c_n = 0$. We denote by π the rational prime below v (or w), apply Theorem 2.1 to find an integer a' such that $1 \leq a' \leq \pi^{2d^2}$ and $\alpha_i^{a'} = \alpha_{i'}^{a'}$ for some $1 \leq i < i' \leq q$, and conclude that $(\alpha_1, \dots, \alpha_n) \in V(\Delta(x_1^{a'}, \dots, x_n^{a'}))$.

We have shown that $(\alpha_1, \dots, \alpha_n) \in V(\Delta(x_1^a, \dots, x_n^a))$ for all $(\alpha_1, \dots, \alpha_n) \in \eta^{-1}(\Sigma)$, where $a = \pi^{2d^2!}$ and $\Sigma \subset K^m \subset \mathbb{C}^m$ is dense in

\mathbb{C}^m . Hence $V(\Delta(x_1^a, \dots, x_n^a)) \cap V(\mathfrak{p})$ is both Zariski-dense and closed in the Zariski-closed set $V(\mathfrak{p})$, i.e. $V(\Delta(x_1^a, \dots, x_n^a)) \supset V(\mathfrak{p})$. Since $I \subset \mathfrak{p} \subset \mathbf{R}$ was an arbitrary prime ideal we obtain (2.10). \square

2.3. COROLLARY. *Let K be a field of characteristic 0, $q \geq 2$, and let $\alpha_1, \dots, \alpha_q$ be elements in K^\times . Suppose that there exist an infinite sequence $m_1 < m_2 < \dots$ in \mathbb{N} and c_1, \dots, c_q in K^\times such that*

$$(2.12) \quad c_1 \alpha_1^{m_j} + c_2 \alpha_2^{m_j} + \dots + c_q \alpha_q^{m_j} = 0$$

for every $j \geq 1$. Then there exist integers a, b such that $a \geq 1$, $0 \leq b < a$,

$$(2.13) \quad c_1 \alpha_1^{ja+b} + c_2 \alpha_2^{ja+b} + \dots + c_q \alpha_q^{ja+b} = 0 \quad \text{for every } j \geq 0,$$

and

$$(2.14) \quad \alpha_i^a = \alpha_{i'}^a \quad \text{for some } i, i' \text{ with } 1 \leq i < i' \leq q.$$

3. Mixing shapes and multiple mixing for group automorphisms. Let (X, μ) be a Lebesgue probability space, $d \geq 1$, and let $\alpha: (\mathbf{n}, x) \rightarrow \alpha_{\mathbf{n}}(x)$, $\mathbf{n} \in \mathbb{Z}^d$, $x \in X$, be a measure preserving \mathbb{Z}^d -action on X . The action α is *mixing of order r* (or *r -mixing*) if, for all measurable sets B_0, B_1, \dots, B_r in X ,

$$(3.1) \quad \lim_{\substack{\mathbf{n}_i \in \mathbb{Z}^d \text{ and } \mathbf{n}_i \rightarrow \infty, \mathbf{n}_i - \mathbf{n}_j \rightarrow \infty \\ \text{for all } i, j = 1, \dots, r, i \neq j}} \mu(B_0 \cap \alpha_{\mathbf{n}_1}(B_1) \cap \dots \cap \alpha_{\mathbf{n}_r}(B_r)) \\ = \mu(B_0) \cdot \mu(B_1) \cdot \dots \cdot \mu(B_r).$$

For a general discussion of mixing (i.e. 1-mixing) group actions we refer to [Dy] or [S1]. In the study of commuting automorphisms of compact groups one is naturally led to another concept related to multiple mixing, that of *mixing shapes*.

3.1. DEFINITION. A *shape* is a nonempty subset of \mathbb{Z}^d . A shape $S = \{\mathbf{n}_0, \mathbf{n}_1, \dots, \mathbf{n}_r\} \subset \mathbb{Z}^d$ is *mixing* under α if, for all measurable sets B_0, B_1, \dots, B_r in X ,

$$(3.2) \quad \lim_{k \rightarrow \infty} \mu(\alpha_{k\mathbf{n}_0}(B_0) \cap \alpha_{k\mathbf{n}_1}(B_1) \cap \dots \cap \alpha_{k\mathbf{n}_r}(B_r)) \\ = \mu(B_0) \cdot \mu(B_1) \cdot \dots \cdot \mu(B_r).$$

Clearly, if α is r -mixing, then every shape $S \subset \mathbb{Z}^d$ of cardinality $r + 1$ is mixing. The converse is probably not true unless, of course, $r = 1$.

