CHARACTERISTIC POLYNOMIAL PATTERNS IN DIFFERENCE SETS OF MATRICES

MICHAEL BJÖRKLUND AND ALEXANDER FISH

Abstract. We show that for every subset E of positive density in the set of integer square-matrices with zero traces, there exists an integer $k \geqslant 1$ such that the set of characteristic polynomials of matrices in $E - E$ contains the set of *all* characteristic polynomials of integer matrices with zero traces and entries divisible by k. Our theorem is derived from results by Benoist-Quint on measure rigidity for actions on homogeneous spaces.

1. Introduction

We recall the celebrated Furstenberg-Sarközy Theorem [6], [8]. Let $E_o \subset \mathbb{Z}$ be a set with

$$\overline{d}_{\mathbb{Z}}(E_o) = \overline{\lim_{n\to\infty}} \frac{|E_o \cap [1,n]|}{n} > 0,$$

and let $p \in \mathbb{Z}[X]$ be a polynomial with $p(0) = 0$. Then, there exists $n \geqslant 1$ such that

$$p(n) \in E_o - E_o = \{x - y \,:\, x, y \in E_o\}.$$

In other words, the difference set of any set of positive density in $\mathbb{Z}$ contains "polynomial patterns".

In this paper, we establish an analogue of Furstenberg-Sarközy Theorem for difference sets of matrices. Let $M_d(\mathbb{Z})$ denote the additive group of $d \times d$-integer matrices, and let $M_d^0(\mathbb{Z})$ denote the subgroup of $M_d(\mathbb{Z})$ consisting of matrices with zero trace. For a subset $E \subset M_d^0(\mathbb{Z})$, we define its *upper asymptotic density* by

$$\overline{d}(E) = \overline{\lim_{n\to\infty}} \frac{|E \cap F_n|}{|F_n|},$$

where $F_n = \big\{A = (a_{ij}) \in M_d^0(\mathbb{Z}) \,:\, |a_{ij}| \leqslant n, \quad \text{for all } (i,j) \neq (d,d)\big\}$.

The main result of this paper can be formulated as follows.

Theorem 1.1. *For every integer $d \geqslant 2$ and $E \subset M_d^0(\mathbb{Z})$ with $\overline{d}(E) > 0$, there exists an integer $k \geqslant 1$ such that for every $f \in \mathbb{Z}[X]$ of the form*

$$f(X) = X^d + k^2 \cdot a_{d-2}X^{d-2} + \ldots + k^d \cdot a_o, \quad \textit{where } a_o, \ldots, a_{d-2} \in \mathbb{Z}, \tag{1.1}$$

there exists a matrix $A \in E - E$ such that f is the characteristic polynomial of A.

By evaluating the characteristic polynomials for elements in $E - E$ at $X = 0$, we get the following corollary.

2010 *Mathematics Subject Classification.* Primary: 37A45; Secondary: 11P99, 11C99.
Key words and phrases. Ergodic Ramsey Theory, Measure rigidity.

Corollary 1.2. *For every integer* $d \geqslant 2$ *and* $E \subset M_d^0(\mathbb{Z})$ *with* $\overline{d}(E) > 0$*, the set*

$$D = \big\{ \det(A) \, : \, A \in E - E \big\} \subset \mathbb{Z}$$

contains a non-trivial subgroup.

Remark 1.3. We note that for every $k \geqslant 1$, the subgroup $E = k \cdot M_d^0(\mathbb{Z}) \subset M_d^0(\mathbb{Z})$ has positive density and all characteristic polynomials of elements $A \in E - E$ have the form (1.1). Hence, in this case, our theorem is sharp.

