From Hyperbolic Geometry to Expander Graphs

Rabib Islam
Department of Mathematics & Statistics
University of Ottawa

April 2015

Preface

This report was written and compiled during the Winter 2015 term under the supervision of Professor Hadi Salmasian. The corresponding research was funded by the NSERC USRA programme and the NSERC grant of Professor Salmasian. This project was also completed as part of a work term for the Co-operative Education Program at the University of Ottawa. This document is intended for a junior to senior undergraduate audience interested in research-level mathematics, and in particular representation theory in relation to expander graphs

Acknowledgements

The author would like to thank Professor Salmasian for his guidance during the research term, and for his editorial efforts with respect to this report.

Contents

1. Representations and Kazhdan's Property (T) **5**
1.1. Preliminaries on representations 5
1.2. Property (T) 6

2. $\mathrm{SL}_n(\mathbb{K})$ has Property (T) for $n \geq 3$ **7**
2.1. Preliminary facts 7
2.2. Proof of Property (T) 11

3. $\mathrm{SL}_3(\mathbb{Z})$ and expander graphs **13**

4. Property (τ) and $\mathrm{SL}_2(\mathbb{Z})$ **18**
4.1. Property (τ) 18
4.2. Graphs and manifolds 19

5. The Expansion Machine **22**

6. Examples of Property (τ) **28**

A. Topology and Analysis **32**

B. Algebraic Structures **35**

C. Differential Geometry **38**

Introduction

As per its namesake, representation theory is concerned primarily with a type of map called a representation, whose domain is an algebraic structure and whose codomain is a the set of linear transformations over a vector space; it additionally satisfies some defining properties. Representation theory has a deep history which spans roughly over a century, and it started with the work of Frobenius and Burnside. Since its beginnings, it has grown into a field of prolific research which has consequences in many different areas of mathematics, such as harmonic analysis, geometry, and algebra. It may also be argued that the approaches one can take with regards to representation theory are as numerous as its applications; indeed, one may use techniques from functional analysis, topology, and combinatorics, among other disciplines, to tackle a wide variety of problems.

In this article, we especially focus on the theory of representations on locally compact groups as it relates to the generation of expander graphs, which are a type of graph known for their usefulness in computer science and engineering. They have also been the source of many interesting and challenging problems for mathematicians. In fact, while their existence was proven in 1972 by Pinsker (according to [6, p. 23]), there was no known explicit construction until one was given by Margulis in [25] the following year. Ever since then, some mathematicians have become interested in finding new ways to construct expanders. Naturally, this has motivated more research into representation theory.

Aside from merely discussing this relationship however, we will enter into exploration concerning other interesting mathematics. We will demonstrate the role of hyperbolic geometry in devising a method to construct families of expander graphs; this will be discussed in tandem with related concepts from Riemannian geometry and modular forms.

The undergraduate reader is forewarned that he or she may be presented with a number of unfamiliar terms. The appendices are meant to serve as an aid in this respect, and explicit references to them will be made whenever particularly advanced definitions and theorems are required. A citation is provided after each item, indicating from where the entry was derived; this can be helpful for those who wish to learn more about a particular topic.

1. Representations and Kazhdan's Property (T)

Our first approach to generating expander graphs involves Kazhdan's Property (T), which is a property of certain locally compact groups that describes their irreducible representations. In this chapter, we carve a path of least resistance to defining Property (T).

1.1. Preliminaries on representations

The information in this section has been adapted from the first pages of [22]. We adopt his notational convention for this paper.

Definition 1.1. Let G be a locally compact group and let H be a Hilbert space. A **representation** of G in H is a homomorphism

$$\pi : G \to \mathrm{GL}(H)$$

of G into the group of continuous linear automorphisms of H, such that for each vector $v \in H$, the map of G into H given by

$$x \mapsto \pi(x)v$$

is continuous.

Definition 1.2. A representation π is called **bounded** if there exists a constant $C > 0$ such that $\|\pi(x)\| \leq C$ for all $x \in G$. If $\pi(x)$ is unitary, then π is called **unitary**.

Definition 1.3. Let $\pi : G \to \mathrm{GL}(H)$ be a representation, and let W be a subspace of H. W is called ***G*-invariant** or simply **invariant** if $\pi(x)W \subset W$ for all $x \in G$. π is called **irreducible** if H has no invariant subspace other than $\{0\}$ and H itself.

The next proposition is for the sake of the reader's intuition, and serves to illustrate sufficient conditions for a map to be a representation.

Proposition 1.4. *Let $\pi : G \to \mathrm{GL}(H)$ be a homomorphism and assume that for a dense set of $v \in H$ the map $x \mapsto \pi(x)$ is continuous. Assume that the image of some neighborhood of the unit element $e \in G$ under π is bounded in* $\mathrm{GL}(H)$. *Under these conditions, π is a representation.*

Proof. Let $v \in H$ and select v_1 close to v such that $x \mapsto \pi(x)v_1$ is continuous. By the triangle inequality,

$$|\pi(x)v - v| \leq |\pi(x)v - \pi(x)v_1| + |\pi(x)v_1 - v_1| + |v_1 - v|.$$

□

1.2. Property (T)

In this section, we define Property (T) itself. Much of the information here is adapted from [1].

Definition 1.5. Let π be a unitary representation of G in H.

(1) For a subset Q of G and a real number $\epsilon > 0$, a vector $\xi \in H$ is **(Q, ϵ)-invariant** if

$$\sup_{x \in Q} \|\pi(x)\xi - \xi\| < \epsilon \|\xi\|.$$

(2) The representation π **almost has invariant vectors** if it has (Q, ϵ)-invariant vectors for every compact subset Q of G and every $\epsilon > 0$. If this holds, we write $1_G \prec \pi$. One also says that π weakly contains the trivial representation (see Definition 6.1 for an explanation of this terminology).

(3) The representation π has non-zero **invariant vectors** if there exists $\xi \neq 0$ in H such that $\pi(x)\xi = \xi$ for all $x \in G$. If this holds, we write $1_G \subset \pi$. One also says that π strongly contains the trivial representation (as a subrepresentation; see Definition 4.3 for details).

Definition 1.6. Let G be a topological group. A subset Q of G is a **Kazhdan set** if there exists $\epsilon > 0$ with the following property: every unitary representation π of G in H which has a (Q, ϵ)-invariant vector also has a non-zero invariant vector. In this case, $\epsilon > 0$ is called a **Kazhdan constant** for G and Q, and (Q, ϵ) is called a **Kazhdan pair** for G. The group G has **Kazhdan's Property (T)**, or is a **Kazhdan group**, if G has a compact Kazhdan set.

Let us try to break down this formal definition to recover some geometric intuition. Let G be a topological group with Kazhdan's Property (T) and a unitary representation π. If π almost has invariant vectors, then it has an invariant vector; what we get then is that the span of this invariant vector is fixed, so the representation is reducible. Thus, Property (T) is really saying that all the nontrivial irreducible representations of G are "pushing around" vectors by at least ϵ, the Kazhdan constant! This leads to an equivalent formulation of Property (T) which says that the nontrivial irreducible representations are "bounded away" from the trivial representation in a topology of representations, called the Fell topology. The eager reader can see what this is in Definition 4.2.

Definition 1.7. Let G be a topological group, and let S be a closed subgroup. The pair (G, S) has **Property (T)** if, whenever a unitary representation π of G in H almost has invariant vectors, it actually has a non-zero $\pi(S)$-invariant vector.

Remark 1.8. Let G be a topological group G. for a compact subset Q and a unitary representation (π, H) of G, we define the Kazhdan constant associated to Q and π as the following non-negative constant:

$$\kappa(G, Q, \pi) = \inf\{\max_{x \in Q} \|\pi(x)\xi - \xi\| : \xi \in H, \|\xi\| = 1\}.$$

It follows that $1_G \prec \pi$ if and only if for all Q's, $\kappa(G, Q, \pi) = 0$.

2. $\mathrm{SL}_n(\mathbb{K})$ has Property (T) for $n \geq 3$

Let $\mathbb{K}$ be a local field (see Definition B.7). In this chapter, it will be shown that $\mathrm{SL}_n(\mathbb{K})$ has Property (T) for $n \geq 3$. This will be instrumental in our first construction of expander graphs.

The theorems and definitions in this section come from [1].

2.1. Preliminary facts

The following lemma is used in Theorem 2.3, and its proof is nice to see for students with some experience in functional analysis.

Lemma 2.1. *Let G be a topological group, and let π be a unitary representation of G in H which almost has invariant vectors. Then there exists a linear functional ϕ on the algebra $\mathscr{L}(H)$ of bounded operators on H with the following properties:*

(1) $\phi(I) = 1$;

(2) ϕ is positive, that is, $\phi(T^*T) \geq 0$ for all $T \in \mathscr{L}(H)$;

(3) $\phi(\pi(x)T) = \phi(T\pi(x)) = \phi(T)$ for all $x \in G$ and $T \in \mathscr{L}(H)$.

Proof. Since π almost has invariant vectors, there is a net of unit vectors $(\xi_i)_{i\in I}$ such that

$$\lim_i \|\pi(x)\xi_i - \xi_i\| = 0, \tag{$*$}$$

for all $x \in G$. For each $T \in \mathscr{L}(H)$, let D_T be the closed disc in $\mathbb{C}$ of radius $\|T\|$, and consider the product space

$$X = \prod_{T\in\mathscr{L}(H)} D_T,$$

endowed with the product topology. By Theorem A.1, X is compact. Since $(\langle T\xi_i, \xi_i\rangle)_{T\in\mathscr{L}(H)}$ is an element of X for all $i \in I$, there exists a subnet $(\xi_j)_{j\in J}$ such that, for all $T \in \mathscr{L}(H)$, the limit

$$\phi(T) = \lim_j \langle T\xi_j, \xi_j\rangle$$

exists. It is clear that $T \mapsto \phi(T)$ is a positive linear functional on $\mathscr{L}(H)$ with $\phi(I) = 1$. Moreover, for every $x \in G$ and $T \in \mathscr{L}(H)$, we have

$$|\langle T\pi(x)\xi_j, \xi_j\rangle - \langle T\xi_j, \xi_j\rangle| = |\langle T(\pi(x))\xi_j - \xi_j), \xi_j| \leq \|T\|\|\pi(x)\xi_j - \xi_j\|$$

and

$$|\langle \pi(x)T\xi_j, \xi_j\rangle - \langle T\xi_j, \xi_j\rangle| = |\langle T\xi_j, \pi(x^{-1})\xi_j - \xi_j\rangle| \leq \|T\|\|\pi(x)\xi_j - \xi_j\|.$$

Hence, using (∗), we obtain

$$\phi(T\pi(x)) = \lim_j \langle T\pi(x)\xi_j, \xi_j\rangle = \lim_j \langle T\xi_j, \xi_j\rangle = \phi(T)$$

and, similarly, $\phi(\pi(x)T) = \phi(T)$. □

If X is a locally compact space, let $\mathcal{B}(X)$ be the σ-algebra of its Borel subsets. Let H be a Hilbert space. Denote by $\mathrm{Proj}(H)$ the set of orthogonal projections on $\mathcal{L}(H)$. For σ-algebra and Borel subsets, see Definition A.2 and Definition A.3.

The next theorem was proven by Stone for the case $G = \mathbb{R}$ and was independently generalized by Naimark, Ambrose, and Godement, and it is thus referred to as the "SNAG Theorem". It serves an important technical purpose in the subsequent theorem. One should note that the integral involved is with respect to a projection-valued measure (which is defined in Definition A.9). When we refer to the dual of a group, which is denoted $\hat{G}$ for a given group G, we mean strictly the Pontryagin dual, defined in Definition B.8.