Now assume that X is a compact group with Haar measure λ and that $d \geq 1$. A homomorphism $\alpha: \mathbf{n} \rightarrow \alpha_{\mathbf{n}}$ from \mathbb{Z}^d into $\text{Aut}(X)$ will be called a \mathbb{Z}^d -action on X by automorphisms. We say that (X, α) satisfies the *descending chain condition* if, whenever $X_1 \supset X_2 \supset \cdots \supset X_n \supset \cdots$ is a decreasing sequence of closed, α -invariant subgroups of X , there exists an integer $N \geq 1$ such that $X_n = X_N$ for all $n \geq N$. The pair (X, α) is *expansive* if there exists an open neighbourhood $N(\mathbf{1})$ of the identity element $\mathbf{1} \in X$ such that

$$(3.3) \quad \bigcap_{\mathbf{n} \in \mathbb{Z}^d} \alpha_{\mathbf{n}}(N(\mathbf{1})) = \{\mathbf{1}\}.$$

It is not difficult to verify that X must be metrizable if (X, α) is either expansive or satisfies the descending chain condition. Furthermore expansiveness implies the descending chain condition (cf. [KS, Theorem 5.2]). Finally, if X is connected and (X, α) satisfies the descending chain condition, then X is abelian (cf. [L]).

In order to analyze such dynamical systems (X, α) in more detail we have to introduce some notation. Let $R_d = \mathbb{Z}[u_1^{\pm 1}, \dots, u_d^{\pm 1}]$ and $\mathbf{R}_d = \mathbb{Q} \cdot R_d = \mathbb{Q}[u_1^{\pm 1}, \dots, u_d^{\pm 1}]$ be the rings of Laurent polynomials with integral (resp. rational) coefficients in the commuting variables u_1, \dots, u_d , and put $u^{\mathbf{n}} = u_1^{n_1} \cdots u_d^{n_d} \in R_d$ for every $\mathbf{n} = (n_1, \dots, n_d) \in \mathbb{Z}^d$. If N is an R_d -module and $\mathbf{n} \in \mathbb{Z}^d$ we define an automorphism $\beta_{\mathbf{n}} = \beta_{\mathbf{n}}^N$ of the additive group N by

$$(3.4) \quad \beta_{\mathbf{n}}^N(a) = u^{\mathbf{n}} \cdot a \quad \text{for every } a \in N$$

and obtain a dual automorphism

$$(3.5) \quad \alpha_{\mathbf{n}} = \alpha_{\mathbf{n}}^N = \hat{\beta}_{\mathbf{n}}^N \in \text{Aut}(\hat{N}),$$

where \hat{N} is the dual group of the additive group N .

3.2. PROPOSITION. *Let X be a compact, metrizable, abelian group, and let $\alpha: \mathbb{Z}^d \rightarrow \text{Aut}(X)$ be a \mathbb{Z}^d -action on X by automorphisms. Then there exists an R_d -module N such that $\hat{N} = X$ and $\alpha_{\mathbf{n}}^N$ for every $\mathbf{n} \in \mathbb{Z}^d$. Conversely, if N is an R_d -module, $X^N = \hat{N}$, and $\{\alpha_{\mathbf{n}}^N: \mathbf{n} \in \mathbb{Z}^d\} \subset \text{Aut}(X^N)$ is defined by (3.4) and (3.5), then $\alpha^N: \mathbf{n} \rightarrow \alpha_{\mathbf{n}}^N$ is a \mathbb{Z}^d -action on X^N by automorphisms, and (X^N, α^N) satisfies the descending chain condition if and only if N is finitely generated. The submodules $N' \subset N$ are in one-to-one correspondence with the closed, α^N -invariant subgroups $X^{N'}$ of X^N , and this correspondence is given by $X^{N'} = N'^{\perp}$, where $N'^{\perp} \subset \hat{N}$ is the annihilator of N' . Finally, if M is a second R_d -module, $X^M = \hat{M}$, and $\{\alpha_{\mathbf{n}}^M: \mathbf{n} \in \mathbb{Z}^d\} \subset \text{Aut}(\hat{M})$ is defined by (3.4)*

and (3.5), then every continuous algebraic isomorphism $\psi: X^M \rightarrow X^N$ with the property that $\psi\alpha_{\mathbf{n}}^M = \chi_{\mathbf{n}}^N\psi$ for all $\mathbf{n} \in \mathbb{Z}^d$ induces a dual module isomorphism $\eta: N \rightarrow M$.

