PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

YEHUDA SHALOM

Bounded generation and Kazhdan's property (T)

Publications mathématiques de l'I.H.É.S., tome 90 (1999), p. 145-168
<http://www.numdam.org/item?id=PMIHES_1999__90__145_0>

BOUNDED GENERATION AND KAZHDAN'S PROPERTY (T)

by YEHUDA SHALOM

1. INTRODUCTION AND DISCUSSION OF THE MAIN RESULTS

I. Introduction

The fascinating subject of arithmetic groups, in its various aspects, has attracted much attention in contemporary mathematics. Its influence on group, representation, and number theory, and its baring on many other fields of research, are by now well recognized. (Recall that a subgroup of a (semisimple) linear algebraic group $\mathbf{G}$ defined over Q, is called **arithmetic** if it is commensurable with $\mathbf{G}(\mathbf{Z})$.) A fundamental question is to understand the finite dimensional linear representation theory of arithmetic groups, a theme which splits naturally into two: representations with finite, and those with infinite image. The latter may be viewed as a part of the rigidity theory, while the former is known essentially as the congruence subgroup problem (or "property"), abbreviated CSP. Another important feature of arithmetic groups is concerned with their infinite dimensional representation theory, pertaining to property (T) of Kazhdan.

The connection between the above three themes is only partially understood, although there is a strong circumstantial evidence that such in fact exists (for simplicity, we confine the discussion here to $\mathbf{Q}$-simple, simply-connected algebraic groups, and leave aside also the S-arithmetic case). Indeed, both superrigidity and property (T) are known to hold for exactly the same family of groups, including the real rank one groups $\mathrm{Sp}(n, 1)$, $F_{4(-20)}$, whose treatment was traditionally different from that of the higher rank groups. This "empirical fact" is partially explained in [Mok] and [Pa], where the same Bochner-type formulae developed in [MSY] for superrigidity, are used to establish Kazhdan's property. The two phenomena are further unified in [Sh2], where they are derived simultaneously from the rigidity theory of harmonic maps. On the other hand, the CSP is known to hold for "most" families of higher rank arithmetic groups, where the first two properties are present as well. Moreover, CSP implies superrigidity (see [BMS, §16] and [Rag, §7]). In a different direction, Lubotzky [Lub2] proved that the CSP is characterized by having a "slow growth" of the number of subgroups of finite index, and it is known that Kazhdan groups share a closely related property [HRV, Prop. IV]. Unfortunately, the current known results on property (T) are not yet sharp enough to be used for the question of CSP (compare also with [Lub1, 10.4.1]).

In the last decade or so, a new notion has been introduced into this circle of ideas: A group G is said to be **boundedly generated** if it admits a finite subset

S, and some number ν depending only on G and S, such that every $g \in G$ may be written as a product: $g = g_1^{k_1} g_2^{k_2} \ldots g_\nu^{k_\nu}$, with $g_i \in S$ and k_i integers. This notion originates in the work of Carter and Keller [CK], establishing bounded generation for the groups $SL_n(\mathcal{O})$ $(n \geqslant 3)$, where $\mathcal{O}$ is the ring of integers of a number field, relying on class field theory (primarily, on Dirichlet's theorem regarding primes in arithmetic progressions). Rapinchuk has established a fairly direct relation between bounded generation and rigidity (see [Rap3] and the references therein). He conjectured [Rap1] that bounded generation and CSP are equivalent, thereby suggesting a clean group theoretic characterization of the latter. (As observed in [Lub2, (5.5)], a conjecture in this general form would be inconsistent with CSP for the word hyperbolic lattices with property (T) – a problem which is fascinating in its own right.) In fact, in [PR] Rapinchuk and Platonov showed that bounded generation implies CSP (and hence also superrigidity), a result which was also established independently by Lubotzky [Lub2]. We remark, however, that bounded generation has not yet provided any new examples of groups with CSP. Moreover, there is no **uniform** lattice of a semisimple algebraic group which is known to posses this property.

In this paper we relate intimately another two of the above notions. More precisely, we make a strong use of bounded generation in the study of property (T) of Kazhdan, motivated by a problem raised by Serre, and by de La Harpe and Valette. Let us first recall the notions involved.