Theorem 2.2 (SNAG Theorem). *(1) Let π be a representation of a locally compact abelian group G in H. There exists a unique regular projection-valued measure $E_\pi \colon \mathcal{B}(\hat{G}) \to \mathrm{Proj}(H)$ on $\hat{G}$ such that*

$$\pi(x) = \int_{\hat{G}} \overline{\hat{x}(x)} dE_\pi(\hat{x}), \quad \textit{for all} \quad x \in G.$$

Moreover, an operator T in $\mathcal{L}(H)$ commutes with $\pi(x)$ for all $x \in G$ if and only if it commutes with $E(B)$ for all $B \in \mathcal{B}(\hat{G})$.

(2) Conversely, if E is a regular projection-valued measure

$$E \colon \mathcal{B}(\hat{G}) \to \mathrm{Proj}(H)$$

on $\hat{G}$, then

$$\pi(x) = \int_{\hat{G}} \overline{\hat{x}(x)} dE(\hat{x}), \quad \textit{for all} \quad x \in G$$

defines a unitary representation π of G on H.

The following theorem demands an assumption which is proven to hold for a particular case in Proposition 2.10. For the definition of the Dirac measure, see Definition A.6, and for the definition of a mean, see Definition A.7.

Theorem 2.3. *Let G be a locally compact group and N an abelian closed normal subgroup. Assume that the Dirac measure at the unit character 1_N of N is the unique mean on the Borel subsets of $\hat{N}$ which is invariant under the action of G on $\hat{N}$ dual to the conjugation action. Then the pair (G, N) has Property (T).*

Proof. Let π be a unitary representation of G in H almost having invariant vectors. We have to prove that H contains a non-zero N-invariant vector. Let $\mathcal{B}(\hat{N})$ be the σ-algebra of the Borel subsets of $\hat{N}$, and let

$$\begin{aligned} E : \mathcal{B}(\hat{N}) &\to \mathcal{L}(H) \\ B &\mapsto E(B) \end{aligned}$$

be the projection-valued measure on $\hat{N}$ associated to the unitary representation $\pi|_N$ of the abelian group N. Thus, by Theorem 2.2,

$$\pi(x) = \int_{\hat{N}} \chi(x) dE(\chi), \quad x \in N.$$

For every $g \in G$, we have

$$\pi(g)\pi(x)\pi(g^{-1}) = \pi(gxg^{-1}) = \int_{\hat{N}} (g^{-1}\chi)(x) dE(\chi), \quad x \in N.$$

Hence,

$$B \mapsto E(gB) \quad \text{and} \quad B \mapsto \pi(g)E(B)\pi(g^{-1})$$

are projection valued measures associated to the unitary representation

$$x \mapsto \pi(gxg^{-1})$$

of N. By uniqueness, it follows that

$$\pi(g)E(B)\pi(g)^{-1} = E(gB), \quad \text{for all} \quad B \in \mathcal{B}(\hat{N}), g \in G. \tag{$*$}$$

By Lemma 2.1, there exists a positive linear functional ϕ on $\mathcal{L}(H)$ such that $\phi(I) = 1$, and such that $\phi(\pi(g)T) = \phi(T\pi(g)) = \phi(T)$ for all $g \in G$ and $T \in \mathcal{L}(H)$. In particular,

$$\phi(T) = \phi(\pi(g)T\pi(g^{-1})), \quad \text{for all} \quad g \in G, T \in \mathcal{L}(H).$$

Define $m \colon \mathcal{B}(\hat{N}) \mapsto \mathbb{R}$ by

$$m(B) = \phi(E(B)), \quad B \in \mathcal{B}(\hat{N}).$$

Then m is a mean on $\mathcal{B}(\hat{N})$. Moreover, m is G-invariant, by ($*$). Hence, m is the Dirac measure at the unit character 1_N of N. In particular, $E(\{1_N\}) \neq 0$. Let ξ be a non-zero vector in the range of the projection $E(\{1_N\})$. Then $\pi(x)\xi = \xi$ for all $x \in N$, that is, ξ is N-invariant. □

Let $\mathbb{K}$ be a field. Things concerning unitary representations of $\mathrm{SL}_2(\mathbb{K})$ are important when it comes to showing that $\mathrm{SL}_n(\mathbb{K})$ has Property (T) for $n \geq 3$. We consider the following subgroups of $\mathrm{SL}_2(\mathbb{K})$:

$$N = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{K} \right\}$$

$$N^- = \left\{ \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} : x \in \mathbb{K} \right\}$$

$$A = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} : \lambda \in^* \mathbb{K} \right\}$$

Note that $N \cup N^-$ generates $\mathrm{SL}_2(\mathbb{K})$. The following lemma is used later on.

Lemma 2.4. *For any field $\mathbb{K}$, the group $\mathrm{SL}_n(\mathbb{K})$ is generated by the set of all elementary matrices $E_{ij}(x)$ for $x \in \mathbb{K}$ and $1 \leq i, j \leq n, i \neq j$.*

This next series of lemmas is very important in helping us use properties of $\mathrm{SL}_2(\mathbb{K})$ as we move forward.

Lemma 2.5. *Let $\mathbb{K}$ be a non-discrete topological field. Let $(\lambda_i)_i$ be a net in $\mathbb{K}$ with $\lambda_i \neq 0$ and $\lim_i \lambda_i = 0$. Then, for $a_i = \left(\begin{smallmatrix} \lambda_i & 0 \\ 0 & \lambda_i^{-1} \end{smallmatrix}\right), h \in N$ and $h^- \in N^-$, we have*

$$\lim_i a_i h a_i^{-1} = \lim_i a_i^{-1} h^- a_i = I.$$

Lemma 2.6 (Mautner's Lemma). *Let G be a topological group, and let π be a unitary representation of G in H. Let $x \in G$ and assume that there exists a net $(y_i)_i$ in G such that $\lim_i y_i x y_i^{-1} = e$. If ξ is a vector in H which is fixed by y_i for all i, then ξ is fixed by x.*

Proof. Since ξ is fixed by the unitary operators $\pi(y_i)$, we have

$$\|\pi(x)\xi - \xi\| = \|\pi(x)\pi(y_i^{-1})\xi - \pi(y_i^{-1})\xi\| = \|\pi(y_i)\pi(x)\pi(y_i^{-1})\xi - \xi\|.$$

As $\lim_i y_i x y_i^{-1} = e$ and π is strongly continuous, $\pi(x)\xi = \xi$. □

The proof of the following has been omitted due to its length, but the lemma itself will help us show invariance of vectors under copies of $\mathrm{SL}_2(\mathbb{K})$, which will be useful in our final proof in this chapter.

Lemma 2.7. *Let $\mathbb{K}$ be a non-discrete topological field, and let π be a unitary representation of $\mathrm{SL}_2(\mathbb{K})$. Let ξ be a vector in H which is invariant under the subgroup N. Then ξ is invariant under $\mathrm{SL}_2(\mathbb{K})$.*

Definition 2.8. Let $n \geq 2$ and $m < n$. Choosing m distinct vectors $e_{i_1}, \ldots, e_{i_m}$ from the standard basis $\{e_1, \ldots, e_n\}$ of $\mathbb{K}^n$, we have an embedding of $\mathrm{SL}_{n-m}(\mathbb{K})$ in $\mathrm{SL}_n(\mathbb{K})$ as the subgroup of matrices in $\mathrm{SL}_n(\mathbb{K})$ which fix $e_{i_1}, \ldots, e_{i_m}$ and leave invariant the linear span of the remaining $n - m$ vectors e_i. We refer to these embeddings as to the **standard embeddings** of $\mathrm{SL}_{n-m}(\mathbb{K})$.

The following proposition will help us apply Lemma 2.7 to effect in the final proof.

Proposition 2.9. *Let $\mathbb{K}$ be a topological non-discrete field, and let $n \geq 2$. Let π be a unitary representation of $\mathrm{SL}_n(\mathbb{K})$ in H. If $\xi \in H$ is invariant under $\mathrm{SL}_2(\mathbb{K})$, for any one of the standard embeddings of $\mathrm{SL}_2(\mathbb{K})$, then ξ is invariant under $\mathrm{SL}_n(\mathbb{K})$.*

2.2. Proof of Property (T)

We now start to apply the knowledge we gained in the previous sections towards a proof that $\mathrm{SL}_n(\mathbb{K})$ has Property (T) for $n \geq 3$. We consider the subgroups

$$G = \left\{ \begin{pmatrix} A & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & I_{n-3} \end{pmatrix} : A \in \mathrm{SL}_2(\mathbb{K}), x \in \mathbb{K}^2 \right\} \cong \mathrm{SL}_2(\mathbb{K}) \ltimes \mathbb{K}^2$$

$$N = \left\{ \begin{pmatrix} I_2 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & I_{n-3} \end{pmatrix} : x \in \mathbb{K}^2 \right\} \cong \mathbb{K}^2$$

of $\mathrm{SL}_n(\mathbb{K})$, where $\mathrm{SL}_2(\mathbb{K}) \ltimes \mathbb{K}^2$ denotes the semidirect product for the natural action of $\mathrm{SL}_2(\mathbb{K})$ on $\mathbb{K}^2$ (see Definition B.3 for semidirect product).

The following proposition shows that the assumption made in the statement of Theorem 2.3 holds for the pair $(\mathrm{SL}_2(\mathbb{K}) \ltimes \mathbb{K}^2, \mathbb{K}^2)$.

Proposition 2.10. *Let $\mathbb{K}$ be a local field. The Dirac measure at 0 is the unique $\mathrm{SL}_2(\mathbb{K})$-invariant mean on the Borel subsets of $\mathbb{K}^2$.*

Proof. Let m be an $\mathrm{SL}_2(\mathbb{K})$-invariant mean on the σ-algebra $\mathscr{B}(\mathbb{K}^2)$ of the Borel sets of $\mathbb{K}^2$. Let $|\cdot|$ be an absolute value defining the topology on $\mathbb{K}$. Consider the following subset of $\mathbb{K}^2 \backslash \{0\}$:

$$\Omega = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{K}^2 \backslash \{0\} : |y| \geq |x| \right\}.$$

Choose a sequence $(\lambda)_n$ in $\mathbb{K}$ with $|\lambda_{n+1}| > |\lambda_n| + 2$ for all $n \in \mathbb{N}$, and set

$$g_n = \begin{pmatrix} 1 & \lambda_n \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{K}).$$

If $\Omega_n = g_n \Omega$, then

$$\Omega_n \subset \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{K}^2 \backslash \{0\} : \frac{|x|}{|\lambda_n| + 1} \leq |y| \leq \frac{|x|}{|\lambda_n| - 1} \right\}.$$

Indeed, for $\begin{pmatrix} x \\ y \end{pmatrix} \in \Omega$,

$$g_n \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + \lambda_n y \\ y \end{pmatrix}$$

and

$$|x + \lambda_n y| \geq |\lambda_n y| - |x| \geq (|\lambda_n| - 1)|y|,$$
$$|x + \lambda_n y| \leq |x| + |\lambda_n y| \leq (|\lambda_n| + 1)|y|.$$

Since

$$\frac{1}{|\lambda_n| - 1} < \frac{1}{|\lambda_m| + 1} \quad \text{for } n > m,$$

the sets Ω_n are pairwise disjoint. Hence,

$$\sum_{i=1}^{n} m(\Omega_i) \leq m(\mathbb{K}^2 \backslash \{0\}) \leq 1$$

for all $n \in \mathbb{N}$. As $m(\Omega_i) = m(g_i\Omega) = m(\Omega)$, it follows that $m(\Omega) = 0$. If

$$\Omega' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \Omega = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{K}^2 \backslash \{0\} : |x| \geq |y| \right\},$$

then $m(\Omega') = m(\Omega) = 0$. Since $\Omega \cup \Omega' = \mathbb{K}^2 \backslash \{0\}$, we have $m(\mathbb{K}^2 \backslash \{0\}) = 0$. Therefore, m is the Dirac measure at 0. □

Corollary 2.11. *The pair* $(\mathrm{SL}_2(\mathbb{K}) \ltimes \mathbb{K}^2, \mathbb{K}^2)$ *has Property (T), for every local field* $\mathbb{K}$.