Proof. [KS, Theorems 11.8 and 5.2]. □

We shall always assume that N is finitely generated. It turns out that many of the dynamical properties of (X^N, α^N) (like ergodicity, mixing, and expansiveness) can be described in terms of the associated prime ideals of the R_d -module N (cf. [S2]). Recall that a prime ideal $p \subset R_d$ is associated with N if and only if there exists an element $a \in N$ such that

$$p = \text{ann}(a) = \{f \in R_d: f \cdot a = 0\}.$$

The set $\{p_1, \dots, p_m\}$ of associated primes of N is finite, and

$$(3.6) \quad \bigcup_{i=1}^m p_i = \{f \in R_d: f \cdot a = 0 \text{ for some } a \neq 0 \text{ in } N\}.$$

For background we refer to [La].

We shall study higher order mixing properties of \mathbb{Z}^d -actions $\alpha: \mathbf{n} \rightarrow \alpha_{\mathbf{n}}$ by automorphisms of a compact group X under the assumption that (X, α) satisfies the descending chain condition. One checks easily that α is mixing (with respect to the Haar measure λ) if and only if $\alpha_{\mathbf{n}}$ is ergodic for every nonzero $\mathbf{n} \in \mathbb{Z}^d$ (cf. e.g. [KS, Theorem 2.4]). If $d = 1$, $\alpha \in \text{Aut}(X)$, and α is ergodic, then it is well known (and easy to see) that $n \rightarrow \alpha^n$ is r -mixing for every $r \geq 1$. As F. Ledrappier pointed out in [Le], the analogous result does not always hold if $d > 1$: there are closed, shift invariant subgroups $X \subset (\mathbb{Z}/2\mathbb{Z})^{\mathbb{Z}^2}$ on which the shift-action of \mathbb{Z}^2 is mixing, but which have nonmixing shapes. In this section we prove the following.

3.3. THEOREM. *Let X be a compact, abelian group, $d > 1$, and let $\alpha: \mathbf{n} \rightarrow \alpha_{\mathbf{n}}$ be a mixing \mathbb{Z}^d -action on X by automorphisms such that (X, α) satisfies the descending chain condition.*

- (1) *If X is connected, every shape $S \subset \mathbb{Z}^d$ is mixing.*
- (2) *If X is zero dimensional, the following conditions are equivalent:*
 - (i) *every shape $S \subset \mathbb{Z}^d$ is mixing;*
 - (ii) *the \mathbb{Z}^d -action α is r -mixing for every $r \geq 1$;*
 - (iii) *the set $\{p_1, \dots, p_m\}$ of associated prime ideals of the R_d -module $M = \hat{X}$ is given by $p_i = \pi_i R_d$, $i = 1, \dots, m$, where $\{\pi_1, \dots, \pi_m\} \subset \mathbb{Z}$ are distinct rational primes.*

3.4. COROLLARY. *Let X be a compact, abelian group and let $\alpha: \mathbf{n} \rightarrow \alpha_{\mathbf{n}}$ be a mixing \mathbb{Z}^d -action on X by automorphisms such that (X, α) satisfies the descending chain condition. Let $M = \hat{X}$ be the finitely generated R_d -module arising from Proposition 3.2, and let $\{p_1, \dots, p_m\}$ be the set of associated prime ideals of M . Then the following conditions are equivalent.*

- (1) *Every shape $S \subset \mathbb{Z}^d$ is mixing under α ;*
- (2) *for all i , either $p_i \cap \mathbb{Z} = \{0\}$, or $p_i = \pi_i R_d$ for a rational prime $\pi_i \in \mathbb{Z}$.*

For the proofs of Theorem 3.3 and Corollary 3.4 we require several lemmas.

3.5. LEMMA. *Let X be a compact, metrizable, abelian group with Haar measure λ and dual group \hat{X} , and let $\alpha: \mathbb{Z}^d \rightarrow \text{Aut}(X)$ be given as in the statement of Theorem 3.3. A shape $S = \{\mathbf{n}_0, \mathbf{n}_1, \dots, \mathbf{n}_r\} \subset \mathbb{Z}^d$ is mixing under α if and only if, for all characters χ_0, \dots, χ_r in \hat{X} with $\chi_j \neq 1$ for some $j \in \{0, \dots, r\}$,*

$$(3.7) \quad \lim_{k \rightarrow \infty} \int (\chi_0 \cdot \alpha_{k\mathbf{n}_0}) \cdot \dots \cdot (\chi_r \cdot \alpha_{k\mathbf{n}_r}) d\lambda = 0.$$