It is worth pointing out that there are sets $E \subset M_d(\mathbb{Z})$ with

$$\overline{d}(E) = \overline{\lim_{n \to \infty}} \frac{|E \cap G_n|}{|G_n|} > 0,$$

where $G_n = \big\{ A = (a_{ij}) \in M_d(\mathbb{Z}) \, : \, |a_{ij}| \leqslant n, \;\; \text{for all } (i,j) \big\}$, such that the set

$$T = \big\{ \operatorname{tr}(A - A') \, : \, A, A' \in E \big\} \subset \mathbb{Z}$$

does not contain a non-trivial subgroup. In other words, there exists a subset $E \subset M_d(\mathbb{Z})$ of positive density with the property that the set of characteristic polynomials of elements in the difference set $E - E$ does not contain the set

$$C_k = \big\{ f \in \mathbb{Z}[X] \, : \, f(X) = \det(X \cdot I - A), \;\; \text{for } A \in k \cdot M_d(\mathbb{Z}) \big\},$$

for any integer $k \geqslant 1$. Indeed, let $\alpha \in \mathbb{R}$ be an irrational number and denote by $I \subset \mathbb{R}/\mathbb{Z}$ an open interval such that the closure of $I - I \subset \mathbb{R}/\mathbb{Z}$ is a proper subset. Define

$$E_o = \big\{ n \in \mathbb{Z} \, : \, n\alpha \mod 1 \in I \big\} \subset \mathbb{Z}$$

and note that $E_o - E_o \subset \big\{ n \, : \, n\alpha \mod 1 \in I - I \big\} \subset \mathbb{Z}$ does not contain a non-trivial subgroup. The set

$$E = \big\{ A \in M_d(\mathbb{Z}) \, : \, \operatorname{tr}(A) \in E_o \big\} \subset M_d(\mathbb{Z})$$

satisfies $\overline{d}(E) > 0$, and $T = E_o - E_o$.

As another application of our main theorem, we prove a "sum-product" analogue of Bogolyubov's Theorem (see e.g. Theorem 7.2 in [7]).

Corollary 1.4. *For every* $E_o \subset \mathbb{Z}$ *with* $\overline{d}_{\mathbb{Z}}(E_o) > 0$*, the set*

$$D = \big\{ xy - z^2 \, : \, x, y, z \in E_o - E_o \big\} \subset \mathbb{Z}$$

contains a non-trivial subgroup of $\mathbb{Z}$*.*

Proof. Fix a set $E_o \subset \mathbb{Z}$ with $\overline{d}_{\mathbb{Z}}(E_o) > 0$ and define the set

$$E = \left\{ \begin{pmatrix} a & -b \\ c & -a \end{pmatrix} \, : \, a, b, c \in E_o \right\} \subset M_2^0(\mathbb{Z}).$$

One can readily check that $\overline{d}(E) > 0$, and thus, by Theorem 1.1, there exists an integer $k \geqslant 1$ such that for every $f \in \mathbb{Z}[X]$ of the form

$$f(X) = X^2 + k^2 \cdot a_0, \quad \text{where } a_o \in \mathbb{Z},$$

there exists an element $A \in E - E$ with $f(X) = \det(X \cdot I - A)$. In particular, given any integer a_o, we can find a matrix

$$A = \begin{pmatrix} z & -y \\ x & -z \end{pmatrix}$$

with $x, y, z \in E_o - E_o$, whose characteristic polynomial has the form $f(X) = X^2 + k^2 \cdot a_o$. Hence,

$$f(0) = \det(-A) = xy - z^2 = k^2 \cdot a_o,$$

which shows that $k^2 \cdot \mathbb{Z} \subset D$. □

We note that Theorem 1.1 is an immediate consequence of the following theorem.

Theorem 1.5. *For every integer* $d \geqslant 2$ *and* $E \subset M_d^0(\mathbb{Z})$ *with* $\overline{d}(E) > 0$*, there exists an integer* $k \geqslant 1$ *such that for every* $A \in k \cdot M_d^0(\mathbb{Z})$*, we have*

$$\overline{d}\big(E \cap (E - gAg^{-1})\big) > 0, \quad \textit{for some } g \in SL_d(\mathbb{Z}).$$

Proof of Theorem 1.1 using Theorem 1.5. Fix $d \geqslant 2$ and $a_o, \ldots, a_{d-2} \in \mathbb{Z}$ and pick an element $A_o \in M_d^0(\mathbb{Z})$ whose characteristic polynomial f_o has the form

$$f_o(X) = X^d + a_{d-2}X^{d-2} + \ldots + a_o.$$

Fix a set $E \subset M_d^0(\mathbb{Z})$ with $\overline{d}(E) > 0$ and use Theorem 1.5 to find an integer $k \geqslant 1$ such that, for every $A \in k \cdot M_d^0(\mathbb{Z})$, we have

$$E \cap (E - gAg^{-1}) \neq \emptyset, \quad \text{for some } g \in SL_d(\mathbb{Z}).$$