Finally, we arrive at the proof that is the goal of this chapter.

Theorem 2.12. *Let* $\mathbb{K}$ *be a local field. The group* $\mathrm{SL}_n(\mathbb{K})$ *has Property (T) for* $n \geq 3$.

Proof. Let π be a unitary representation of $\mathrm{SL}_n(\mathbb{K})$ in H almost having invariant vectors. Let $G \cong \mathrm{SL}_2(\mathbb{K}) \ltimes \mathbb{K}^2$ and $N \cong \mathbb{K}^2$ be the subgroups of $\mathrm{SL}_n(\mathbb{K})$ introduced above. By the previous corollary, the pair (G, N) has Property (T). Hence, there exists a non=zero N-invariant vector $\xi \in H$. By Lemma 2.7, ξ is invariant under the following copy of $\mathrm{SL}_2(\mathbb{K})$

$$\begin{pmatrix} * & 0 & * & 0 \\ 0 & 1 & 0 & 0 \\ * & 0 & * & 0 \\ 0 & 0 & 0 & I_{n-3} \end{pmatrix}$$

inside $\mathrm{SL}_n(\mathbb{K})$. It follows from Proposition 2.9 that ξ is invariant under the whole group $\mathrm{SL}_n(\mathbb{K})$. □

3. $\mathrm{SL}_3(\mathbb{Z})$ and expander graphs

Using the fact that $\mathrm{SL}_3(\mathbb{K})$ has Property (T), we display the first construction of a family of expander graphs we will see in this paper. This example is again borrowed from the book of Bekka et al. [1]. We begin by noting that $\mathrm{SL}_3(\mathbb{Z})$ has Property (T): this is because it embeds as a lattice in $\mathrm{SL}_3(\mathbb{R})$ (see Definition B.6 of lattice) and the following theorem. See Definition A.10 for the definition of a (regular) Borel measure.

Theorem 3.1. *Let G be a locally compact group, and let H be a closed subgroup of G such that G/H has a finite invariant regular Borel measure. The following are equivalent:*

(1) G has Property (T);

(2) H has Property (T).

In particular, if Γ is a lattice in G, then Γ has Property (T) if and only if G has Property (T).

The proof for this is very long and technical so we skip it.

Since $\mathrm{SL}_3(\mathbb{Z})$ has Property (T), we know that it has a Kazhdan constant. As we will see in this section, the Kazhdan constant of a group is closely related to the expansion constant of a particular family of Schreier graphs. The following definitions explain these terms.

Definition 3.2. The **expansion constant** or **isoperimetric constant** of a graph $\mathcal{G}$ with vertex set V is the positive real number

$$h(\mathcal{G}) = \min\Big\{\frac{|\partial A|}{\min\{|A|, |V \setminus A|\}} : A \subsetneq V, 0 < |A| < \infty\Big\}.$$

Definition 3.3. Let Γ be a finitely generated group, and let S be a finite generating set of Γ with $S^{-1} = S$. Let Γ act on a set V. Define the **Schreier graph** $\mathcal{S}(V, S)$ as follows:

- the set of vertices is V,
- $(x, y) \in V \times V$ is an edge if and only if $y = sx$ for some $s \in S$.

The expansion constant is particularly useful in specifying a condition for expander graphs which we informally introduced in the Introduction. A formal definition follows from Kowalski's book [20].

Definition 3.4. A family $(\mathcal{G}_i)_{i \in I}$ of finite non-empty connected graphs $\mathcal{G}_i = (V_i, E_i, ep)$ is an **expander family** or **family of expanders** if there exist constants $v \geq 1$ and $h \geq 1$ independent of i such that

(1) For any $N \geq 1$, there are only finitely many $i \in I$ such that $\mathcal{G}_i$ has at most N vertices;

(2) For each $i \in I$, we have
$$\max_{x \in V_i} val(x) \leq v;$$

(3) For each $i \in I$, the expansion ratio satisfies
$$h(\mathcal{G}_i) \geq h.$$

One may however wish to speak of a single expander graph, in which case this definition offered by Breuillard in [6] suffices.

Definition 3.5. A finite k-regular graph $\mathcal{G}$ is said to be an ϵ-expander if for every subset A of vertices in $\mathcal{G}$, with $|A| \leq \frac{1}{2}|\mathcal{G}|$, one has the following isoperimetric inequality:

$$|\partial A| \geq \epsilon |A|,$$

where ∂A denotes the set of edges of $\mathcal{G}$ which connect a point in A to a point in its complement.

We now make our way towards the construction of a family of expanders using the fact that $\mathrm{SL}_3(\mathbb{Z})$ has Property (T). First, some technical definitions are necessary.

Definition 3.6. Let Δ be the modular function of G. A continuous function $\rho \colon G \to \mathbb{R}_+^*$ satisfying the identity

$$\rho(xh) = \frac{\Delta_H(h)}{\Delta_G(h)}\rho(x), \quad \text{for all} \quad x \in G, h \in H$$

for any locally compact group G and any closed subgroup H is called a **rho-function** for the pair (G, H).

Definition 3.7. The measure μ is **invariant** if $g\mu = \mu$ for all $g \in G$. We say that μ is **quasi-invariant** if μ and $g\mu$ are equivalent measures for all $g \in G$. Recall that two measures μ_1 and μ_2 on Ω are **equivalent** if, for every measurable subset A of Ω, we have $\mu_1(A) = 0$ if and only if $\mu_2(A) = 0$.

Definition 3.8. Let H be a closed subgroup of the locally compact group G. Let ρ be a rho-function for (G, H) and let μ be the corresponding quasi-invariant measure on G/H. The unitary representation $\lambda_{G/H}$ of G defined on $L^2(G/H) = L^2(G/H, \mu)$ by

$$\lambda_{G/H}(g)\xi(x) = \Big(\frac{\rho(g^{-1}x)}{\rho(x)}\Big)^{1/2}\xi(g^{-1}x), \quad g, x \in G, \quad ,\xi \in L^2(G/H)$$

is called the **quasi-regular representation** of G associated to H.

Now let Γ be a finitely generated group and $\mathcal{S}(V,S)$ be a Schreier graph with the vertex set V and finite symmetric generating set S of Γ. Let π_V be the quasi-regular representation of Γ on $\ell^2(V)$, thus

$$\pi_V(\gamma)\xi(x) = \xi(\gamma^{-1}x), \quad \xi \in \ell^2(V), x \in V, \gamma \in \Gamma.$$

Assume that V is finite. Then the constant functions on V belong to $\ell^2(V)$ and the subspace

$$\ell^2_0(V) = \{\xi \in \ell^2(V) \colon \sum_{x\in V} \xi(x) = 0\} = \{1_V\}^\perp$$

is Γ-invariant, where 1_V is the trivial map. The corresponding representation π^0_V of Γ on $\ell^2_0(V)$ has no non-zero invariant vectors. We set the following:

$$\kappa(\Gamma, S, \pi^0_V) = \inf\{\max_{x\in S} \|\pi_V(s)\xi - \xi\| \colon \xi \in \ell^2_0(V), \|\xi\| = 1\}.$$

This is the Kazhdan constant associated to S and π^0_v (see Remark 1.8). The following lemma relates this to the expansion constant of a graph.

Lemma 3.9. *Where Γ is a finitely generated group, S is a finite generating set of Γ with $S^{-1} = S$, V is a set,*

$$h(\mathcal{S}(V,S)) \geq \frac{\kappa(\Gamma, S, \pi^0_V)^2}{4}.$$

Proof. Let A be a proper non-empty subset of V. We have to show that there exists a unit vector $\xi \in \ell^2_0(V)$ such that

$$\frac{|\partial A|}{\min\{|A|, |V\setminus A|\}} \geq \frac{1}{4} \max_{s\in S} \|\pi_V(s)\xi - \xi\|^2.$$

Set $B = V \setminus A, n = |V|, a = |A|$, and $b = |B| = n - a$. Let $f \colon V \to \mathbb{C}$ be defined by

$$f(x) = \begin{cases} b & \text{if } x \in A \\ -a & \text{if } x \in B. \end{cases}$$

Then $f \in \ell^2_0(V)$ and

$$\|f\|^2 = ab^2 + ba^2 = nab.$$

Fix $x \in S$. We have

$$f(s^{-1}x) - f(x) = \begin{cases} b + a & \text{if } s^{-1}x \in A \text{ and } x \in B \\ -a - b & \text{if } s^{-1}x \in B \text{ and } x \in A \\ 0 & \text{otherwise.} \end{cases}$$

It follows that

$$\|\pi_V(s)f - f\|^2 = (a+b)^2|E_s| = n^2|E_s|,$$

where

$$E_s = (B \cap sA) \cup (A \cap sB) = (B \cap sA) \cup s(B \cap s^{-1}A).$$

It is clear that $|E_s| \leq 2|\partial A|$. Hence, with

$$\xi = \frac{1}{\sqrt{nab}} f,$$

we have $\|\xi\| = 1$ and

$$\begin{aligned} |\partial A| &\geq \frac{|E_s|}{2} = \frac{1}{2n^2}\|\pi_v(s)f - f\|^2 \\ &= \frac{nab}{2n^2}\|\pi_V(s)\xi - \xi\|^2 = \frac{ab}{2n}\|\pi_V(s)\xi - \xi\|^2. \end{aligned}$$

As

$$\min\{|A|, |V \setminus A|\} = \min\{a, b\} \leq \frac{2ab}{a+b} = \frac{2ab}{n},$$

we have

$$\frac{|\partial A|}{\min\{|A|, |V \setminus A|\}} \geq \frac{1}{4} \max_{s \in S} \|\pi_V(s)\xi - \xi\|^2$$

and this ends the proof. □

While this lemma deals with the case of a single Schreier graph, the upcoming theorem applies this knowledge to a particular family of Schreier graphs. This is the tool which we finally use to construct our example.

Theorem 3.10. *Let Γ be a group generated by a finite set S with $S^{-1} = S$. Let $(H_n)_n$ be a sequence of subgroups of Γ of finite index with*

$$\lim_n |(\Gamma / H_n)| = \infty.$$

Assume that there exists $\epsilon > 0$ such that, for every n, there is no (S, ϵ)-invariant vector in $\ell_0^2(\Gamma/H_n)$.

Then the family of the Schreier graphs $\mathcal{S}(\Gamma/H_n, S)$ is a family of $(k, \epsilon^2/4)$-expanders, where $k = |S|$.

Proof. Let $n \in \mathbb{N}$. Write π_n for π_{Γ/H_n}. Since there is no (S, ϵ)-invariant vector in $\ell_0^2(\Gamma/H_n)$, we have

$$\max_{s \in S} \|\pi_n(s)\xi - \xi\| \geq \epsilon$$

for all $\xi \in \ell_0^2(\Gamma/H_n)$ with $\|\xi\| = 1$. Hence $h(\mathcal{S}_n) \geq \epsilon^2/4$, by the previous lemma. □

Example 3.11. Let $\Gamma = \mathrm{SL}_3(\mathbb{Z})$. Then

$$S = \{E_{ij}^{\pm 1} : 1 \leq i, j \leq 3, i \neq j\}$$

is a generating set of Γ, where $E_{ij}^{\pm 1}$ is the elementary matrix. Yehuda Shalom proved in 1999 that $\mathrm{SL}_n(\mathbb{Z})$ has Property (T), while also giving an explicit Kazhdan constant (see Theorem 4.2.5 of [1]). We thereby have that

$$\epsilon = 1/960 \geq 1/(20\nu_3(\mathbb{Z}))$$

is a Kazhdan constant for the set S.