The action α is r -mixing if and only if, for all characters χ_0, \dots, χ_r in \hat{X} with $\chi_j \neq 1$ for some $j \in \{0, \dots, r\}$,

$$(3.8) \quad \lim_{\substack{\mathbf{n}_i \in \mathbb{Z}^d \text{ and } \mathbf{n}_i \rightarrow \infty, \mathbf{n}_i - \mathbf{n}_j \rightarrow \infty \\ \text{for all } i, j = 1, \dots, r, i \neq j}} \int (\chi_0 \cdot \alpha_{\mathbf{n}_0}) \cdot \dots \cdot (\chi_r \cdot \alpha_{\mathbf{n}_r}) d\lambda = 0.$$

Proof. Expand the indicator functions of B_0, \dots, B_r in (3.2) as Fourier series. □

3.6. LEMMA. *If the group X in Theorem 3.3 is connected, every shape $S \subset \mathbb{Z}^d$ is mixing.*

Proof. We apply Lemma 3.2 to obtain a finitely generated R_d -module M such that $X = \hat{M}$ and $\alpha_{\mathbf{n}} = \alpha_{\mathbf{n}}^M$ for every $\mathbf{n} \in \mathbb{Z}^d$. Let $\{p_1, \dots, p_m\}$ be the set of prime ideals in R_d associated with M and let $\{W_1, \dots, W_m\}$ be a reduced primary decomposition of 0 in M such that M/W_i is associated with p_i for all $i = 1, \dots, m$ (cf. [La]). In particular,

$$(3.9) \quad \bigcap_{i=1, \dots, m} W_i = \{0\}.$$

Now assume that the \mathbb{Z}^d -action α is mixing, but that there exists a shape $S = \{\mathbf{n}_0, \dots, \mathbf{n}_r\} \subset \mathbb{Z}^d$ which is not mixing. Lemma 3.5 implies that there exist elements $a_i \in M$, $i = 0, \dots, r$, and a sequence $k_1 < k_2 < \dots$ in \mathbb{N} such that $a_i \neq 0$ for some $i \in \{0, \dots, r\}$, but

$$(3.10) \quad (\chi_{a_0} \cdot \alpha_{k_j \mathbf{n}_0}) \cdot \dots \cdot (\chi_{a_r} \cdot \alpha_{k_j \mathbf{n}_r}) = 1$$

for every $j \geq 1$, where $\chi_a \in \hat{X}$ is the character of X corresponding to an element $a \in M \cong \hat{X}$. According to (3.4) and (3.5), equation (3.10) is equivalent to the assertion that

$$(3.11) \quad u^{k_j \mathbf{n}_0} a_0 + \dots + u^{k_j \mathbf{n}_r} a_r = 0 \quad \text{for every } j \geq 1.$$

Equation (3.9) shows that there exists an integer $i \in \{1, \dots, m\}$ such that $a_j \notin W_i$ for at least one $j \in \{0, \dots, r\}$, and we set $N = M/W_i$, denote the image of a_i in N under the quotient map again by a_i , and regard (3.11) as an equation in N . Since the group X is connected, the module M is torsion-free as an additive group, and (3.6) shows that $p_i \cap \mathbb{Z} = \{0\}$ where $\mathbb{Z} \subset R_d$ is the set of constants. Since N is associated with the prime ideal p_i we know that the additive group N is again torsion-free. Put $\mathbf{N} = \mathbb{Q} \otimes_{\mathbb{Z}} N$, and note that the natural homomorphism $\iota: N \rightarrow \mathbf{N}$ is injective, and that \mathbf{N} is an \mathbf{R}_d -module with associated prime ideal $\mathbf{p} = \mathbb{Q} \otimes_{\mathbb{Z}} p_i$. An elementary argument allows us to choose sub- \mathbf{R}_d -modules $\mathbf{N} = \mathbf{N}_0 \supset \dots \supset \mathbf{N}_s = \{0\}$ of \mathbf{N} such that, for every $j = 0, \dots, s-1$, $\mathbf{N}_j/\mathbf{N}_{j+1} \cong \mathbf{R}_d/\mathbf{q}_j$ for some prime ideal $\mathbf{p} \subset \mathbf{q}_j \subset \mathbf{R}_d$, and $\mathbf{q}_{s-1} = \mathbf{p}$. We set $a_{1,i} = \iota(a_i) \in \mathbf{N}$ and obtain that $a_{1,i} \neq 0$ for some $i \in \{1, \dots, r\}$, but that

$$u^{k_j \mathbf{n}_0} a_{1,0} + \dots + u^{k_j \mathbf{n}_r} a_{1,r} = 0 \quad \text{for every } j \geq 1.$$