Definition **1.1.** — *Let* G *be a topological group,* $K \subset G$ *a subset,* $\varepsilon > 0$, *and* $(\pi, \mathcal{H})$ *a continuous unitary* G*-representation. A vector* $v \in \mathcal{H}$ *is called* (K, ε)*-invariant, if* $\|\pi(g)v - v\| < \varepsilon\|v\|$ $\forall g \in K$. *The group* G *is said to have* **property (T) (of Kazhdan)** *if there exist a compact* $K \subset G$ *and* $\varepsilon > 0$, *such that every continuous unitary* G*-representation with a* (K, ε)*-invariant vector, contains a non-zero* G*-invariant vector. In that case,* (K, ε) *(or sometimes just* ε, *when the set* K *is clear from the context), are called* **Kazhdan constants** *for* G.

The fundamental work of Kazhdan [Kaz] showed that higher rank simple algebraic groups over local fields, as well as their lattices, have property (T), but without supplying explicitly any Kazhdan constants. Over the years, property (T) turned out to be an extremely interesting and powerful tool, and such constants make many of the numerous applications of it, quantitative (cf. [HV] for details). While there is no natural choice of a subset $K \subset G$ when G is an algebraic group, for many lattices, e.g., $SL_n(\mathbf{Z})$ $n \geqslant 3$, it is natural to seek a bound on ε for certain generating sets (such as the unit elementary matrices in the preceding example), as was posed by Serre and by de la Harpe-Valette (cf. [Bur] and [HV, p. 133]).

The question of Kazhdan constants for semisimple groups and their lattices was solved in general in [Sh1] (see there for more related literature). However, while the solution for the continuous groups is in a certain sense optimal, producing a Kazhdan set K of **two** elements, with the largest possible ε, the results for the lattices are much less satisfactory, being dependent on a fundamental domain, and giving ε for a "large" Kazhdan set, of a geometric, rather than algebraic type [Sh1, Theorem B]. Although it might be possible to work out individual cases, the results of [Sh1] seem hopeless in studying fundamental questions such as the behaviour of the constant over $SL_n(\mathcal{O})$, when the dimension n, or the ring $\mathcal{O}$, are varied. A partial result on Kazhdan constants for the group $SL_3(\mathbf{Z})$ was obtained by Burger in [Bur]. Here we shall establish a complete result, presenting a general, quite unexpected phenomenon of uniformity of the constant for any dimension $n \geqslant 3$, over various families of finite, infinite, locally compact and even infinite dimensional rings, and an explicit lower bound $O(n^{-2})$ over n. In particular, we present for some arithmetic groups (such as $SL_3(\mathbf{Z})$) the first treatment of property (T), which is based only on their internal structure.

II. Statement and discussion of the main results

In the case of $G = SL_n(\mathbf{Z})$, the bounded generation property is known to hold with respect to the set S of the unit elementary matrices (see Definition 1.2 and the Main Theorem below). It seems important to remark, however, that the bounded generation property may depend in general on the choice of S (for instance, a somewhat surprising fact which does not seem to appear in the literature is that the group $SL_n(\mathbf{Z}[\frac{1}{p}])$ is **not** boundedly generated by **any** finite set of unipotent matrices. As shown by Tavgen [Tav], by using appropriate semisimple elements one can make this group boundedly generated). Since we shall be interested also in rings which are not finitely generated as **Z**-modules, we consider a more general bounded generation property. Here is the precise notion we shall use.

Definition **1.2.** — *Let* R *be a commutative ring with unit, and* $SL_n(R)$ *the group of determinant one* $n \times n$ *matrices over* R. *An* **elementary matrix** $E_{i,j}(t) \in SL_n(R)$, $1 \leqslant i \neq j \leqslant n$, $t \in R$, *is the matrix having 1 in its diagonal,* t *in the entry* (i,j), *and 0 elsewhere. The group* $SL_n(R)$ *is said to be* **boundedly elementary generated** *if there is some* $\nu = \nu_n(R) < \infty$ *such that every matrix in* $SL_n(R)$ *may be written as a product of at most* ν *elementary matrices. When this property is satisfied, we shall sometimes denote it simply by writing* $\nu_n(R) < \infty$.

In the case where $R = \mathcal{O}$ is the ring of integers of a number field, bounded elementary generation is precisely the property established in [CK] (for $n \geqslant 3$), and is easily seen to imply the previous group theoretic bounded generation property, for an appropriate finite subset S. Trivial examples of rings with $\nu_n(R) < \infty$ are fields, and even these will be of interest to us in the sequel. The knowledgeable reader will notice the connection between this notion (and some of our discussion in the sequel), and K-theory, although we will avoid using K-theoretic terminology.