For every prime integer p, let

$$\Gamma(p) = \{A \in \Gamma \colon A \equiv I \mod p\},$$

that is, $\Gamma(p)$ is the kernel of the surjective homomorphism $\mathrm{SL}_3(\mathbb{Z}) \to \mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$ given by reduction module p. Since $\Gamma/\Gamma(p) \cong \mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$, the subgroup $\Gamma(p)$ has finite index

$$p^3(p^3-1)(p^2-1) \approx p^8.$$

The family of Schreier graphs $(\mathcal{G}(\Gamma/\Gamma(p), S))_p$ is a family of regular (k, ϵ')-expanders with

$$k = 12 \quad \text{and} \quad \epsilon' \approx \frac{1}{4}10^{-6}.$$

4. Property (τ) and $\mathrm{SL}_2(\mathbb{Z})$

Up until now, we have only been discussing Property (T) for $\mathrm{SL}_n(\mathbb{K})$ for $n \geq 3$. A natural question follows: what about $\mathrm{SL}_2(\mathbb{K})$? Does it have Property (T)?

Example 4.1. The free group F_2 of two generators embeds as a lattice in $\mathrm{SL}_2(\mathbb{R})$ as it is isomorphic to the group generated by $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$. Since F_2 does not have Property (T) as is seen in Example 1.3.7(i) of [1], by 3.1, neither does $\mathrm{SL}_2(\mathbb{R})$.

Thus our question is answered in the negative. One might think then that we cannot construct expanders from $\mathrm{SL}_2(\mathbb{Z})$, but interestingly enough, this is incorrect. While $\mathrm{SL}_2(\mathbb{Z})$ indeed does not have Property (T), it has something called Property (τ) with respect to its congruence subgroups, and we explore this property and its implications in this chapter. Here, we rely primarily on the book of Lubotzky [24] and lecture notes of Breuillard [6].

4.1. Property (τ)

Since Property (τ) uses a notion of "distance" between representations, it is helpful first for us to define a topology. This is called the Fell topology.

Definition 4.2. Let G be a locally compact group, $\tilde{G}, \tilde{G}_0$ denoting the space of equivalence classes of all unitary representations of G and those without invariant vectors respectively. Consider a representation (H, π) in $\tilde{G}$. For a compact subset K of G, $\epsilon > 0$ and $v \in H$ of norm one we define the neighbourhood $W(K, \epsilon, v)$ as those representations (H', π') in $\tilde{G}$ for which there exists $v' \in H'$ of norm one such that for every $g \in K$

$$|\langle v, \pi(g)v \rangle - \langle v', \pi'(g)v' \rangle| < \epsilon.$$

This defines the **Fell topology**.

It is also important to define the notions of subrepresentation and equivalence of representations. We borrow these definitions from [1].

Definition 4.3. Let π be a unitary representation of G in H, and let K be a closed G-invariant subspace of H. Denoting, for every g in G, by

$$\pi^K(g) \colon K \to K$$

the restriction of the operator $\pi(g)$ to K, we obtain a unitary representation π^K of G on K. We say that π^K is a subrepresentation of π, and this relation is denoted $\pi^K \subset \pi$.

Definition 4.4. An **intertwining operator** between two unitary representations π_1 of G in H_1 and π_2 of G in H_2 is a continuous linear operator T from H_1 to H_2 such that $T\pi_1(g) = \pi_2(g)T$ for all $g \in G$. The representations π_1 and π_2 are **equivalent** if there exists an intertwining operator $T \in \mathscr{L}(H_1, H_2)$ which is isometric and onto. The **unitary dual** of G is the set of all equivalence classes of irreducible unitary representations of G.

Now we come to the definition of Property (τ). Note that the notion of "isolated point" is with respect to the recently defined Fell topology.

Definition 4.5. Let Γ be a finitely generated group, $\tilde{\Gamma}$ be its unitary dual, and $\mathscr{L} = \{N_i\}$ be a family of finite index subgroups of Γ. Let $R = R(\mathscr{L}) = \{\phi \in \tilde{\Gamma}; \phi$ appears as a subrepresentation of the action of Γ on $L^2(\Gamma/N_i)$ for some $i\}$. Let $R_0 = R_0(\mathscr{L}) = R \cap \tilde{\Gamma}_0$. We say that Γ has **property** (τ) **with respect to the family** $\mathscr{L}$, or for short, Γ has $\tau(\mathscr{L})$, if the trivial representation is isolated from the set R_0 in $\tilde{\Gamma}$. We say that Γ has property (τ) if it has this property with respect to the family of all finite index subgroups.

It is the case that Property (T) implies Property (τ), although this may not be obvious from the definition given here. This is because our definition of Property (T) did not make use of the Fell topology; indeed if it did, the implication would appear obvious.

4.2. Graphs and manifolds

Property (τ) has equivalent definitions in various branches of mathematics. We will focus on two of these: the combinatorial definition, and a geometrical definition which relates it to Riemannian manifolds (see Definition C.3). We will combine these into a proof that $\mathrm{SL}_2(\mathbb{Z})$ has Property (τ) with respect to its congruence subgroups. We begin with the combinatorial definition.

Proposition 4.6. *A finitely generated group Γ is said to have property (τ) with respect to a family of finite index normal subgroups $(\Gamma_n)_n$ if and only if there exists a symmetric subset S of Γ such that the family of Schreier graphs $\mathcal{S}(\Gamma/\Gamma_n, S)$ is a family of expanders. If the family $(\Gamma_n)_n$ consists of all finite index normal subgroups of Γ, then we say that Γ has property (τ).*

Suppose we have a k-regular graph $\mathcal{G}$. One can define a function Δ on $\ell^2(\mathcal{G})$ in the following way:

$$\Delta f(x) := f(x) - \frac{1}{k}\sum_{x\sim y} f(y).$$

where we write $x \sim y$ to say that x is a neighbour of y in $\mathcal{G}$. This function is called the combinatorial Laplacian, and its spectrum is real and contained in $[0,2]$. Its eigenvalues are commonly denoted $\lambda_0 = 0 < \lambda_1 \leq \ldots \leq \lambda_{|\mathcal{G}|}$. The spectrum is related to the expansion constant of $\mathcal{G}$ in the following way:

Proposition 4.7 (Discrete Cheeger-Buser inequality). *Given a connected, k-regular graph, we have*

$$\frac{1}{2}\lambda_1(\mathcal{G}) \leq \frac{1}{k}h(\mathcal{G}) \leq \sqrt{2\lambda_1(\mathcal{G})}.$$

There is an analagous function on connected Riemannian manifolds called the Laplace-Beltrami operator, which is a non-negative self-adjoint operator on L^2 functions. For a compact, connected Riemannian manifold, the spectrum of the Laplace-Beltrami operator is discrete just as is the manner of the combinatorial Laplacian: $\lambda_0(M) = 0 < \lambda_1(M) \leq \ldots$. Note that in both cases, λ_1 is sometimes called the "spectral gap".

The fundamental group of M, denoted $\pi_1(M)$ (see Definition C.5), acts on the universal cover $\tilde{M}$ (see Definition C.6) by isometries called "deck transformations", and given a base point $x_0 \in \tilde{M}$, we can construct a fundamental domain (see Definition B.20) in the following way:

$$\mathcal{F}_M = \{x \in \tilde{M}; d(x, x_0) < d(x, \gamma \cdot x_0) \forall \gamma \in \pi_1(M) \backslash \{1\}\}.$$

We obtain a finite symmetric set for $\pi_1(M)$: $\{\gamma \in \pi_1(M) \colon \gamma \cdot \mathcal{F}_M \cap \mathcal{F}_M \neq \emptyset\}$.

The relation of all this to Property (τ) lies in the following theorem from Burger [8] and its corollary.

Theorem 4.8. *Let M be a compact Riemannian manifold with fundamental group $\Gamma = \pi_1(M)$. Let S be the finite symmetric generating set of Γ obtained from a fundamental domain $\mathcal{F}_M$ as above. Then there are constants $c_1, c_2 > 0$ depending on M only such that for every finite cover M_0 of M*

$$c_1 \lambda_1(M_0) \leq \lambda_1(\mathcal{S}(\Gamma/\Gamma_0, S)) \leq c_2 \lambda_1(M_0),$$

where Γ_0 is the fundamental group of M_0 and $\mathcal{S}(\Gamma/\Gamma_0, S))$ the Schreier graph of the finite coset space Γ/Γ_0 associated to the generating set S.

Corollary 4.9. *Suppose $(M_n)_n$ is a sequence of finite covers of M. Then there is a uniform lower bound on $\lambda_1(M_n)$ if and only if $\Gamma := \pi_1(M)$ has Property (τ) with respect to the sequence of finite index subgroups $\Gamma_n := \pi_1(M_n)$.*

There exists a statement called the uniformization theorem which tells us that the universal cover of any Riemmanian manifold is equivalent to one of three possibilities: the Riemann sphere, the complex plane, or the upper half plane $\mathbb{H}^2 = \{x + iy | y > 0\}$. Thus, one can classify a Riemannian manifold as being one of three types: elliptic, parabolic, or hyperbolic, respectively. A hyperbolic manifold M has a nontrivial fundamental group $\pi_1(M)$ which is isomorphic to a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$.

$\mathrm{SL}_2(\mathbb{R})$ acts on the upper half plane $\mathbb{H}^2$ by Mobius transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az + b}{cz + d}.$$

The stabilizer of i is $SO(2)$, so Theorem B.12 tells us that $\mathbb{H}^2 \cong \mathrm{SL}_2(\mathbb{R})/SO(2)$.

The following theorem is central one in our study, as we will see shortly.

Theorem 4.10 (Selberg's theorem). *Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and $\Gamma(m) = \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}))$. Then*

$$\lambda_1(\Gamma(m) \backslash \mathbb{H}^2) \geq \frac{3}{16}$$

where $\mathbb{H}^2 = \mathrm{SL}_2(\mathbb{R})/SO(2)$ is the upper half plane on which $G = \mathrm{SL}_2(\mathbb{Z})$ acts.

Corollary 4.11. $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ *has Property* (τ) *with respect to the family of its congruence subgroups* $\Gamma(m)$.

Proof. We can immediately apply Theorem 4.8 to see that $\lambda_1(\mathcal{S}(\Gamma/\Gamma(m), S))$ is nonzero. We follow this up with Proposition 4.7 to see that $h(\mathcal{S}(\Gamma/\Gamma(m), S))$ is nonzero. Our conclusion is then evident from Proposition 4.6. □

Returning to one of the themes of this paper, we see that indeed we can construct expander graphs using $\mathrm{SL}_2(\mathbb{Z})$ despite the fact that it does not have Property (T).

5. The Expansion Machine

After the results in the previous chapter were found, Lubotzky asked the following question, now known as the **Lubotzky 1-2-3 problem**. Let

$$S_a = \left\{ \begin{pmatrix} 1 & \pm a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \pm a & 1 \end{pmatrix} \right\}.$$

We know that the Schreier graphs of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, for p prime, with respect to S_1 form a family of expanders since $\langle S_1 \rangle = \mathrm{SL}_2(\mathbb{Z})$ and we can apply Selberg's theorem. We also know this holds for S_2 and $p = 2$ because $\langle S_2 \rangle$ form a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and we can again apply Selberg's theorem. However, this method does not work for S_3, as $\langle S_3 \rangle$ forms an infinite index subgroup. Nonetheless, does $\mathcal{S}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), S_3)$ form a family of expanders for $p > 3$?

This is in fact a simple example of a more general problem, but we have chosen to keep the advanced terminology to a minimum in this paper, as the reader is not expected to have any background in graduate-level algebra. For additional information, we refer to [23].

In 2005, Bourgain and Gamburd [4] gave a positive answer to Lubotzky's question using an argument which is today called the Bourgain-Gamburd expansion machine. Their theorem is as follows:

Theorem 5.1. *Let S be a set of elements in $\mathrm{SL}_2(\mathbb{Z})$, and let S_p be the projection of S modulo p. Then the $\mathcal{S}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), S_p)$ form a family of expanders if and only if $\langle S \rangle$ is not virtually solvable.*

They prove this through another result of theirs which is related to the girth of the relevant Schreier graphs.

Definition 5.2. The **girth** of a graph is the length of the shortest cycle contained in the graph.