There exists an integer $t \in \{0, \dots, s-1\}$ such that $\{a_{1,0}, \dots, a_{1,r}\} \subset \mathbf{N}_t$ and

$$u^{k_j \mathbf{n}_0} a_{1,0} + \dots + u^{k_j \mathbf{n}_r} a_{1,r} = 0 \in \mathbf{N}_{t+1},$$

but $a_{1,i} \notin \mathbf{N}_{t+1}$ for some $i \in \{0, \dots, r\}$. After renumbering the \mathbf{n}_i and $a_{1,i}$, if necessary, we obtain nonzero elements $b_0, \dots, b_{r'}$ in $\mathbf{R}_d/\mathbf{q}_t$, $0 \leq r' \leq r$, with

$$(3.12) \quad u^{k_j \mathbf{n}_0} b_0 + \dots + u^{k_j \mathbf{n}_{r'}} b_{r'} = 0 \in \mathbf{R}_d/\mathbf{q}_t$$

for every $j \geq 1$. Since $\mathbf{R}_d/\mathbf{q}_t$ is an integral domain we can apply Corollary 2.3 to the field of fractions of $\mathbf{R}_d/\mathbf{q}_t$ and conclude from (3.12) that there exist integers $b \geq 1$ and $i, i' \in \{0, \dots, r'\}$ such that

$i \neq i'$ and $u^{bn_i} - u^{bn_{i'}} \in \mathfrak{q}_t$. If $u^{bn_i} - u^{bn_{i'}} \notin \mathfrak{p}$ we set

$$a_{2,j} = (u^{bn_i} - u^{bn_{i'}}) \cdot a_{1,j} \in \mathbf{N}_{t+1}, \quad j = 0, \dots, r.$$

Then $a_{2,j} \neq 0$ for at least one $j \in \{1, \dots, r\}$, but

$$u^{k_j n_0} a_{2,0} + \dots + u^{k_j n_r} a_{2,r} = 0$$

for every $j \geq 1$, and a repetition of the previous argument yields integers $c \geq 1$ and $j, j' \in \{0, \dots, r\}$ such that $j \neq j'$ and $u^{cn_j} - u^{cn_{j'}} \in \mathfrak{q}_{t+1}$. If $u^{cn_j} - u^{cn_{j'}} \notin \mathfrak{p}$ we continue this process. Since $\mathfrak{q}_{s-1} = \mathfrak{p}$ we eventually obtain integers $k \geq 1$ and l, l' with $l \neq l'$ and $u^{kn_l} - u^{kn_{l'}} \in \mathfrak{p}$. Hence $u^{kn_l} - u^{kn_{l'}} \in p_i$, and [S2, Theorem 3.5] shows that α is not mixing, in contradiction to our assumption. It follows that every shape $S \subset \mathbb{Z}^d$ must be mixing. \square

3.7. LEMMA. *Suppose that X is zero dimensional, and that every shape $S \subset \mathbb{Z}^d$ is mixing under the \mathbb{Z}^d -action α . If $\{p_1, \dots, p_m\}$ is the set of associated primes of the R_d -module $M = \hat{X}$, then there exist rational primes π_1, \dots, π_m such that $p_i = \pi_i R_d$ for $i = 1, \dots, m$.*

Proof. As in the proof of Lemma 3.6 we choose a reduced primary decomposition $\{M_1, \dots, M_m\}$ of 0 in M such that M/M_i is associated with p_i for every i . If $i \in \{1, \dots, m\}$ is fixed, a standard argument allows us to find an element $a \in M$ such that $\text{ann}(a) = \{f \in R_d : f \cdot a = 0\} = p_i$, so that the submodule $N = R_d a \subset M$ is isomorphic to R_d/p_i . Since N is a torsion group, there exists a rational prime (constant) $\pi_i \in p_i$. Suppose that $p_i \supsetneq \pi_i R_d$, fix a polynomial $f \in p_i \setminus \pi_i R_d$, and write $f = \sum_{\mathbf{n} \in S} c_{\mathbf{n}} \cdot u^{\mathbf{n}}$, where $S \subset \mathbb{Z}^d$ is a nonempty finite set and $c_{\mathbf{n}} \in \{1, \dots, \pi_i - 1\}$ for all $\mathbf{n} \in S$. For all $j \geq 1$,

$$f^{\pi^j} \cdot a = \sum_{\mathbf{n} \in S} c_{\mathbf{n}} \cdot u^{\pi^j \mathbf{n}} \cdot a = 0$$

and

$$(3.13) \quad \prod_{\mathbf{n} \in S} (\chi_{c_{\mathbf{n}} \cdot a} \cdot \alpha_{\pi^j \mathbf{n}}) = 1,$$

where, for every $\mathbf{n} \in S$, $\chi_{c_{\mathbf{n}} \cdot a}$ is the nontrivial character of X corresponding to the nonzero element $c_{\mathbf{n}} \cdot a \in N \subset M$. By lemma 3.5 the set S is not mixing, contrary to our assumption. We conclude that $p_i = \pi_i R_d$ for every $i = 1, \dots, m$. \square