The main result of the paper is the following:

Main Theorem. — *Fix an integer* $n \geqslant 3$, *let* R *be a commutative topological ring with unit, and suppose* $\nu_n(\mathrm{R}) < \infty$. *Assume that for some* $1 \leqslant m < \infty$ *there exist elements* $\alpha_1, \ldots, \alpha_m \in \mathrm{R}$ *generating a* **dense** *subring. Let* $\mathrm{F}_1 \subset \mathrm{SL}_n(\mathrm{R})$ *be the set of unit elementary matrices (i.e., having 1 off the diagonal), and* F_2 *be the set of elementary matrices* $\{\mathrm{E}_{i,j}(t)\}$ *with* $|i-j| = 1$ *and* $t = \alpha_k$ $(1 \leqslant k \leqslant m)$. *Then* $\mathrm{SL}_n(\mathrm{R})$ *has property* (T), *with* $\varepsilon = \nu_n(\mathrm{R})^{-1} 22^{-m-1}$ *as a Kazhdan constant for the set* $\mathrm{F}_1 \cup \mathrm{F}_2$. *Moreover, if for some fixed m,* α_i*'s as above can be found in every neighborhood of* $0 \in \mathrm{R}$, *then* F_1 *alone is a Kazhdan set for* $\mathrm{SL}_n(\mathrm{R})$, *with the same Kazhdan constant.*

For instance, if R is any locally compact, non discrete field, the assumptions of the theorem are trivially verified ($m = 2$ suffices, when R is connected the last assertion applies). We remark that the proof will show that the formulation of the Main Theorem can be made more general: R need not be a topological ring, but merely a ring with some topology. Then the above Kazhdan constants apply, for the family of unitary representations which are strongly continuous with respect to this topology (i.e., for every vector v the map $g \rightarrow gv$ is continuous from $\mathrm{SL}_n(\mathrm{R})$ with the topology induced by its natural inclusion in R^{n^2}, to the Hilbert space). Thus, the conclusion of the Main Theorem holds, for instance, for the set of all continuous unitary representations of $\mathrm{SL}_n(\mathrm{K})$, if K is any field equipped with a topology for which some finitely generated subring is dense.

Before stating some consequences of the Main Theorem, which are discussed in Section 4, we remark that in the theorem and its corollaries below one may replace, with similar proofs, the group ("scheme") SL_n, by any Chevalley group of rank > 1. Elementary matrices should then be replaced by "root subgroups", and the notion of bounded elementary generation modified accordingly.

Throughout the rest of this section n denotes an integer $\geqslant 3$.

Corollary **1.** — *The value* $\varepsilon = (33n^2 - 11n + 1122)^{-1}$ *is a Kazhdan constant for the group* $\mathrm{SL}_n(\mathbf{Z})$, *for the set of all elementary matrices with 1 off the diagonal. If* $\mathcal{O}$ *is the ring of integers of a number field* K, *and it is generated* **as a ring** *by* $1, \alpha_1, \ldots, \alpha_m$, *then* $\varepsilon = 22^{-m-1}[\frac{n}{2}(3n-1) + 68\Delta + 2]^{-1}$ *is a Kazhdan constant for the generating set* $\mathrm{F} \subset \mathrm{SL}_n(\mathcal{O})$ *described in the Main Theorem, where* Δ *denotes the number of distinct (rational) primes dividing the discriminant of* K. *The same estimate holds if we replace* $\mathcal{O}$ *by any localization* $\mathcal{O}_{\mathrm{S}}$.

Corollary 1 follows from the Main Theorem using the bounds on ν_n in [CK]. Corresponding bounds on ν_n for all higher rank arithmetic Chevalley groups can be obtained from the work of Tavgen [Tav] (who established their bounded generation). In the case of $\mathrm{SL}_n(\mathbf{Z})$, a proof of bounded generation appears in [AM], which modulo Dirichlet's theorem, is completely elementary. Section 2 below is devoted to the study of $SL_n(\mathbf{Z})$ in the Main Theorem, both because several ingredients of the proof will be needed for the general case (discussed in Section 3), and to supply, together with [AM], a complete and more accessible treatment of this particularly interesting case (see Theorem 2.6). No induced representations appear in our approach, and the only tool used from representation theory is the spectral theorem for representations of discrete abelian groups (recalled in the proof). A remark which was pointed out to us by A. Zuk, is that the optimal Kazhdan constant for $SL_n(\mathbf{Z})$ (with the above generators) is bounded from above by $\sqrt{2/n}$, and in particular it must depend on n. This follows easily by considering the natural representation on $\ell^2(\mathbf{Z}^n - \{0\})$, and the action on the characteristic function of the set of n "standard basis" unit vectors. It therefore seems of interest to close (even asymptotically) the gap between $O(n^{-2})$ and $O(n^{-1/2})$, of the optimal Kazhdan constant, left by this work.