Theorem 5.3. *Fix $k \geq 2$ and suppose that $S_p = \{g_1, g_1^{-1}, \ldots, g_k, g_k^{-1}\}$ is a symmetric generating set for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ such that*

$$\mathrm{girth}(\mathcal{S}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), S_p)) \geq \kappa \log_{2k} p,$$

where $\kappa > 0$ is a fixed constant independent of p. Then the $\mathcal{S}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), S_p)$ form a family of expanders.

Since the logarithmic girth condition assumed in the statement of Theorem 5.3 was proven in [13] for $\langle S \rangle$ a free group, it follows for $\langle S \rangle$ not virtually solvable since $\langle S \rangle \cap \Gamma(2)$ is a free nonabelian group.

A central tool in the argument of Bourgain and Gamburd is that of the random walk.

Definition 5.4. Let $\mathcal{G}$ be a k-regular graph, and select a vertex v. A **random walk** is a random sequence of vertices $v_0, v_1, \ldots$ defined in the following way: given vertices $v_0, \ldots, v_i$, we choose v_{i+1} randomly from among the neighbours of v_i.

To study random walks on the Schreier graph $\mathcal{S}(G,S)$ of a finite group G with respect to a symmetric generating set S, we define a probability measure on G supported on S by

$$\mu_S = \frac{1}{|S|}\delta_{v_0}$$

where v_0 is the initial vertex and

$$\delta_x(y) = \begin{cases} 1 \text{ if } x = y \\ 0 \text{ if } x \neq y. \end{cases}$$

We further define the convolution of two measures ω and ν on G to be

$$\omega * \nu := \sum_{y \in G} f(y)g(y^{-1}x) = \sum_{y \in G} f(xy^{-1})g(y).$$

We denote n-fold convolution product of ω by ω^n. Returning to the probability measure μ_S, the probability distribution of the vertex v_i is μ_S^i. We get the recursion formula

$$\mu_S^{i+1} = \frac{1}{|S|} A \mu_S^i,$$

where A is the adjacency operator. The general formula is then

$$\mu_S^i = \frac{1}{|S|^i} A^i \delta_{v_0}.$$

We also define the ℓ^2 norm for a measure ω to be

$$\|\omega\|_2 = \left(\sum_{g \in G} \omega^2(g) \right)^{1/2}.$$

Another tool, which was used to great effect in the proof, is the notion of an approximate group, which was first defined by Tao in [30].

Definition 5.5. A finite subset A of a group G with $K \geq 1$ is said to be a K-approximate subgroup of G if A is symmetric, contains the identity, and if there is a symmetric subset $X \subset G$ of size $|X| \leq K$ such that $A \cdot A \subset X \cdot A$.

By $X \cdot A$, we mean $\{x \cdot a \colon x \in X, a \in A\}$.

Before we start the proof, we define some symbols. Let $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ and S be a symmetric generating set for G of size $2k$. Let $\mu = \mu_S$ be the probability measure on G supported on S. We use the notation $X = O(Y)$ and $Y = \Omega(X)$ to denote $X \leq CY$ for some absolute constant C.

We begin by noting a theorem of Helfgott from [16].

Theorem 5.6. *Let H be a subset of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Assume that $|H| < p^{3-\delta}$ for $\delta > 0$ and H is not contained in any proper subgroup of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Then*

$$|H \cdot H \cdot H| > c|H|^{1+\sigma}$$

where $c > 0$ and $\sigma > 0$ depends only on δ.

The essential meaning here is that the subset H grows under multiplication. We can combine this with a standard lemma to arrive at a classification of the approximate subgroups of G.

Lemma 5.7. *Let H be a finite subset of a group G and $K \geq 1$ a parameter. If $|A \cdot A \cdot A \leq K|A|$, then $(A \cup A^{-1} \cup \{1\})^2$ is a $O(K^{O(1)})$-approximate subgroup of G.*

Theorem 5.8. *Let H be a generating set of G and let $K \geq 1$. Then one of the following holds:*

- $|A| \leq K^C$.
- $|A| \geq K^{-C}|G|$.
- $|A \cdot A \cdot A| \geq K|A|$.

One can interpret this to say that there are no non-trivial approximate subgroups of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Given this, we want to use the following theorem by Tao [30].

Theorem 5.9. *Let G be a group, let ν be a finitely supported probability measure on G which is symmetric (i.e. $\forall g \in G, \nu(g) = \nu(g^{-1})$), and let $K \geq 1$. Then one of the following hold:*

- $\|\nu * \nu\|_2 \leq \frac{1}{K}\|\nu\|_2$;
- *There exists a $O(K^{O(1)})$-approximate subgroup H in G with $|H| \ll \frac{K^{O(1)}}{\|\nu\|_2^2}$ and $x \in G$ such that $\nu(xH) \gg K^{-O(1)}$.*

Since we see from Helfgott that there is no such approximate subgroup of G, we arrive at the other statement, which is commonly called flattening for the reason that it describes the flattening of the probability distribution under convolution. What this ensures is that a random walk on $\mathcal{S}(G, S)$ will not get stuck in a proper subgroup. This is a crucial fact used in the proof of the following proposition.

Proposition 5.10. *Suppose $\mathcal{S}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), S_p)$ with $|S_p| = 2k$ satisfies*

$$\mathrm{girth}(\mathcal{S}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}), S_p)) \geq \kappa \log_{2k} p.$$

Then for any $\epsilon > 0$ there is $C(\epsilon, \kappa)$ such that for $l > C(\epsilon, \kappa)\log_{2k} p$

$$\|\mu_{S_p}^l\|_2 < p^{-\frac{3}{2}+\epsilon}.$$

Finally, we want to prove expansion via the spectral gap of the graph. Recall that the spectral gap of the combinatorial Laplacian determines the expansion constant of a graph. This has a direct analogue in the eigenvalues of the adjacency matrix $A := A(\mathcal{S}(G,S))$: $2k = \alpha_0 > \alpha_1 \geq \ldots \geq \alpha_{|G|-1} \geq -2k$. Thus, to prove expansion for our family of graphs, we need to find a lower bound on $2k - \alpha_1$.

By right regular representation π_R, we mean the representation which acts by permutation on $\ell^2(G)$. In other words,

$$\pi_R(g)\colon f(x) \mapsto f(xg^{-1}).$$

One can check that the following sum holds:

$$A = \sum_{s\in S} \pi_R(s)$$

We can decompose the regular representation in the following way:

$$\pi_R = \rho_0 \oplus \bigoplus_{\substack{\rho\in\hat{G}\\ \rho\neq\rho_0}} \underbrace{\rho\oplus\cdots\oplus\rho}_{d_\rho},$$

where ρ_0 the trivial representation and d_ρ is the dimension of ρ. That is, each nontrivial irreducible representation ρ appears d_ρ times in the sum; this is a standard fact for the representation theory of finite groups (see [29]). A result of Frobenius [12] states that for our current case, $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, we have

$$d_\rho \geq \frac{p-1}{2}$$

for each nontrivial irreducible representation. Since A preserves each of the subspaces corresponding to the irreducible ρ, the nontrivial eigenvalues of A each have multiplicity greater than or equal to $\frac{p-1}{2}$.

We devise a trace formula for A^n. First, we denote by W_m the number of closed walks from the identity to itself with length m on the graph $\mathcal{S}(G,S)$. One particular interpretation of $A^n_{i,j}$ is that it counts the number of walks of length n from v_i to v_j. This gives us

$$\sum_{i=0}^{|G|-1} \alpha_i^n = |G|W_n$$

Note that we also have $\mu^n(1) = \frac{W_n}{(2k)^n}$ where $2k^{2l}$ is the number of all walks from the identity of length $2l$ since $|S| = 2k$. We know $\mu^{2n}(1) = \|\mu^n\|_2^2$, and so by Proposition 5.10 we have for $l > C(\epsilon,\kappa)$,

$$\mu^{2l}(1) < p^{2\epsilon-3}.$$

We get

$$W_{2l} < \frac{(2k)^{2l}}{p^{3-2\epsilon}}.$$

Now, it is obvious that, letting α be the largest eigenvalue of A,

$$\sum_{i=0}^{|G|-1} \alpha_i^2 l > m_p(\alpha)\alpha^{2l}$$

where $m_p(\alpha)$ is the multiplicity of α. Recall that a lower bound on $m_p(\alpha)$ is $\frac{p-1}{2}$. Therefore, setting $l > C(\epsilon, \kappa)$ and using Proposition 5.10, we arrive at

$$\frac{p-1}{2}\alpha^{2l} < \sum_{i=0}^{|G|-1} \alpha_i^{2l} = |G|W_{2l} < |G|\frac{(2k)^{2l}}{p^{3-2\epsilon}}.$$

We compute $|G| = p(p^2-1) < p^3$ and so

$$\alpha^{2l} = O(\frac{(2k)^{2l}}{p^{1-2\epsilon}}).$$

We then set $l = C(\epsilon, \kappa)$ to get

$$\alpha_1 \leq \alpha < (2k)^{1-\frac{1-2\epsilon}{C(\epsilon)}} < 2k = \alpha_0,$$

which demonstrates a spectral gap independent of p, giving us expansion of the family we were looking for. This ends the proof of Theorem 5.3. For more details, the reader is referred to [4].

We now cover some algebrogeometric material. An *algebraic variety* is, simply speaking, the set of solutions to a system of polynomials. We can define a topology with algebraic varieties, and it is called the *Zariski topology*. Rather than being defined by its open sets, the Zariski topology is defined by its closed sets: a closed set is the algebraic variety to a system of polynomials. An *algebraic group* is a group that is also an algebraic variety and whose multiplication and inversion are given by so-called *regular maps*, and furthermore, a *linear algebraic group* is an algebraic group that is a subgroup of $\mathrm{GL}_n(\mathbb{K})$ where $\mathbb{K}$ is a field (or equivalently, a Zariski-closed linear group), an example of which is $\mathrm{SL}_2(\mathbb{R})$.

Observe the following theorem which was proven in the 1980s by Nori and Weisfeiler.

Theorem 5.11 (Strong approximation theorem). *Suppose $\mathbb{G}$ is a connected, simply connected, semisimple algebraic group defined over $\mathbb{Q}$, and let $\Gamma \leq \mathbb{G}(\mathbb{Q})$ be a finitely generated Zariski-dense subgroup. Denote by $\mathbb{G}_p$ the smooth reduction of $\mathbb{G}$ over $\mathbb{Z}/p\mathbb{Z}$. Then for all sufficiently large prime numbers p, the reduction Γ_p of Γ is equal to $\mathbb{G}_p(\mathbb{Z}/p\mathbb{Z})$.*

This theorem tells us that for any Zariski-dense subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, we have $\Gamma_p = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ for p large enough; applying Theorem 5.1, this allows us to achieve Property (τ) with respect to the family of prime principal congruence subgroups for Γ.

When reading [4] for the first time, one might not immediately catch on to the generality of the argument. However it is actually predicated on three key assumptions.

Theorem 5.12. *Let G_0 be a finite group and S_0 be a symmetric generating subset of size k. Suppose there are constants $0 < \kappa < 1 < \Lambda$ for which the following hold:*

- *The dimension of nontrivial representations of G are bounded below by $|G|^\kappa$;*
- *For all $\delta > 0$, there is $\delta' = \delta'(\delta) > 0$ such that if $H \subseteq G$ is a $|G|^{\delta'}$-approximate subsgroup with $|G|^\delta \leq |H| \leq |G|^{1-\delta}$, then H generates a proper subgroup of G;*
- *There is an even number $n \leq \Lambda \log |G|$ such that*

$$\sup_{H<G} \mu^n(H) < |G|^{-\kappa},$$

where H is a proper subgroup of G.

Then $\mathcal{S}(G_0, S_0)$ is an ϵ-expander for $\epsilon = \epsilon(k, \kappa, \Lambda, \delta'(\cdot))$.