3.8. LEMMA. *Let $\{p_1, \dots, p_m\}$ be the set of associated primes of the R_d -module $M = \hat{X}$, and assume that there exist rational primes π_1, \dots, π_m such that $p_i = \pi_i R_d$ for $i = 1, \dots, m$. Then α is r -mixing for every $r \geq 1$.*

Proof. We use the notation of Lemma 3.7. Since $\{M_1, \dots, M_m\}$ is a reduced primary decomposition of 0 in $M = \hat{X}$, $\bigcap_{i=1, \dots, m} M_i = \{0\}$, the homomorphism $\eta: a \rightarrow (a + M_1, \dots, a + M_m)$ from M into $N_1 \oplus \dots \oplus N_m$ is injective, where $N_i = M/M_i$, and the dual homomorphism $\tau: \hat{N}_1 \oplus \dots \oplus \hat{N}_m \rightarrow X$ is surjective. We define $\beta_{\mathbf{n}}^{N_i}$ and $\alpha_{\mathbf{n}}^{N_i}$ by (3.4) and (3.5), write $\beta_{\mathbf{n}}$ for the automorphism of M dual to $\alpha_{\mathbf{n}}$, and note that

$$\eta \cdot \beta_{\mathbf{n}} = (\beta_{\mathbf{n}}^{N_1} \oplus \dots \oplus \beta_{\mathbf{n}}^{N_m}) \cdot \eta$$

and

$$(3.14) \quad \tau \cdot \alpha_{\mathbf{n}} = (\alpha_{\mathbf{n}}^{N_1} \oplus \dots \oplus \alpha_{\mathbf{n}}^{N_m}) \cdot \tau$$

for every $\mathbf{n} \in \mathbb{Z}^d$. We set $X_i = \hat{N}_i$, $i = 1, \dots, m$, and claim that the \mathbb{Z}^d -action $\mathbf{n} \rightarrow \alpha_{\mathbf{n}}^{N_1} \oplus \dots \oplus \alpha_{\mathbf{n}}^{N_m}$ on $X_1 \oplus \dots \oplus X_m$ is r -mixing for every $r \geq 1$. In view of (3.14) this will prove that α is r -mixing for every $r \geq 1$.

Suppose that there exists an integer $r \geq 1$ such that the \mathbb{Z}^d -action $\mathbf{n} \rightarrow \alpha_{\mathbf{n}}^{N_1} \oplus \dots \oplus \alpha_{\mathbf{n}}^{N_m} = \delta_{\mathbf{n}}$ on $X_1 \oplus \dots \oplus X_m$ is not r -mixing. Lemma 3.5 implies that there exist characters χ_0, \dots, χ_r of $X_1 \oplus \dots \oplus X_m$ such that $\chi_i \neq 1$ for some $i \in \{0, \dots, r\}$, but

$$(3.15) \quad (\chi_0 \cdot \delta_{\mathbf{n}_{0,j}}) \cdot \dots \cdot (\chi_r \cdot \delta_{\mathbf{n}_{r,j}}) = 1$$

for every $j \geq 1$, where $((\mathbf{n}_{0,j}, \dots, \mathbf{n}_{r,j}), j \geq 1)$ is a sequence in $\mathbb{Z}^{(r+1)d}$ with

$$\lim_{j \rightarrow \infty} \mathbf{n}_{i,j} = \lim_{j \rightarrow \infty} (\mathbf{n}_{i,j} - \mathbf{n}_{i',j}) = \infty \quad \text{for all } i, i' \in \{0, \dots, r\} \text{ with } i \neq i'.$$

There exists an integer $K \geq 1$ such that $\pi_i^K a = 0$ for every $i \in \{1, \dots, m\}$ and every $a \in N_i$. Put $P_{i,j} = \{a \in N_i: \pi_i^j a = 0\}$ and $P_j = P_{1,j} \oplus \dots \oplus P_{m,j}$, $i = 1, \dots, m$, $j = 0, \dots, K$. We write $Y_j = P_j^\perp$ for the annihilator of P_j in $X_1 \oplus \dots \oplus X_m$. Assume that, for some $j \geq 0$, the restriction of every χ_i to Y_j is trivial. We shall complete the proof of this lemma by showing that the restriction of each χ_i to Y_{j+1} is also trivial. An induction argument then shows that the characters χ_0, \dots, χ_r of $X_1 \oplus \dots \oplus X_m$ are all trivial, and the resulting contradiction implies that the \mathbb{Z}^d -actions $\mathbf{n} \rightarrow \delta_{\mathbf{n}}$ and $\mathbf{n} \rightarrow \alpha_{\mathbf{n}}$ are mixing of every order.