Notice that Corollary 1 yields for families of rings $\mathcal{O}$ a uniform Kazhdan constant for $SL_n(\mathcal{O})$, with respect to generating sets with fixed cardinality. For instance, this is the case if we consider all localizations of any given ring of integers, or take rings of the form $\mathbf{Z}[\sqrt{p}]$, when p varies over all primes, or $\mathbf{Z}[\omega]$, when ω varies over all prime power roots of unity. We should also add that W. van der Kallen has shown, relying upon [CW], that assuming a Generalized Riemann Hypothesis, the bound on $\nu_n(\mathcal{O})$ does not depend on $\mathcal{O}$ at all! In this direction Loukanidis and Murty showed (see [Mu]) that if S is a sufficiently large set of valuations of $\mathcal{O}$ (depending linearly on the degree of the field extension, $|S| \geqslant 5$ suffices for $\mathbf{Z}$), then $\nu_n(\mathcal{O}_S)$ depends only on n, with an explicit quadratic bound, and not on $\mathcal{O}$ or S. Since the number of generators of $\mathcal{O}$ as a ring is typically small, these results, together with the Main Theorem, suggest a general and quite surprising phenomenon of uniformity of property (T) for families of arithmetic groups.

Corollary **2.** — *Suppose that* R *is compact, and* m *elements of* R *(including 1) generate a dense subring. Then* $\varepsilon = (5n^2 22^m)^{-1}$ *is a Kazhdan constant for the finite set* $F \subset SL_n(R)$, *as constructed in the Main Theorem.*

For the proof see 4.1 and 4.5 below. This corollary is of interest already for finite rings, as there are few known non trivial estimates for Kazhdan constants even for finite groups. For instance, any finite field is generated by one element, so for any fixed $n \geqslant 3$, the groups $SL_n(K)$ (where K varies over all finite fields) are all generated by $n^2 + n - 2$ elements, for which $(1000n^2)^{-1}$ is a Kazhdan constant. It would be interesting to see whether the latter result holds (even qualitatively) when $n = 2$ as well. Also notice that Corollary 2 implies that for compact groups of the form $SL_n(R)$ ($n \geqslant 3$), the existence of a finitely generated dense subgroup suffices to ensure that of a **finite** Kazhdan set. Moreover, the size of the Kazhdan set and constant depend only on the cardinality of a topologically generating set. (In particular, these compact groups have a positive answer to the "Banach-Ruziewicz problem", and their finite quotients form an expander family.)

Corollary **3.** — *Let* R *be any finite (commutative) ring. Consider the ring* $R((t))$ *of Laurent series over* R, *equipped with the usual topology where high powers of t are close to 0. Then* $SL_n(R((t)))$ *(which is locally compact) has property* (T) *of Kazhdan, with explicit Kazhdan constants as in Corollary 2.*

See 4.1 and 4.6 below for details. The proof of Corollary 3 will show that, as in Corollary 2, one has $\nu_n \leqslant 5n^2$ for these rings, independently of R. Taking a family of cyclic rings, say $R_n = \mathbf{Z}/p^n\mathbf{Z}$, yields a construction of a sequence of locally compact Kazhdan groups, each a homomorphic image of its preceding, so that the Kazhdan constants for the (compatible) Kazhdan sets are all uniformly bounded from below. The inverse limit of these groups, which is a non locally compact topological group, also has property (T). Notice that the discrete group $SL_n(R[t^{-1}])$, with R as in Corollary 3, is a lattice in $SL_n(R((t)))$, hence has property (T) as well.