This is what is now known as the "Bourgain-Gamburd expansion machine", and it has been used very fruitfully since its inception. Soon after his growth theorem for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Helfgott proved the same for $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$ in [17]. Pyber-Szabó [28] and Breuillard-Green-Tao [5] subsequently proved this for finite simple groups of Lie type. The probabilistic condition was proven for $\mathrm{SL}_n(\mathbb{Z})$ by Bourgain and Gamburd in [3], and this was extended to further generality by Varjú in [32] and subsequently by Salehi-Golsefidy and Varjú in [15]. In particular, the following strengthening of Theorem 5.11 was found.

Theorem 5.13 (Super-strong approximation). *Suppose $\mathbb{G}$ is a connected, simply connected, semi-simple algebraic group defined over $\mathbb{Q}$, and let $\Gamma \leq \mathbb{G}(\mathbb{Q})$ be a Zariski-dense subgroup generated by a finite set S. Then there is $\epsilon = \epsilon(S) > 0$ such that for all large enough prime numbers p, the reduction Γ_p of Γ is equal to $\mathbb{G}_p(\mathbb{Z}/p\mathbb{Z})$ and the associated Schreier graph $\mathcal{S}(\mathbb{G}_p(\mathbb{Z}/p\mathbb{Z}), S_p)$ is an ϵ-expander.*

One can see that this is a formulation of Property (τ) with respect to a family of subgroups for a very large class of groups. In particular, Γ has Property (τ) with respect to its prime principal congruence subgroups.

6. Examples of Property (τ)

One might ask: what groups do not have Property (τ)? The following definition, proposition, and theorem set the stage for our first two examples. They come from [1], [24], and [11] respectively.

Definition 6.1. Let π and ρ be unitary representations of the topological group G into H and K respectively. We say that π is **weakly contained** in ρ if every function of positive type associated to π can be approximated, uniformly on compact subsets of G, by finite sums of functions of positive type associated to ρ. This means, for every $\xi \in H$, every compact subset $Q \subset G$, and every $\epsilon > 0$, there exist $\eta_1, \ldots, \eta_n \in K$ such that, for all $x \in Q$,

$$\left| \langle \pi(x)\xi, \xi \rangle - \sum_{i=1}^{n} \langle \rho(x)\eta_i, \eta_i \rangle \right| < \epsilon.$$

We write for this $\pi \prec \rho$.

If $\pi \prec \rho$ and $\rho \prec \pi$, we say that π and ρ are **weakly equivalent** and denote this by $\pi \sim \rho$.

For a compact space X with a finite measure μ, let $\ell_0^2(X)$ be the set of complex valued functions f such that $\int_X |f(x)|^2 d\mu(x) < \infty$ and $\int_X f(x) d\mu(x) = 0$.

Proposition 6.2. *A group Γ has property $\tau(\mathcal{L})$ if and only if the representation of Γ on $\hat{\oplus}\ell_0^2(\Gamma/N_i)$ does not weakly contain the trivial representation.*

Theorem 6.3 (Schur's orthogonality relations). *Let π and π' be irreducible unitary representations of a compact group G in H_π and H'_π respectively, and consider E_π and $E_{\pi'}$ as subspaces of $L^2(G)$ (where E_π and $E_{\pi'}$ are the linear spans of the matrix coefficients of π and π').*

(1) If $[\pi] \neq [\pi']$ then $E_\pi \perp E_{\pi'}$.

(2) If $\{e_j\}$ is any orthonormal basis for H_π and π_{ij} is given by $\pi_{ij}(x) = \langle \pi(x)e_j, e_i \rangle$, then $\{\sqrt{d_\pi}\pi_{ij} : i, j = 1, \ldots, d_\pi\}$ is an orthonormal basis for E_π.

Example 6.4. We show that $\mathbb{Z}$ does not have (τ) using Proposition 6.2. To start, every irreducible character of $\mathbb{Z}/n\mathbb{Z}$ can be considered an element of $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}] = L^2[\mathbb{Z}/n\mathbb{Z}]$, i.e. $\chi_{n,j}(k) = e^{2\pi i jk/n} = \xi^{jk}$, so $\chi_{n,j} = \sum_{k \in \mathbb{Z}/n\mathbb{Z}} \xi^{jk} \cdot k$. These characters form an orthogonal basis for $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}]$ by Schur's orthogonality relations (Theorem 6.3), so we say

$$L^2[\mathbb{Z}/n\mathbb{Z}] = \oplus_{j=1}^{n} \mathbb{C}\chi_{n,j}.$$

Let $\sigma_n : \mathbb{Z}/n\mathbb{Z} \to \mathcal{B}(\ell_0^2[\mathbb{Z}/n\mathbb{Z}])$ be the left regular representation. Then

$$\sigma_n(x)f(g) = f(g - x) = \sum_{j \in \mathbb{Z}/n\mathbb{Z}} c_j \chi_{n,j}(g - x).$$

We directly show that the left regular representation $\sigma = \oplus\sigma_n$ of $\mathbb{Z}$ in $\hat{\oplus}\ell^2_0(\mathbb{Z}/n\mathbb{Z})$ contains the trivial representation. Given a compact $Q \subset \mathbb{Z}$ and an $\epsilon > 0$, we must find functions $\eta_m \in \hat{\oplus}\ell^2_0(\mathbb{Z}/n\mathbb{Z})$ such that

$$\left|1 - \sum_{m=1}^{r} \langle \sigma(x)\eta_m, \eta_m \rangle\right| < \epsilon.$$

Note that the irreducible character $\chi_{n,j}$ are eigenfunctions of $\sigma(x)$. Indeed,

$$\sigma(x)\chi_{n,j}(k) = \sigma_n(x)\chi_{n,j}(k) = \chi_{n,j}(k-x) = e^{-2\pi ijx/n} \cdot e^{2\pi ijk/n}.$$

Notice here how σ is "factoring through" a finite quotient. That is, it can be seen as reducing modulo n as it acts due to its direct sum decomposition. Also, observe that $\chi_{n,j}$ is in $\ell^2_0(\mathbb{Z}/n\mathbb{Z})$ as it averages to 0 over its values.

Now we look for a root of unity $\xi = e^{2\pi ik/n}$ such that $|\xi^k - 1| < \epsilon$, where k is element of greatest magnitude in Q. Specifically, we look for $n(k,\epsilon)$ such that $|e^{2\pi ik/n} - 1| < \epsilon$.

$$\begin{aligned}
&|\cos(2\pi k/n) + i\sin(2\pi k/n) - 1| < \epsilon \\
\implies &(\cos(2\pi k/n) - 1)^2 + (\sin(2\pi k/n))^2 < \epsilon^2 \\
\implies &\cos^2(2\pi k/n) + \sin^2(2\pi k/n) - 2\cos(2\pi k/n) + 1 < \epsilon^2 \\
\implies &2 - 2\cos(2\pi k/n) < \epsilon^2 \\
\implies &1 - \frac{\epsilon^2}{2} < \cos(2\pi k/n) \\
\implies &\frac{2\pi k}{\arccos(1 - \frac{\epsilon^2}{2})} < n
\end{aligned}$$

In the case where $\epsilon > 2$, setting $\epsilon = 2$ works and allows the computation of arccos.

We thus see the following, letting $n = \lceil \frac{2\pi k}{\arccos(1-\frac{\epsilon^2}{2})} \rceil$:

$$\begin{aligned}
\max_{x\in Q} |1 - \langle \sigma(x)\chi_{n,1}, \chi_{n,1}\rangle| &= \max_{x\in Q} |1 - e^{-2\pi ix/n}\langle \chi_{n,1}, \chi_{n,1}\rangle| \\
&= \max_{x\in Q} |1 - e^{-2\pi ix/n}| \\
&< \epsilon.
\end{aligned}$$

Notice how $\sum_{k\in\mathbb{Z}/n\mathbb{Z}} \chi_{n,1}(k) = 0$, so it is in $\ell^2_0(\mathbb{Z}/n\mathbb{Z})$. Thus the trivial representation is weakly contained in $(\sigma, \hat{\oplus}\ell^2_0(\mathbb{Z}/n\mathbb{Z}))$. By Proposition 6.2, $\mathbb{Z}$ does not have Property (τ).

Example 6.5. We show that $\mathbb{Z}^n$ does not have Property (τ) using a modified argument. Let $\mathcal{L} = \{m\mathbb{Z}^n\}_{m\geq 2}$ be a family of finite index subgroups of $\mathbb{Z}^n$. The irreducible representations of $\mathbb{Z}^n/m\mathbb{Z}^n \cong (\mathbb{Z}/m\mathbb{Z})^n$ are defined as the direct products of the irreducible representations identified in Example 6.4:

$$\begin{aligned}
\beta_{m,j} \colon (\mathbb{Z}/m\mathbb{Z})^n &\to \mathbb{C}^\times \\
(y_1, \ldots, y_n) &\mapsto \chi_{m,j}(y_1)\cdots\chi_{m,j}(y_n).
\end{aligned}$$

The regular representation α of $\mathbb{Z}^n$ in $\hat{\oplus}\ell_0^2[\mathbb{Z}^n/m\mathbb{Z}^n]$ weakly contains the trivial representation. To show this, note that $\beta_{m,j}$ is an eigenfunction of $\alpha(x_1,\dots,x_n)$:

$$\alpha(x_1,\dots,x_n)\beta_{m,j}(y_1,\dots,y_n) = \beta_{m,j}(y_1-x_1,\dots,y_n-x_n) = \prod_{s=1}^{n} e^{-2\pi i j x_s/m}\cdot e^{2\pi i j y_s/m}.$$

Pick a compact subset $Q \subset \mathbb{Z}^n$ and $\epsilon > 0$. Then, using the method of Example 6.4, we see that there is $r \in \mathbb{N}$ such that for the point $(x_1,\dots,x_n)$ with the highest value of $x_1\cdots x_n$, we have $|1-\prod_{s=1}^{n} e^{2\pi i j x_s/r}| < \epsilon$. Finally,

$$\begin{aligned}\max_{(x_1,\dots,x_n)\in Q} |1-\langle\alpha(x)\beta_{r,1},\beta_{r,1}\rangle| &= \max_{(x_1,\dots,x_n)\in Q} |1-\prod_{s=1}^{n} e^{-2\pi i j x_s/r}\langle\beta_{r,1},\beta_{r,1}\rangle| \\ &= \max_{(x_1,\dots,x_n)\in Q} |1-\prod_{s=1}^{n} e^{-2\pi i j x_s/r}| \\ &< \epsilon,\end{aligned}$$

so we see $1_{\mathbb{Z}^n} \prec (\alpha, \hat{\oplus}\ell_0^2[\mathbb{Z}^n/m\mathbb{Z}^n])$, and $\mathbb{Z}^n$ does not have $\tau(\mathscr{L})$, meaning $\mathbb{Z}^n$ cannot have Property (τ).

We now want to show that virtually solvable groups do not have Property (τ) (see Definition B.17 for the definition of "solvable" and Definition B.19 for the meaning of "virtually"). We start off again by establishing two facts which come from [24].

Definition 6.6. Let G be a group and let $\mathscr{L} = \{N_i\}_{i\in I}$ be a family of finite index subgroups of G. We say that G has FAb($\mathscr{L}$) if for every i, $|N_i/[N_i,N_i]| < \infty$. If $\mathscr{L}$ is the family of all finite index subgroups of G, then we say that G has Property FAb.

Corollary 6.7. *If G is a finitely generated group with Property (τ), then it has Property FAb.*

Lemma 6.8. *All solvable groups with Property FAb are finite.*

Proof. Let $G_1 = [G,G]$ be the first derived subgroup of G. By FAb, $G_1/[G_1,G_1]$ is finite, so $G/[G_1,G_1]$ must be finite. Call $G_2 = [G_1,G_1]$. We see by the same method that $G/[G_2,G_2]$ is finite. By repetition, we see that $G/[G_n,G_n] = G/[\{1\},\{1\}] = G$ because G is soluble, thereby having a terminating derived series by Theorem B.18. This shows that G is finite. □

Corollary 6.9. *Infinite virtually solvable groups do not have Property FAb, and thus do not have Property (τ).*

There exists a well-known theorem attributed to Jacques Tits which poses a dichotomy with regards to linear groups. It is recounted here.