For every $i = 1, \dots, m$, put $L_i = P_{i,j+1}/P_{i,j}$, and fix i for the moment. Since $\pi_i L_i = \{0\}$ we may regard L_i in an obvious manner as an $R_{\pi_i, d}$ -module, where $R_{\pi_i, d} = \mathbb{Z}/\pi_i[u_1^{\pm 1}, \dots, u_d^{\pm 1}]$ is the ring of Laurent polynomials in u_1, \dots, u_d with coefficients in the prime field $\mathbb{Z}/\pi_i = \mathbb{Z}/\pi_i \mathbb{Z}$. Put

$$\mathbf{L}_i = k \otimes_{R_{\pi_i, d}} L_i,$$

where k is the field of fractions of the integral domain $R_{\pi_i, d}$. Since $f \cdot a \neq 0$ for every $f \neq 0$ in $R_{\pi_i, d}$ and $a \neq 0$ in L_i , the natural injection $\iota_i: L_i \rightarrow \mathbf{L}_i$ is injective. Choose a basis e_1, \dots, e_s of the vector space \mathbf{L}_i over k , assume without loss in generality that $\{e_1, \dots, e_s\} \subset \iota_i(L_i)$, and find an element $\kappa \in k$ such that $\iota_i(L_i) \subset R_{\pi_i, d} \cdot \kappa e_1 + \dots + R_{\pi_i, d} \cdot \kappa e_s = Q_i \subset \mathbf{L}_i$. In this manner we obtain an $R_{\pi_i, d}$ -module $Q_i \cong (R_{\pi_i, d})^s$ and an injective module homomorphism $\iota_i: L_i \rightarrow Q_i$. Since every $R_{\pi_i, d}$ -module may also be regarded as an R_d -module we shall view $R_{\pi_i, d}$, $(R_{\pi_i, d})^s$ and Q_i as R_d -modules and ι_i as an injective R_d -module homomorphism. There is an obvious isomorphism $\psi: \hat{R}_{\pi_i, d} \rightarrow (\mathbb{Z}/\pi_i)^{\mathbb{Z}^d}$ such that

$$\psi \alpha_{\mathbf{n}}^{R_{\pi_i, d}} = T_{\mathbf{n}} \quad \text{for every } \mathbf{n} \in \mathbb{Z}^d,$$

where $T_{\mathbf{n}}$ denotes the shift on $(\mathbb{Z}/\pi_i)^{\mathbb{Z}^d}$ defined by

$$(3.16) \quad (T_{\mathbf{n}} \chi)(\mathbf{m}) = \chi(\mathbf{m} + \mathbf{n}), \quad \mathbf{m} \in \mathbb{Z}^d.$$

This allows us to identify \hat{Q}_i with $((\mathbb{Z}/\pi_i)^s)^{\mathbb{Z}^d}$ and to assume that $\alpha_{\mathbf{n}}^{Q_i} = T_{\mathbf{n}}$ for all \mathbf{n} , where $T_{\mathbf{n}}$ now denotes the shift (3.16) on $((\mathbb{Z}/\pi_i)^s)^{\mathbb{Z}^d}$. The surjective homomorphism $\eta_i: \hat{Q}_i \rightarrow \hat{L}_i$ dual to $\iota_i: L_i \rightarrow Q_i$ satisfies that $\eta \alpha_{\mathbf{n}}^{Q_i} = \alpha_{\mathbf{n}}^{L_i} \eta$ for every $\mathbf{n} \in \mathbb{Z}^d$. Since the \mathbb{Z}^d -action $\mathbf{n} \rightarrow \alpha_{\mathbf{n}}^{Q_1} \oplus \dots \oplus \alpha_{\mathbf{n}}^{Q_m}$ on $\hat{Q}_1 \oplus \dots \oplus \hat{Q}_m$ is (isomorphic to) a cartesian product of full d -dimensional shifts it is r -mixing for every $r \geq 1$, and we conclude that the factor action $\mathbf{n} \rightarrow \alpha_{\mathbf{n}}^{L_1} \oplus \dots \oplus \alpha_{\mathbf{n}}^{L_m}$ of \mathbb{Z}^d on the group $\hat{L}_1 \oplus \dots \oplus \hat{L}_m$ is also mixing of every order. Note that $\hat{L}_1 \oplus \dots \oplus \hat{L}_m = Y_{j+1}/Y_j$, and that the \mathbb{Z}^d -action $\mathbf{n} \rightarrow \alpha_{\mathbf{n}}^{L_1} \oplus \dots \oplus \alpha_{\mathbf{n}}^{L_m}$ is equal to the action on Y_{j+1}/Y_j induced by $\mathbf{n} \rightarrow \delta_{\mathbf{n}}$. The characters χ_0, \dots, χ_r are trivial on Y_j by assumption, and we may regard their restrictions to Y_{j+1} as characters of Y_{j+1}/Y_j . However, since $\mathbf{n} \rightarrow \alpha_{\mathbf{n}}^{L_1} \oplus \dots \oplus \alpha_{\mathbf{n}}^{L_m}$ is r -mixing, lemma 3.5 implies that these restrictions must be trivial, i.e. that $\chi_i \equiv 1$ on Y_{j+1} for every $i \in \{0, \dots, r\}$. As we have pointed out earlier, this completes the proof of the lemma. \square