In particular, we can take $A = k \cdot A_o$, and we conclude that $k \cdot gA_o g^{-1} \in E - E$. Since the characteristic polynomial f of $k \cdot A_o$ (and $k \cdot gA_o g^{-1}$) equals

$$f(X) = X^d + k^2 \cdot a_{d-2}X^{d-2} + \ldots + k^d \cdot a_o,$$

and $a_o, \ldots, a_{d-2}$ are arbitrary integers, we are done. □

We now say a few words about the strategy of the proof of Theorem 1.5. The basic steps can be summarized as follows:

- In Section 2 we reduce the theorem to a problem concerning recurrence of $SL_d(\mathbb{Z})$-conjugation orbits in $M_d^0(\mathbb{Z})$.
- In Section 3 we show that this kind of recurrence can be linked to the behavior of random walks on $SL_d(\mathbb{Z})$ acting on the dual group of $M_d^0(\mathbb{Z})$.
- In Section 4 and Section 5 we use the work on measure rigidity by Benoist-Quint [1] to establish the necessary recurrence.

2. Proof of Theorem 1.5

Let $H_d = M_d^0(\mathbb{Z})$ and recall that the *dual* T_d of H_d is defined as the multiplicative group of all homomorphisms $\chi : H_d \to \mathbb{T}$, where $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$. We note that T_d is a compact metrizable abelian group and that we have a natural isomorphism $M_d^0(\mathbb{R})/M_d^0(\mathbb{Z}) \to T_d$ given by $\Theta \mapsto \chi_\Theta$, where

$$\chi_\Theta(A) = e^{2\pi i \operatorname{tr}(\Theta^t A)}, \quad \text{for } A \in H_d.$$

We denote by 1 the trivial character on T_d (the one corresponding to $\Theta = 0$), and we let $\mathcal{P}(T_d)$ denote the space of Borel probability measures on T_d.

Given $A \in H_d$, we define $\phi_A(\chi) = \chi(A)$ for $\chi \in T_d$, and given a Borel probability measure η on T_d, we define its *Fourier transform* $\widehat{\eta}$ by

$$\widehat{\eta}(A) = \int_{T_d} \phi_A(\chi)\, d\eta(\chi) = \int_{T_d} \chi(A)\, d\eta(\chi), \quad \text{for } A \in H_d.$$

The following proposition implies Theorem 1.5.

Proposition 2.1. *For every $d \geqslant 2$ and $\eta \in \mathcal{P}(T_d)$ with $\eta(\{1\}) > 0$, there exists $k \geqslant 1$ such that for every $A \in k \cdot M_d^0(\mathbb{Z})$, we have*

$$\widehat{\eta}(gAg^{-1}) \neq 0, \quad \textit{for some } g \in SL_d(\mathbb{Z}).$$

Proof of Theorem 1.5 using Proposition 2.1. By the proof of Furstenberg's Correspondence Principle (see Section 1, [5]) for the countable *abelian* group $H_d = M_d^0(\mathbb{Z})$, we can find a compact metrizable space Z, equipped with an action of H_d on Z by homeomorphisms, denoted by $(A, z) \mapsto A \cdot z$, a H-invariant (not necessarily ergodic) Borel probability measure ν on Z and a Borel set $B \subset Z$ with $\nu(B) > 0$ such that

$$\overline{d}\big(E \cap (E - A)\big) \geqslant \nu(B \cap A \cdot B), \quad \text{for all } A \in H_d.$$

We note that $A \mapsto \nu(B \cap A \cdot B)$ is a positive definite function on H_d, and thus, by Bochner's Theorem (Theorem 4.18 in [3]), we can find a probability measure η on the dual group $T_d = \widehat{H}_d$, such that

$$\frac{\nu(B \cap A \cdot B)}{\nu(B)} = \widehat{\eta}(A) = \int_{T_d} \chi(A)\, d\eta(\chi), \quad \text{for all } A \in H_d.$$