Corollary **4.** — *Let* $L(SL_n(\mathbf{C}))$ *denote the* **loop group** *associated with* $SL_n(\mathbf{C})$, *namely, the group of continuous maps from the circle to* $SL_n(\mathbf{C})$, *under pointwise multiplication and the topology of uniform convergence. Then* $L(SL_n(\mathbf{C}))$ *has property* (T). *Moreover,* $\varepsilon = (3n^2 \cdot 22^4)^{-1} > 10^{-6} \cdot n^{-2}$ *is a Kazhdan constant for the set* F *of* $n^2 - n$ *maps taking constant values on each of the unit elementary matrices.*

These groups are the first examples of infinite dimensional Lie groups (in particular, non locally compact groups) with property (T). They also seem the first constructions of Kazhdan groups whose group of outer automorphisms is infinite (see Paulin's question in [HV, p. 134]). Indeed, the group of homeomorphisms of the circle is embedded naturally in their outer automorphism group. There is still no known example of such locally compact group, excluding trivial constructions coming from infinite products of one compact group (which may be excluded by considering only Kazhdan groups with a **finite** Kazhdan set). We should also mention that Corollary 4 holds if one considers smooth, rather than continuous maps, with the appropriate smooth topology.

Some of the important facts about unitary representations of loop groups were first observed by physicists, and the subject was studied in depth by many authors, with applications in quantum field theory and elementary particle physics, as well as relativity and gravitation theory – see e.g. [PS], [Is] and the references therein (and also [VGG] for a detailed treatment of the case $SL_2(\mathbf{R})$). Also notice that since any connected group is a homomorphic image of its loop group, a necessary condition for the loop group to have property (T) is that the original group has it. This condition is however not sufficient, as the case of $SO(n, 2)$ $(n \geqslant 3)$ will show (see the discussion following the proof of Lemma 4.8). It may be interesting to study more generally the question of property (T) for loop groups of simple Lie groups (the case of $\mathrm{Sp}(n, 1)$ being especially challenging).

If one replaces S^1 by higher dimensional spheres, our method of proving property (T) for the above groups (more precisely, the bounded elementary generation over appropriate rings) fails, so this larger family of so called "current groups" may also be interesting to study by different methods. We remark that if G is a p-adic algebraic group, there is of course no loop group associated to it, but one can study the current group obtained by replacing S^1 with a Cantor set. Our method will establish property (T) for groups of this type as well (see Theorem 4.9).

Corollary **5.** — *Let* $R = \mathbf{Z}[x_1, \ldots, x_m]$ *denote the ring of polynomials with m variables over* $\mathbf{Z}$. *If* $v_n(R) < \infty$ *then* $SL_n(R)$ *has property* (T).

It is an open question, raised by W. van der Kallen [Kal] in the context of K-theory, whether $v_n(R) < \infty$ (even in the case $m = 1$). It was shown in [Kal] that if $\mathbf{Z}$ is replaced by $\mathbf{C}$ the answer is negative, but even the situation with $\mathbf{Q}$ seems unknown. Notice that specializing the variables to non algebraic complex values embeds Γ as a linear group which is not a lattice (having elements with non algebraic eigenvalues). It would be most interesting to see whether $SL_n(R)$ has property (T), and we conjecture that this is indeed the case. An affirmative answer would produce first examples of linear Kazhdan groups which are not lattices. In addition, varying the specializations continuously yields non trivial continuous deformations of $SL_n(R)$, a phenomenon which is quite unexpected for Kazhdan groups (compare with [Rap2]). On the other hand, showing that $SL_n(R)$ does not have property (T) would answer negatively van der Kallen's question. It was shown in [Su, 6.6] that for any m the group $SL_n(R)$ is indeed generated by the elementary matrices, and is hence finitely generated (an easy consequence of the Steinberg commutator relations). Finally, notice that $SL_n(R)$ surjects onto lattices as in Corollary 1, but also, by surjecting $\mathbf{Z}$ on finite prime fields, onto lattices in linear groups of positive characteristic. It seems that this "universal lattice" should receive more attention than it had so far in the literature.

Acknowledgments. — This paper was written while visiting Geneva and Neuchâtel Universities. We wish to thank the Swiss National Science Foundation and the Troisième Cycle Romand de Mathématiques, for making these visits possible, and to thank Pierre de La Harpe and Alain Valette, for a most pleasant and productive visit. Thanks are due also to W. van der Kallen and G. Keller, for communicating useful information regarding bounded generation, and to Alain Valette for helpful remarks on the manuscript. The author gratefully acknowledges the NSF support, under grant DMS 9970774.