Proof of Theorem 3.3. Assertion (1) follows from Lemma 3.6. If X is zero dimensional, then (i) \Rightarrow (iii) by Lemma 3.7, and Lemma 3.8 shows that (iii) \Rightarrow (ii). The implication (ii) \Rightarrow (i) is obvious. Theorem 3.3 is proved. \square

Proof of Corollary 3.4. Let X^0 be the connected component of the identity in X . If a shape $S = \{\mathbf{n}_0, \dots, \mathbf{n}_r\} \subset \mathbb{Z}^d$ is not mixing under α , choose characters χ_0, \dots, χ_r of X such that at least one χ_i is nontrivial, but $(\chi_0 \cdot \alpha_{k\mathbf{n}_0}) \cdot \dots \cdot (\chi_r \cdot \alpha_{k\mathbf{n}_r}) = 1$ for infinitely many $k \geq 1$ (cf. Lemma 3.5). From [S2, Corollary 3.6] we know that the restriction of α to the closed, α -invariant subgroup X^0 of X is still mixing, and Lemma 3.5 implies that the restrictions of the characters χ_i to X^0 must all be trivial. Hence the characters χ_0, \dots, χ_r can be regarded as elements of \hat{Y} , where $Y = X/X^0$. The set of associated prime ideals of the R_d -module $N = \hat{Y} \subset M$ (cf. Proposition 3.2) is given by $\{p_i: 1 \leq i \leq m \text{ and } p_i \cap \mathbb{Z} \neq \emptyset\}$, and lemma 3.8 implies that there exist an $i \in \{1, \dots, m\}$ and a rational prime π_i such that $p_i \supsetneq \pi_i R_d$. This shows that (2) \Rightarrow (1).

If every shape $S \subset \mathbb{Z}^d$ is mixing, then every shape is also mixing for the quotient action induced by α on the zero dimensional group $Y = X/X^0$, and Lemma 3.7 implies that every prime ideal associated with the module $N = \hat{Y} \subset M$ is of the form $p_i = \pi_i R_d$ for some rational prime π_i . This proves that (1) \Rightarrow (2). \square

3.9. Problem. Let X be a compact, connected abelian group and let $\alpha: \mathbf{n} \rightarrow \alpha_{\mathbf{n}}$ be a mixing \mathbb{Z}^d -action on X by automorphisms. Is α r -mixing for every $r \geq 1$?

REFERENCES

- [AM] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.
- [Dy] H. A. Dye, *On the ergodic mixing theorem*, Trans. Amer. Math. Soc., **118** (1965), 123–130.
- [KS] B. Kitchens and K. Schmidt, *Automorphisms of compact groups*, Ergodic Theory Dynamical Systems (to appear).
- [L] P.-F. Lam, *On expansive transformation groups*, Trans. Amer. Math. Soc., **150** (1970), 131–138.
- [La] S. Lang, *Algebra*, Addison-Wesley, 1984 (2nd edition).
- [Le] F. Ledrappier, *Un champ markovien peut être d'entropie nulle et mélangeant*, C. R. Acad. Sci. Paris, Ser. A., **287** (1978), 561–562.
- [Ma] K. Mahler, *Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen*, Proc. Acad. Sci. Amsterdam, **38** (1935), 50–60.

- [S1] K. Schmidt, *Asymptotic properties of unitary representations and mixing*, Proc. London Math. Soc., **48** (1984), 445–460.
- [S2] ———, *Automorphisms of compact abelian groups and affine varieties*, preprint.

Received April 15, 1988.

INSTITUTE FOR ADVANCED STUDY
PRINCETON, NJ 08540

AND

UNIVERSITY OF WARWICK
COVENTRY CV4 7AL, UK