Theorem 6.10 (Tits alternative). *Let Γ be a finitely generated linear group over some field $\mathbb{K}$. Then either*

- Γ *is virtually solvable, or*
- Γ *contains a non-abelian free subgroup on two generators* F_2.

One might then wonder – does the free group have Property (τ)? The answer is no, as it has a surjective homomorphism to $\mathbb{Z}$, which we have already shown does not have (τ). Yet, the Tits alternative does show us that every finitely generated linear group with Property (τ) does have a free group in it. Another theorem can take us further.

Theorem 6.11 (Lubotzky alternative). *Let* Γ *be a finitely generated linear group over some field* $\mathbb{K}$ *of characteristic zero. Then either*

- Γ *is virtually solvable, or*
- *there exists a non-trivial connected, simply connected semisimple algebraic group* $\mathbb{G}$ *defined over* $\mathbb{Q}$ *and a group homomorphism from a finite index subgroup of* Γ *into* $\mathbb{G}(\mathbb{Q})$ *with a Zariski-dense image.*

Applying Theorem 5.11, we see that the finite index subgroup admits $\mathbb{G}_p(\mathbb{Z}/p\mathbb{Z})$ as a quotient for almost all p. We can go even further by applying Theorem 5.13.

Theorem 6.12 (Lubotzky super-alternative). *Let* S *be a finite symmetric subset of* $\mathrm{GL}_d(\mathbb{K})$, *where* $\mathbb{K}$ *is a field of characteristic zero. Then the subgroup* $\Gamma = \langle S \rangle$ *contains a subgroup* Γ_0 *whose index* m *in* Γ *is finite and bounded in terms of* d *only such that either*

- Γ_0 *is solvable, or*
- *there exists a connected, simply connected, semisimple algebraic group* $\mathbb{G}$ *defined over* $\mathbb{Q}$, *such that for all large enough prime numbers* p, *there is a surjective group homomorphism* ρ_p *from* Γ_0 *to* $\mathbb{G}(\mathbb{Z}/p\mathbb{Z})$ *such that the Schreier graph* $\mathcal{S}(\mathbb{G}_p(\mathbb{Z}/p\mathbb{Z}), \rho_p(S_0))$ *is an* ϵ*-expander, for some* $\epsilon > 0$ *independent of* p, *where* S_0 *is a subset of* S^{2m} *generating* Γ_0.

This effectively states that if one picks a non-solvable subgroup $\Gamma_0 \leq \Gamma$, then Γ_0 has Property (τ) with respect to its prime principal congruence subgroups for p large enough.

We can refine the alternative further. A well-known theorem is the next one.

Theorem 6.13 (Lie-Kolchin theorem). *Every irreducible representation of a connected, solvable linear algebraic group over an algebraically closed field has dimension* 1.

In particular, the theorem implies that the image of a finite-dimensional representation of such a group is simultaneously triangularizable (i.e. there is a basis in which all these matrices are upper triangular). One sees also in [14] that the Zariski closure of a solvable group is solvable. Thus, with respect to the symbols in Theorem 6.12, if $\mathbb{K}$ is an algebraically closed field, and if Γ_0 is solvable, and the Zariski closure of Γ_0 (call it Γ_1) is connected, we have that the image of Γ_1 under any finite-dimensional representation is simultaneously triangularizable by Theorem 6.13.

A. Topology and Analysis

Theorem A.1 (Tychonoff's theorem). *An arbitrary product of compact spaces is compact in the product topology. [26, p. 234]*

Definition A.2. A class of sets $\mathfrak{F}$ is called a **sigma-algebra** (σ**-algebra**, σ**-ring**, or **Borel field of events**) if for any sequence $\{A_n\}$ of sets from $\mathfrak{F}$, then

$$\bigcup_{n=1}^{\infty} A_n \in \mathfrak{F}, \qquad \bigcap_{n=1}^{\infty} A_n \in \mathfrak{F}.$$

[2, p. 14]

Definition A.3. Let (Ω, τ) be a topological space. The σ-algebra

$$\mathscr{B}(\Omega) \coloneqq \mathscr{B}(\Omega, \tau) \coloneqq \sigma(\tau)$$

that is generated by the open sets is called the **Borel** σ**-algebra** on Ω. The elements $A \in \mathscr{B}(\Omega, \tau)$ are called **Borel sets** or **Borel measurable sets**. [19, p. 9]

Definition A.4. A set X together with a σ-algebra Σ is called a **measurable space**, and the elements of Σ are called its **measurable sets**. [21, p.113]

Definition A.5. Let X be a measurable space and let Σ be the collection of its measurable sets. A **positive measure** on Σ (or on X, by abuse of language) is a map

$$\mu \colon \Sigma \to [0, \infty]$$

which is **countably additive**. In other words $\mu(\emptyset) = 0$, and if $\{A_n\}$ is a sequence of measurable sets which are mutually disjoint ($A_n \cap A_m$ is empty if $n \neq m$), then

$$\mu\Big(\bigcup_{n=1}^{\infty} A_n\Big) = \sum_{n=1}^{\infty} \mu(A_n).$$

If A is measurable, we call $\mu(A)$ its **measure**, or μ-measure if the reference to μ is necessary to avoid confusion. [21, p. 120]

Definition A.6. Let X be a set and x_0 an element of X. If A is a subset of X containing x_0, we define $\mu(A) = 1$. If A does not contain x_0 we define $\mu(A) = 0$. It is immediately verified that this defines a measure called the **Dirac** measure at x_0.

Definition A.7. A **mean** m on a ring $\mathcal{R}$ of subsets of X containing X is a finitely additive probability measure on $\mathcal{R}$, that is, m is a function from $\mathcal{R}$ to $\mathbb{R}$ with the following properties:

(1) $m(A) \geq 0$ for all $A \in \mathcal{R}$;

(2) $m(X) = 1$;

(3) $m(A_1 \cup \cdots \cup A_n) = m(A_1) + \cdots + m(A_n)$ if $A_1, \ldots, A_n \in \mathcal{R}$ are pairwise disjoint.

If a group G acts on X leaving $\mathcal{R}$ invariant, then m is said to be a ***G*-invariant mean** if

(4) $m(gA) = m(A)$ for all $g \in G$ and $A \in \mathcal{R}$.

[1, p. 421]

Let X be a locally compact space, equipped with the σ-algebra $\mathcal{B}(X)$ of its Borel subsets. Let H be a Hilbert space. Denote by $\mathrm{Proj}(H)$ the set of orthogonal projections on $\mathcal{L}(H)$.

Definition A.8. A **projection-valued measure** on X is a mapping

$$E \colon \mathcal{B}(X) \to \mathrm{Proj}(H)$$

with the following properties:

(1) $E(\emptyset) = 0$ and $E(X) = I$;

(2) $E(B \cap B') = E(B)E(B')$ for all $B, B' \in \mathcal{B}(X)$;

(3) if $(B_n)_n$ is a sequence of pairwise disjoint sets from $\mathcal{B}(X)$, then

$$E\Big(\bigcup_{n\in\mathbb{N}} B_n\Big) = \sum_{n\in\mathbb{N}} E(B_n),$$

where the sum is convergent in the strong operator topology on $\mathcal{L}(H)$.

[1, p. 374]

Definition A.9. Let P be a projection-valued measure. If f is a simple function, say $f = \sum_1^n c_j \chi_{E_j}$, then

$$\int f dP_{u,v} = \sum c_j P_{u,v}(E_j) = \sum c_j \langle P(E_j)u, v\rangle = \langle \sum c_j P(E_j)u, v\rangle,$$

so that $\int f dP = \sum c_j P(E_j)$ as one would expect. Moreoever, since every $f \in B(\Omega)$ is a uniform limit of a sequence $\{f_n\}$ simple functions, and since $\| \int f dP - \int f_n dP\| \leq 4\|f - f_n\|_{\sup}$, we can obtain $\int f dP$ as a limit (in the norm topology) of "Riemann sums" just as we do for ordinary integrals. [11, p. 21]

Definition A.10. A **Borel measure** on X is a (not necessarily finite) positive measure on $\mathcal{B}(X)$. A Borel measure μ on X is said to be regular if

(1) $\mu(B) = \inf\{\mu(V)\colon V \text{ is open and } B \subset V\}$ for every Borel set B,

(2) $\mu(U) = \sup\{\mu(K)\colon K \text{ is compact and } K \subset U\}$ for every open subset U of X,

(3) $\mu(K) < \infty$ for every compact subset K of X.

If every open subset of X is σ-compact (that is, a countable union of compact subsets), then (3) implies (1) and (2). [1, p. 299]

Definition A.11. Suppose f and g are functions on the real line. Their **convolution** is defined by the integral

$$f * g(y) = \int_{-\infty}^{\infty} f(x)g(y-x)dx.$$

[21, p. 223]

B. Algebraic Structures

Definition B.1. A **topological group** is a group together with a Hausdorff topology such that the maps

$$\begin{aligned} \Gamma \times \Gamma &\to \Gamma & (\alpha, \beta) &\mapsto \alpha\beta \\ \Gamma &\to \Gamma & \alpha &\mapsto \alpha^{-1} \end{aligned}$$

are continuous. [10, p. 1]

Theorem B.2. *Let K and H be groups and let $\theta\colon H \to \operatorname{aut} K$ be a homomorphism. Write $\theta(h) = \sigma_h$ for all $h \in H$. If $G = K \times H$ is the cartesian product, define an operation on G as follows:*

$$(k,h)(k_1,h_1) = (k\sigma_h(k_1), hh_1), \quad \text{for all } (k,h) \text{ and } (k_1,h_1) \text{ in } G.$$

Write $K_1 = K \times 1$ and $H_1 = 1 \times H$. Then:

(1) G is a group using this operation with unity $(1_K, 1_H)$ and inverses given by $(k,h)^{-1} = (\sigma_{h^{-1}}(k^{-1}), h^{-1})$.

(2) Then K_1 and H_1 are subgroups of G, with $K_1 \cong K$ and $H_1 \cong H$.

(3) $G = K_1H_1, K_1 \lhd G$ and $K_1 \cap H_1 = \{1\}$.

[27, p. 379]

Definition B.3. If K and H be groups and $\theta\colon H \to \operatorname{aut} K$ is a homomorphism, the group G constructed in Theorem B.2 is called the **semidirect product** of K by H, and is denoted $K \ltimes H$. [27, p. 380]

Definition B.4. A space X is said to be **compact** if every open covering $\mathscr{A}$ of X contains a finite subcollection that also covers X. [26, p. 164] A **compact group** is a topological group that is a compact topological space. [10, p. 1]

Definition B.5. A space X is said to be **locally compact at x** if there is some compact subspace C of X that contains a neighbourhood of x. [26, p. 182] If X is locally compact at each of its points, X is said simply to be **locally compact**. A **locally compact group** is a topological group that is a locally compact topological space.

Definition B.6. A **lattice** in a locally compact group G is a discrete subgroup Γ of G such that G/Γ carries a finite invariant regular Borel measure. Note that such a measure is unique up to a constant factor. [1, p. 332]

Definition B.7. A field $\mathbb{K}$ is a **local field** if $\mathbb{K}$ can be equipped with an absolute value for which $\mathbb{K}$ is locally compact and not discrete. [1, p. 377]

Definition B.8. A **unitary character** of G is a continuous homomorphism $\chi\colon G \to \boldsymbol{S}^1$, where $\boldsymbol{S}^1$ is the multiplicative group of all complex numbers of modulus 1. The set of all unitary characters is called the **dual group** or **Pontryagin dual** of G and is denoted $\hat{G}$.

Definition B.9 (Group Actions). Let G be a group and let X be a nonempty set. A mapping $G \times X \to X$, denoted $(a, x) \mapsto a \cdot x$, is called an **action** of G if it satisfies the following conditions.