Furthermore, by the weak Ergodic Theorem, using the fact that $\nu(B) > 0$, we have $\eta(\{1\}) > 0$. By Proposition 2.1, we can find an integer $k \geqslant 1$ such that for every $A \in k \cdot H_d$, we have

$$\widehat{\eta}(gAg^{-1}) \neq 0, \quad \text{for some } g \in SL_d(\mathbb{Z})$$

and thus, $\nu(B \cap (gAg^{-1}) \cdot B) > 0$, and

$$\overline{d}\big(E \cap (E - gAg^{-1})\big) \geqslant \nu(B \cap (gAg^{-1}) \cdot B) > 0,$$

for some $g \in SL_d(\mathbb{Z})$, which finishes the proof. □

3. Stationary measures and the proof of Proposition 2.1

The main point of this section is to show that it suffices to establish Proposition 2.1 for a more restrictive class of Borel probability measures on $\mathbb{T}_d$.

Let μ be a probability measure on $SL_d(\mathbb{Z})$. We say that μ is *generating* if its support generates $SL_d(\mathbb{Z})$ as a semigroup, and we say that μ is *finitely supported* if its support is finite. Given an integer $n \geqslant 1$, we define

$$\mu^{*n}(g) = \sum_{g_1 \cdots g_n = g} \mu(g_1)\mu(g_2)\cdots\mu(g_n), \quad \text{for } g \in SL_d(\mathbb{Z}),$$

where the sum is taken over all n-tuples $(g_1, \ldots, g_n)$ in $SL_d(\mathbb{Z})$ such that $g_1 \ldots g_n = g$. Recall that $T_d = \widehat{H}_d$, and $SL_d(\mathbb{Z})$ acts on T_d by

$$(g \cdot \chi)(A) = \chi(g^{-1}Ag), \quad \text{for } A \in SL_d(\mathbb{Z}) \text{ and } \chi \in T_d.$$

We note that this induces a weak*-homeomorphic action of $SL_d(\mathbb{Z})$ on the space $\mathcal{P}(T_d)$ of Borel probability measures on T_d (which we shall here think of as elements in the dual of the space $C(T_d)$ of continuous functions on T_d) by

$$\int_{T_d} \phi(\chi)\, d(g \cdot \eta)(\chi) = \int_{T_d} \phi(g \cdot \chi)\, d\eta(\chi), \quad \text{for } \eta \in \mathcal{P}(T_d) \text{ and } \phi \in C(T_d).$$

Furthermore, we define the Borel probability measure $\mu * \eta$ on T_d by

$$\int_{T_d} \phi(\chi)\, d(\mu * \eta)(\chi) = \sum_{g \in SL_d(\mathbb{Z})} \Big(\int_{T_d} \phi(g \cdot \chi)\, d\eta(\chi) \Big) \cdot \mu(g), \quad \text{for } \phi \in C(T_d).$$

In particular, given $A \in M_d^0(\mathbb{Z})$, we let ϕ_A denote the character on T_d given by $\phi_A(\chi) = \chi(A)$ for $\chi \in T_d$, and we note that

$$\begin{aligned} \widehat{\mu * \eta}(A) &= \int_{T_d} \phi_A(\chi)\, d(\mu * \eta)(\chi) = \sum_{g \in SL_d(\mathbb{Z})} \int_{T_d} \chi(g^{-1}Ag)\, d\eta(\chi)\, d\mu(g) \\ &= \sum_{g \in SL_d(\mathbb{Z})} \widehat{\eta}(g^{-1}Ag) \cdot \mu(g), \quad \text{for all } A \in M_d^0(\mathbb{Z}). \end{aligned}$$

We say that a Borel probability measure ξ on T_d is μ-*stationary* if $\mu * \xi = \xi$. It is not hard to prove (see e.g. Proposition 3.3, [2]) that the set $\mathcal{P}_\mu(T_d)$ of μ-stationary Borel probability measures on T_d is never empty, and the measure class of any element $\xi \in \mathcal{P}_\mu(T_d)$ is invariant under the semi-group generated by the support of μ. If μ is a generating measure on $SL_d(\mathbb{Z})$, we say that an element $\xi \in \mathcal{P}_\mu(T_d)$ is *ergodic* if a $SL_d(\mathbb{Z})$-invariant Borel set in T_d is either ξ-null or ξ-conull.