2. THE CASE OF $\mathrm{SL}_n(\mathbf{Z})$

First, a general remark is in order: For the ring $R = \mathbf{Z}$ (in this section) and other rings (in the next ones), we shall consider various homomorphisms and actions of the group $\mathrm{SL}_2(R)$, some of them coming through the adjoint automorphism $g \to {}^t g^{-1}$. To keep notations simple we will specify this only occasionally. However, as we shall always arrange the (Kazhdan) sets involved to be invariant under this automorphism, this abuse of notation will not interfere with our arguments.

We begin with a detailed analysis of the relative property (T) for the semi-direct product $\mathrm{SL}_2(\mathbf{Z}) \ltimes \mathbf{Z}^2$, with respect to $\mathbf{Z}^2$. The following result was proven by Burger in [Bur]. However, our proof does not involve any analysis on an "ambient group", and in particular no induction operation is applied. This proof will be used, and its idea generalized, in the discussion of a general finitely generated ring, replacing $\mathbf{Z}$.

Theorem **2.1.** — *Denote by* $T^{\pm}$, $S^{\pm} \in \mathrm{SL}_2(\mathbf{Z})$, *the elementary matrices with* ± 1 *above and below the diagonal respectively. Set* $\alpha^{\pm} = (\pm 1, 0)$, $\beta^{\pm} = (0, \pm 1) \in \mathbf{Z}^2$. *Denote by* F *the set of these 8 elements, embedded naturally in* $G = \mathrm{SL}_2(\mathbf{Z}) \ltimes \mathbf{Z}^2$. *Let* $(\pi, \mathcal{H})$ *be a unitary* G*-representation containing a vector which is* $(F, 1/10)$*-invariant (see Definition 1.1). Then* $\mathcal{H}$ *contains a non-zero* $\mathbf{Z}^2$*-invariant vector.*

Proof. — Consider $\pi|_{\mathbf{Z}^2}$ and let P denote the corresponding projection valued measure. Recall that P assigns to every Borel set $B \subseteq \hat{\mathbf{Z}}^2 \cong \mathbf{T}^2$ an orthogonal projection $P(B)$ of $\mathcal{H}$, and satisfies:

(1) For every unit vector v, $\mu_v(B) = \langle P(B)v, v\rangle$ is a probability measure on $\mathbf{T}^2$.
(2) $P(\{0\})$ is the projection on the subspace of $\mathbf{Z}^2$-invariant vectors.
(3) $P(gB) = \pi(g)^{-1} P(B) \pi(g)$ for all $g \in \mathrm{SL}_2(\mathbf{Z})$ and $B \subseteq \mathbf{T}^2$. (Here the action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathbf{T}^2$ is through the adjoint.)

Set $\varepsilon = 1/10$ and let us assume that $v \in \mathcal{H}$ is a unit vector which is (F, ε)-invariant, but there is no $\mathbf{Z}^2$-invariant vector. We argue to obtain a contradiction. Let μ_v denote the corresponding measure on $\mathbf{T}^2$, given by (1). By (2) and our assumption, μ_v has no mass at 0, and so may be viewed as a measure on $\mathbf{T}^2 - \{0\}$. Our strategy will now be as follows: First, identify $\mathbf{T}^2$ with $(-\frac{1}{2}, \frac{1}{2}]^2 \subseteq \mathbf{R}^2$. We will use the fact that v is "almost $\alpha^{\pm}, \beta^{\pm}$-invariant" to deduce that most of the mass of μ_v is contained in $(-\frac{1}{4}, \frac{1}{4})^2$. On the other hand, using (3) we will observe that μ_v is "almost invariant" for the action of $T^{\pm}, S^{\pm}$. The fact that $T^{\pm}, S^{\pm}(-\frac{1}{4}, \frac{1}{4})^2 \subseteq (-\frac{1}{2}, \frac{1}{2})^2$ for the ordinary linear action on $\mathbf{R}^2$, will then imply that there is an "almost invariant" measure for the action of these four matrices on $\mathbf{R}^2 - \{0\}$, which we finally show to be impossible. Of course, we will argue with explicit estimates, making the notion "almost invariant" quantitative.

Recall that v is the assumed $(\mathrm{F}, \varepsilon)$-invariant vector (with $\varepsilon = 1/10$), and that we identify (measurably) $(-\frac{1}{2}, \frac{1}{2}]^2$ with $\hat{\mathbf{Z}}^2$ by assigning to $(x, y) \in (-\frac{1}{2}, \frac{1}{2}]^2$ the character $\chi(n, m) = e^{2\pi i(xn+ym)}$. Denote $\mathrm{X} = (-\frac{1}{4}, \frac{1}{4})^2$.