(1) $1 \cdot x = x$ for all $x \in X$.

(2) $a \cdot (b \cdot x) = (ab) \cdot x$ for all $x \in X$ and for all $a, b \in G$.

In this case, G is said to **act** on X and X is called a ***G*-set**. [27, p. 365]

Definition B.10. If X is a G-set, we define a relation $\equiv$ as follows. If $x, y \in X$, we write

$$x \equiv y \mod G, \quad \text{if} \quad y = a \cdot x \text{ for some } a \in G.$$

One easily verifies that $\equiv$ is an equivalence on X. Moreover, we may describe the equivalence class $[x]$ of an element x of X in terms of the action:

$$[x] = \{y \in X | y \equiv x\} = \{a \cdot x | a \in X\}.$$

This equivalence class is called the **orbit** of x under G and is denoted

$$G \cdot x = \{a \cdot x | a \in G\}.$$

[27, p. 367]

Definition B.11. If X is a G-set and $x \in X$, the subgroup

$$S(x) = \{a \in G | a \cdot x = x\}$$

is called the **stabilizer** of x. [27, p. 368]

Theorem B.12 (Cauchy-Frobenius Lemma). *Let X be a G-set and assume that G and X are finite. If n is the number of distinc orbits of G in X, then*

$$n = \frac{1}{|G|} \sum_{a \in G} |F(a)|.$$

[27, p. 383]

Definition B.13. An element in a group G of the form $aba^{-1}b^{-1}$ is called a **commutator** and is denoted

$$[a, b] = aba^{-1}b^{-1}, \quad \forall a, b \in G.$$

Hence, if $H \triangleleft G$ then G/H is ablian if and only if H contains every commutator. [27, p. 134]

Definition B.14. The **commutator subgroup** or **derived subgroup** G' of G is defined by

$$G' = \{\text{all finite products of commutators from } G\}.$$

[27, p. 134]

Theorem B.15. *Let G be a group and let H be a subgroup of G.*

(1) G' is a normal subgroup of G and G/G' is abelian.

(2) $G' \subseteq H$ if and only if H is normal in G and G/H is abelian.

[27, p. 135]

Definition B.16. A **subnormal series** for a group G is a chain

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{1\}$$

of subgroups of G such that $G_{i+1} \triangleleft G_i$ for each i. The factor groups G_i/G_{i+1} are called the **factors** of the subnormal series. [27, p. 389]

Definition B.17. A group G is called a **solvable group** if there exists a subnormal series

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$$

such that each factor G_i/G_{i+1} is abelian. Such a series is called a **solvable** series for G. [27, p. 395]

Theorem B.18. *A group is solvable if and only if its derived series terminates. [27, p. 396]*

Definition B.19. A group **virtually has property (Π)** if it contains a finite index subgroup with property (Π). [9, p. 5]

Definition B.20. Let G be a group and S be a topological G-set. Then a closed subset F of S is called a fundamental domain of G in S if S is the union of conjugates of F, i.e.,

$$S = \bigcup_{g \in G} gF$$

and the intersection of two conjugates has no interior. [31]

C. Differential Geometry

Definition C.1. A **smooth premanifold** of dimension n is a Hausdorff topological space M together with a set $\mathcal{U}$ of pairs (U,ϕ), where the set of U such that $(U,\phi) \in \mathcal{U}$ for some ϕ is an open cover of M and such that, for each $(U,\phi) \in \mathcal{U}$, the image $\phi(U)$ of ϕ is an open subset of $\mathbb{R}^n$ and ϕ is a homeomorphism of U onto $\phi(U)$. We assume that if $U,V \in \mathcal{U}$, then $\phi_V \circ \phi_U^{-1}$ is a diffeomorphism from $\phi_U(U \cap V)$ onto $\phi_V(U \cap V)$. The set $\mathcal{U}$ is called an **atlas**. [7, p. 39]

Definition C.2. If M is a premanifold with atlas $\mathcal{U}$, and if we replace $\mathcal{U}$ by the larger set $\mathcal{U}'$ of all pairs (U,ϕ), where U is an open subset of M and ϕ is a diffeomorphism of U onto an open subset of $\mathbb{R}^n$, then the set of smooth maps $M \to N$ or $N \to M$, where N is another premanifold, is unchanged. If $\mathcal{U} = \mathcal{U}'$, then we call $\mathcal{U}'$ a **maximal atlas** and M a **smooth manifold**. [7, p. 39]

Definition C.3. A **Riemannian metric** on a differentiable manifold M is given by a scalar product on each tangent space T_pM which depends smoothly on the base point p. A **Riemannian manifold** is a differentiable manifold equipped with a Riemannian metric. [18, p. 13]

Definition C.4. A **path** or **curve** in a connected manifold M is a continuous map

$$c\colon [0,a] \to M \quad (a \geq 0).$$

A **loop** is a path with $c(0) = c(a)$, and that point then is called the **base point** of the loop. [18, p. 557]

Definition C.5. Two paths $c_i\colon [0,a_i]$ with $c_1(0) = c_2(0)$ and $c_1(a_1) = c_2(a_2)$ are called **equivalent** or **homotopic** if there exists a continuous function

$$H\colon [0,1] \times [0,1] \to M$$

with

$$\begin{aligned} H(t,0) &= c_1\left(\frac{t}{a_1}\right), \\ H(t,1) &= c_2\left(\frac{t}{a_2}\right), \quad \forall t, \\ H(0,s) &= c_1(0) = c_2(0), \\ H(1,s) &= c_1(a_1) = c_2(a_2), \quad \forall s. \end{aligned}$$

The equivalence or homotopy classes of loops with fixed base point $p \in M$ form a group $\pi_1(M,p)$ called the **fundamental group** of the connected manifold M with **base point** p.

If p and q are in M and $\gamma\colon [0,1] \to M$ satisfies $\gamma(0) = p, \gamma(1) = q$, then for every loop c with base point q, $\gamma^{-1}c\gamma$ is a loop with base point p, and this induces an isomorphism between $\pi_1(M,q)$ and $\pi_1(M,p)$. We may thus speak of the fundamental group $\pi_1(M)$ of M without reference to a base point. M is called **simply connected** if $\pi_1(M) = 0$. [18, p. 557]

Definition C.6. A continuous map

$$\pi\colon X \to M$$

is called a **covering map** if each $p \in M$ has a neighborhood U with the property that each connected component of $\pi^{-1}(U)$ is mapped homeomorphically onto U. If $p \in M$ and H is a subgroup of $\pi_1(M,p)$, there exists a covering $\pi\colon X \to M$ with the property that for any $x \in X$ with $\pi(x) = p$, we have $\pi_*(\pi_1(X,x)) = H$.

If we choose $H = \{1\}$, we obtain a simply connected manifold $\tilde{M}$ and a covering

$$\pi\tilde{M} \to M.$$

$\tilde{M}$ is called the **universal covering** of M. [18, p. 558]

Bibliography

[1] M. Bachir Bekka, Pierre de la Harpe, and Alain Valette. *Kazhdan's Property (T)*. New Mathematical Monographs: 11. Cambridge: Cambridge University Press, 2008.

[2] Alexandr A. Borovkov. *Probability Theory*. Fifth. Universitext. London: Springer-Verlag, 2013.

[3] Jean Bourgain and Alex Gamburd. "Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$". In: *J. Eur. Math. Soc.* 11.5 (2009), pp. 1057–1103.

[4] Jean Bourgain and Alex Gamburd. "Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$". In: *Ann. of Math.* 167 (2008), pp. 625–642.

[5] E. Breuillard, B. Green, and T. Tao. "Approximate subgroups of linear groups". In: *Geom. Funct. Anal.* 21.4 (2011), pp. 774–819.

[6] Emmanuel Breuillard. "Expander Graphs, Property (τ) and Approximate Groups". 2012. URL: www.math.u-psud.fr/~breuilla/BreuillardPCMI.pdf.

[7] Daniel Bump. *Lie Groups*. Graduate Texts in Mathematics: 225. New York: Springer, 2013.

[8] Marc Burger. "Spectre du laplacien, graphs et topologie de Fell". In: *Comment. Math. Helv.* 63.2 (1988), pp. 226–252.

[9] Cornelia Druţu. "Geometry of Nilpotent and Solvable Groups". 2011. URL: https://people.maths.ox.ac.uk/drutu/tcc/TCC-transp1.pdf.

[10] Joel Feldman. "Haar Measure". 2002. URL: http://www.math.ubc.ca/~feldman/m606/haar.pdf.

[11] Gerard B. Folland. *A course in abstract harmonic analysis*. Studies in advanced mathematics. Boca Raton: CRC Press, 1995.

[12] Georg Frobenius. "Über Gruppencharaktere". In: *Sitzungsber. Kön. Preuss. Akad. Wiss. Berlin* (1896), pp. 985–1021.

[13] Alex Gamburd. "On the spectral gap for infinite index "congruence" subgroups of $\mathrm{SL}_2(\mathbb{Z})$". In: *Israel J. Math* 127 (2002), pp. 157–200.

[14] William M. Goldman and Morris W. Hirsch. "Flat bundles with solvable holonomy". In: *Proc. Amer. Math. Soc.* 82.3 (1981), pp. 491–494.

[15] A. S. Golsefidy and P. P. Varjú. "Expansion in perfect groups". In: *Geom. Funct. Anal.* 22.6 (2012), pp. 1832–1891.

[16] Harald Helfgott. "Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$". In: *Ann. of Math.* 167 (2008), pp. 601–623.

[17] Harald Helfgott. "Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$". In: *J. Eur. Math. Soc.* 13.3 (2011), pp. 761–851.

[18] Jürgen Jost. *Riemannian Geometry and Geometric Analysis*. Springer-Verlag, 2008.

[19] Achim Klenke. *Probability Theory*. Universitext. London: Springer-Verlag, 2008.

[20] E. Kowalski. "Expander graphs". 2013. URL: http://www.math.ethz.ch/~kowalski/expander-graphs.pdf.

[21] Serge Lang. *Real and Functional Analysis*. Graduate Texts in Mathematics: 142. New York: Springer-Verlag, 1993.

[22] Serge Lang. $SL_2(\mathbb{R})$. Graduate Texts in Mathematics: 105. New York: Springer-Verlag, 1985.

[23] Alexander Lubotzky. "Expander graphs in pure and applied mathematics". In: *Bull. Amer. Math. Soc. (N.S.)* 49.1 (2012), pp. 113–162. URL: http://www.ams.org/journals/bull/2012-49-01/S0273-0979-2011-01359-3/S0273-0979-2011-01359-3.pdf.

[24] Alexander Lubotzky. "On property (τ)". 2003. URL: www.ma.huji.ac.il/~alexlub/BOOKS/On%20property/On%20property.pdf.

[25] G. A. Margulis. "Explicit Constructions of Concentrators". In: *Probl. Peredachi Inf.* 9.4 (1973), pp. 71–80.

[26] James R. Munkres. *Topology*. Second. Upper Saddle River, NJ: Prentice Hall, 2000.

[27] W. Keith Nicholson. *Introduction to abstract algebra*. John Wiley & Sons, 2012.

[28] L. Pyber and E. Szabó. "Growth in finite simple groups of Lie type". In: *J. Amer. Math. Soc.* (2014).

[29] J.P. Serre. *Linear representations of finite groups*. Trans. by Leonard L. Scott. Springer-Verlag, 1977.

[30] Terence Tao. "Product set estimates in noncommutative groups". In: *Combinatorica* 28 (2008), pp. 547–594.

[31] David Terr and Richard Peterson. *Fundamental Domain. From MathWorld–A Wolfram Web Resource*. Visited on 14/03/15. URL: http://mathworld.wolfram.com/FundamentalDomain.html.

[32] P. P. Varjú. "Expansion in $\mathrm{SL}_d(\mathcal{O}_K/I), I$ square-free". In: *J. Eur. Math. Soc.* 14.1 (2012), pp. 273–305.