The following proposition implies Proposition 2.1.

Proposition 3.1. *There exists a finitely supported probability measure μ on $SL_d(\mathbb{Z})$ whose support generates $SL_d(\mathbb{Z})$ with the property that for every $\xi \in \mathcal{P}_\mu(T_d)$ with $\xi(\{1\}) > 0$, there exists an integer $k \geqslant 1$ such that for every $A \in k \cdot M_d^0(\mathbb{Z})$, we have*

$$\widehat{\xi}(g^{-1}Ag) \neq 0, \quad \textit{for some } g \in SL_d(\mathbb{Z}).$$

Proof of Proposition 2.1 using Proposition 3.1. Pick $\eta \in \mathcal{P}(T_d)$ with $\eta(\{1\}) > 0$, and write

$$\eta = \lambda \cdot \delta_1 + (1 - \lambda) \cdot \eta_o, \quad \text{for some } 0 < \lambda \leqslant 1,$$

where $\eta_o(\{1\}) = 0$. Since 1 is fixed by the $SL_d(\mathbb{Z})$-action, we have

$$\mu^{*n} * \eta = \lambda \cdot \delta_1 + (1 - \lambda) \cdot \mu^{*n} * \eta_o, \quad \text{for every } n \geqslant 1,$$

and thus

$$\eta_N = \frac{1}{N} \sum_{n=1}^{N} \mu^{*n} * \eta = \lambda \cdot \delta_1 + (1 - \lambda) \cdot \frac{1}{N} \sum_{n=1}^{N} \mu^{*n} * \eta_o, \quad \text{for every } N \geqslant 1.$$

Since $\mathcal{P}(T_d)$ is weak*-compact, we can find a subsequence (N_j) such that η_{N_j} converges to a probability measure ξ on T_d in the weak*-topology, which must be μ-stationary and satisfy the bound $\xi(\{1\}) \geqslant \lambda > 0$. By Proposition 3.1, there exists an integer $k \geqslant 1$ such that for every $A \in k \cdot H_d$, we have

$$\widehat{\xi}(g^{-1}Ag) \neq 0, \quad \text{for some } g \in SL_d(\mathbb{Z}).$$

We now claim that for every $A \in k \cdot H_d$, we have

$$\widehat{\eta}(g^{-1}Ag) \neq 0, \quad \text{for some } g \in SL_d(\mathbb{Z}).$$

Indeed, suppose that this is not the case, so that $\widehat{\eta}(g^{-1}Ag) = 0$ for all $g \in SL_d(\mathbb{Z})$, and thus

$$\widehat{\eta}_N(h^{-1}Ah) = \frac{1}{N}\sum_{n=1}^{N}\sum_{g \in SL_d(\mathbb{Z})} \widehat{\eta}(g^{-1}h^{-1}Ahg) \cdot \mu^{*n}(g) = 0,$$

for all $N \geqslant 1$ and $h \in SL_d(\mathbb{Z})$. Since $\eta_{N_j} \to \xi$ in the weak*-topology, we conclude that we must have $\widehat{\xi}(h^{-1}Ah) = 0$ for all $h \in SL_d(\mathbb{Z})$, which is a contradiction. $\square$

4. Measure rigidity and the proof of Proposition 3.1

Definition 4.1. Let X be a compact *abelian* group and $\Gamma < \mathrm{Aut}(X)$. Let μ be a generating probability measure on Γ. We say that the action of Γ on X is μ-*nice* if the following conditions are satisfied:

- Every ergodic and μ-stationary Borel probability measure on X is either the Haar measure m_X or supported on a finite Γ-orbit in X.
- There are only countably many finite Γ-orbits in X, and each element in a finite Γ-orbit has finite order.

In particular, by the ergodic decomposition for μ-stationary Borel probability measures, see e.g. Proposition 3.13, [2], if the Γ-action is μ-nice, then every μ-stationary (not necessarily ergodic) Borel probability measure ξ on X can be written as

$$\xi = r \cdot m_X + (1-r) \cdot \sum_P q_P \cdot \nu_P, \quad \text{for some } 0 \leqslant r \leqslant 1,$$

where ν_P denotes the counting probability measure on a finite Γ-orbit $P \subset X$, and q_P are non-negative real numbers such that $\sum_P q_P = 1$.

In order to prove Proposition 3.1, we shall need the following "measure rigidity" result, which will be proved in Section 5 using results by Benoist-Quint [1].

Proposition 4.1. *For every finitely supported generating probability measure* μ *on* $SL_d(\mathbb{Z})$*, the dual action* $SL_d(\mathbb{Z}) \curvearrowright T_d$ *is* μ*-nice.*

Proof of Proposition 3.1 using Proposition 4.1. Fix $\xi \in \mathcal{P}_\mu(T_d)$ with $\xi(\{1\}) = q > 0$ and a finitely supported generating probability measure μ on $SL_d(\mathbb{Z})$. Since the dual action of $SL_d(\mathbb{Z})$ on T_d is μ-nice by Proposition 4.1, we can write ξ as

$$\xi = q \cdot \delta_1 + r \cdot m_X + (1-r-q) \cdot \sum_{P \neq \{1\}} q_P \cdot \nu_P,$$

for some $r \geqslant 0$ with $0 < r + q \leqslant 1$, where ν_P and q_P are as in Definition 4.1, and thus

$$\widehat{\xi} = q + r \cdot \delta_0 + (1-r-q) \cdot \sum_{P \neq \{1\}} q_P \cdot \widehat{\nu}_P.$$

If $q + r = 1$, then $\widehat{\xi}(A) \geqslant q > 0$ for every $A \in H_d$, so we may assume from now on that the inequalities $0 < r + q < 1$ hold. Since (q_P) is summable, we can find a finite subset F of the set of finite $SL_d(\mathbb{Z})$-orbits in T_d such that

$$\sum_{P \notin F} q_P < \frac{q}{1 - r - q}.$$

Since the action is μ-nice, we note that, for each finite $SL_d(\mathbb{Z})$-orbit P, every element in P has finite order, and thus we can find an integer n_P such that $\chi^{n_P} = 1$ for all $\chi \in P$. Since F is finite, we can further find an integer k such that $\chi^k = 1$ for every $\chi \in P$ and for every $P \in F$. Hence, $\chi(k \cdot A) = 1$ for all $A \in H_d$ and for every $\chi \in P$ and for every $P \in F$, and thus

$$\widehat{\nu}_P(k \cdot A) = \frac{1}{P} \sum_{\chi \in P} \chi(k \cdot A) = 1, \quad \text{for all } A \in H_d.$$

We conclude that

$$\widehat{\xi}(k \cdot A) = q + (1 - r - q) \cdot \sum_{P \in F} q_P + (1 - r - q) \cdot \sum_{P \notin F} q_P \cdot \widehat{\nu_P}(k \cdot A),$$

for every non-zero $A \in H_d$, and thus

$$\left|\widehat{\xi}(k \cdot A)\right| \geqslant q - (1 - r - q) \cdot \sum_{P \notin F} q_P > 0,$$

since $|\widehat{\nu}_P(A)| \leqslant 1$ for every $A \in H_d$, which finishes the proof. □

5. Proof of Proposition 4.1

Let us briefly recall the setting so far. We have

$$H_d = M_d^0(\mathbb{Z}) \quad \text{and} \quad T_d = \widehat{H}_d \cong M_d^0(\mathbb{R})/M_d^0(\mathbb{Z})$$

and a polynomial homomorphism $\mathrm{Ad} : SL_d(\mathbb{R}) \to GL(M_d^0(\mathbb{R}))$ defined by

$$\mathrm{Ad}(g)A = (g^t)^{-1} A g^t, \quad \text{for } g \in SL_d(\mathbb{R}) \text{ and } A \in M_d^0(\mathbb{R}),$$

where g^t denotes the transpose of g.

We note that $\mathrm{Ad}(g)M_d^0(\mathbb{Z}) = M_d^0(\mathbb{Z})$ for all $g \in SL_d(\mathbb{Z})$ and thus we can define a homeomorphic action of the group $SL_d(\mathbb{Z})$ on $M_d^0(\mathbb{R})/M_d^0(\mathbb{Z})$ by

$$g \cdot (A + M_d^0(\mathbb{Z})) = \mathrm{Ad}(g)A + M_d^0(\mathbb{Z}), \quad \text{for } A + M_d^0(\mathbb{Z}) \in M_d^0(\mathbb{R})/M_d^0(\mathbb{Z}).$$

We note that this action of $SL_d(\mathbb{Z})$ is isomorphic to the one on T_d via the map $\Theta \mapsto \chi_\Theta$ introduced in Section 3.

We wish to prove that for every finitely supported generating probability measure μ on the group $\mathrm{Ad}(SL_d(\mathbb{Z})) < \mathrm{Aut}(T_d)$, the action on T_d is μ-nice.

This is a special case of the following more general setting. Let V be a real finite-dimensional vector space and suppose that $\rho : SL_d(\mathbb{R}) \to GL(V)$ is a polynomial homomorphism defined over $\mathbb{Q}$ and set $\Gamma = \rho(SL_d(\mathbb{Z}))$. Let $\Lambda < V$ be a subgroup which is isomorphic to $\mathbb{Z}^n$, where $n = \dim_{\mathbb{R}}(V)$, so that the quotient group $X = V/\Lambda$ is compact. In the setting described above, we have

$$V = M_d^0(\mathbb{R}) \quad \text{and} \quad \Lambda = M_d^0(\mathbb{Z}) \quad \text{and} \quad \rho = \mathrm{Ad} \quad \text{and} \quad n = d^2 - 1.$$

Recall that the action of a subgroup $G < GL(V)$ is *irreducible* if it does not admit any non-trivial proper G-invariant subspaces, and we say that it is *strongly irreducible* if the action of any finite-index subgroup of G is irreducible. The following theorem of Benoist-Quint (Theorem 1.3, [1]) will be the main technical ingredient in the proof of Proposition 4.1.

Theorem 5.1. *Let μ be a finitely supported generating probability measure on Γ and suppose that $\Gamma \curvearrowright V$ is strongly irreducible. Then a μ-stationary ergodic probability measure on X is either the Haar measure on X or the counting probability measure on some finite Γ-orbit in X.*

Given a subset $Y \subset GL(V)$, we denote by $\overline{Y}^Z$ the Zariski closure of Y. The following proposition provides a condition which ensures that Γ acts strongly irreducibly on V.

Proposition 5.2. *Suppose that $\overline{\Gamma}^Z = G < GL(V)$ is a Zariski-connected group which acts irreducibly on V. Then, Γ acts strongly irreducibly on V, and for every finite-index subgroup $\Gamma_o < \Gamma$, any non-trivial Γ_o-invariant subgroup of Λ has finite index.*

Furthermore, there are countably many finite Γ-orbits in X, and for every finite Γ-orbit $P \subset X$ there exists an integer n such that $\chi^n = 1$ for all $\chi \in P$.

Proof. Suppose that Γ_o is a finite-index subgroup of Γ and let $U < V$ be a non-trivial Γ_o-invariant subspace. Since G is connected it must also be equal to the Zariski closure of Γ_o, and thus U is also fixed by G (since ρ is a polynomial map and being invariant subspace is an algebraic condition). Hence, $U = V$. This shows that Γ acts strongly irreducibly.

Now suppose that $\Lambda_o < \Lambda$ is a non-trivial Γ_o-invariant subgroup. Since Λ is assumed to be isomorphic to $\mathbb{Z}^n$ for some n, and every subgroup of a free abelian group is free, we can find a $\mathbb{Z}$-basis $e_1, \dots, e_m$ of Λ_o, and one readily checks that the real subspace

$$U := \mathbb{R}e_1 \oplus \dots \oplus \mathbb{R}e_m < V$$

is Γ_o-invariant as well. Since the Γ-action on V is assumed to be strongly irreducible, we can conclude that $U = V$, and thus $m = n$. From this it follows that the subgroup Λ_o has finite index in $\Lambda \cong \mathbb{Z}^n$.

Now suppose that $P \subset X$ is a finite Γ-orbit, and pick $\chi_o \in P$. We note that there exists a finite-index subgroup Γ_o of Γ which fixes χ_o, and thus the kernel $\Lambda_o = \ker \chi_o$ is a non-trivial Γ_o-invariant subgroup of Λ. Hence, from the previous paragraph, it must have finite index in Λ, and thus χ_o has finite order in X. Since there are only countably many finite-index subgroups of $\Lambda \cong \mathbb{Z}^n$, we conclude that there are only countably many choices of elements χ_o in X which belong to a finite Γ-orbit, and thus there are at most countably many finite Γ-orbits in X. ☐

Corollary 5.3. *Let μ be a finitely supported generating probability measure on Γ and suppose that $\Gamma \curvearrowright V$ is strongly irreducible. Then the Γ-action on X is μ-nice.*

Proof. By Theorem 5.1, a μ-stationary and *ergodic* Borel probability measure on X is either the Haar measure m_X on X or the counting probability measure on a finite Γ-orbit. By Proposition 5.2, there are (at most) countably many finite Γ-orbits in X, and each element in a finite Γ-orbit has finite order. ☐

The following corollary, in combination with Corollary 5.3, proves Proposition 4.1.

Corollary 5.4. *The action of* $\mathrm{Ad}(\mathrm{SL}_d(\mathbb{Z}))$ *on* $M_d^0(\mathbb{R})$ *is strongly irreducible.*

Proof. Let Γ_o be a finite-index subgroup of $\Gamma = \mathrm{Ad}(\mathrm{SL}_d(\mathbb{Z}))$ and let $V = M_d^0(\mathbb{R})$. We note that in this case, the Zariski closure $G := \overline{\Gamma_o}^{\mathbb{Z}}$ equals $\mathrm{PSL}_d(\mathbb{R})$ by the Borel Density Theorem [4], which is Zariski-connected (since it is algebraically simple) and it acts irreducibly on V. Indeed, any linear subspace of $M_d^0(\mathbb{R}) \cong \mathfrak{sl}_d(\mathbb{R})$, which is invariant under the adjoint representation, is an ideal in $\mathfrak{sl}_d(\mathbb{R})$. Since $\mathfrak{sl}_d(\mathbb{R})$ is simple as a Lie algebra, we see that the adjoint action is irreducible. By Proposition 5.2, this shows that Γ acts strongly irreducibly. $\square$

6. Acknowledgements

The authors are grateful to Yvés Benoist for enlightening and very encouraging discussions. The second author would also like to thank the Department of Mathematical Sciences at Chalmers University, Gothenburg, for their hospitality during the time this paper was written.

References

1. Benoist, Y.; Quint, J.-F. *Mesures stationnaires et fermés invariants des espaces homogénes.* (French) [Stationary measures and invariant subsets of homogeneous spaces] Ann. of Math. (2) 174 (2011), no. 2, 1111–1162.
2. Björklund, M.; Fish, A. *Product set phenomena for countable groups.* Adv. Math. 275 (2015), 47–113.
3. Folland, G. *A course in abstract harmonic analysis.* Studies in Advanced Mathematics. CRC Press, Boca Raton, FL, 1995. x+276 pp.
4. Furstenberg, H. *A note on Borel's density theorem.* Proc. Amer. Math. Soc. 55 (1976), no. 1, 209–212.
5. Furstenberg, H. *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions.* J. Analyse Math. 31 (1977), 204–256.
6. Furstenberg, H. *Recurrence in ergodic theory and combinatorial number theory.* M. B. Porter Lectures. Princeton University Press, Princeton, N.J., 1981. xi+203 pp.
7. Ruzsa, I. *Sumsets and structure.* Combinatorial number theory and additive group theory, 87–210, Adv. Courses Math. CRM Barcelona, Birkhäuser Verlag, Basel, 2009.
8. Sárközy, A. *On difference sets of sequences of integers. III.* Acta Math. Acad. Sci. Hungar. 31 (1978), no. 3–4, 355–386.

Department of Mathematics, Chalmers, Gothenburg, Sweden
E-mail address: micbjo@chalmers.se

School of Mathematics and Statistics, University of Sydney, Australia
E-mail address: alexander.fish@sydney.edu.au