Claim **1.** — $\mu_v(\mathrm{X}) \geqslant 1 - \varepsilon^2$.

Proof of Claim **1.** — Write $v = \int v_\chi d\mu_v(\chi)$. Recall that for any $z \in \mathbf{Z}^2$ we have $\pi(z)v = \int \chi(z) v_\chi d\mu_v(\chi)$. Therefore, with our identification of $\mathbf{T}^2$ and $(-\frac{1}{2}, \frac{1}{2}]^2$, we have:

$$\text{(i)}\quad \|\pi(\alpha^{\pm})v - v\|^2 = \int_{(-\frac{1}{2}, \frac{1}{2}]^2} |e^{\pm 2\pi i x} - 1|^2 d\mu_v(x, y) \leqslant \varepsilon^2$$

$$\text{(ii)}\quad \|\pi(\beta^{\pm})v - v\|^2 = \int_{(-\frac{1}{2}, \frac{1}{2}]^2} |e^{\pm 2\pi i y} - 1|^2 d\mu_v(x, y) \leqslant \varepsilon^2.$$

(We trust the reader will not confuse the representation π with $\pi = 3.141\ldots$). Since $|e^{\pm 2\pi i t} - 1|^2 = (\cos(2\pi t) - 1)^2 + \sin^2 2\pi t = 2 - 2\cos 2\pi t = 4\sin^2 \pi t \geqslant 2$ for $\frac{1}{4} \leqslant |t| \leqslant \frac{1}{2}$, we get from (i) and (ii):

$$\mu_v(\{\, |x| \geqslant \frac{1}{4} \}) \leqslant \varepsilon^2/2 \qquad \mu_v(\{\, |y| \geqslant \frac{1}{4} \}) \leqslant \varepsilon^2/2. \quad \square$$

Claim **2.** — *For every Borel set* $\mathrm{B} \subseteq \mathbf{T}^2$ *and* $g \in \{\mathrm{T}^{\pm}, \mathrm{S}^{\pm}\}$, *one has:*

$$|\mu_v(g\mathrm{B}) - \mu_v(\mathrm{B})| \leqslant 2\varepsilon.$$

Proof of Claim **2.** — By properties (1) and (3) above we have for every Borel subset $\mathrm{B} \subseteq \mathbf{T}^2$ and $g \in \{\mathrm{T}^{\pm}, \mathrm{S}^{\pm}\}$:

$$\begin{aligned}
&|\mu_v(g\mathrm{B}) - \mu_v(\mathrm{B})| = |\langle \pi(g^{-1})\mathrm{P}(\mathrm{B})\pi(g)v, v\rangle - \langle \mathrm{P}(\mathrm{B})v, v\rangle| \\
&\leqslant |\langle \pi(g^{-1})\mathrm{P}(\mathrm{B})\pi(g)v, v\rangle - \langle \pi(g^{-1})\mathrm{P}(\mathrm{B})v, v\rangle| + |\langle \pi(g^{-1})\mathrm{P}(\mathrm{B})v, v\rangle - \langle \mathrm{P}(\mathrm{B})v, v\rangle| \\
&= |\langle \pi(g^{-1})\mathrm{P}(\mathrm{B})(\pi(g)v - v), v\rangle| + |\langle \mathrm{P}(\mathrm{B})v, (\pi(g)v - v)\rangle| \\
&\leqslant \|\pi(g)^{-1}\mathrm{P}(\mathrm{B})\| \, \|\pi(g)v - v\| + \|\mathrm{P}(\mathrm{B})\| \, \|\pi(g)v - v\| \leqslant \varepsilon + \varepsilon = 2\varepsilon. \quad \square
\end{aligned}$$

Consider now the measure μ on $(-\frac{1}{2}, \frac{1}{2}]^2$ defined by $\mu(\mathrm{B}) = \mu_v(\mathrm{B} \cap \mathrm{X})$. By Claim 1 for every B we have $0 \leqslant \mu_v(\mathrm{B}) - \mu(\mathrm{B}) \leqslant \varepsilon^2$. Fix some $g \in \{\mathrm{T}^{\pm}, \mathrm{S}^{\pm}\}$. From Claim 2 it follows that for every Borel set B:

$$\mu(g\mathrm{B}) - \mu(\mathrm{B}) = (\mu(g\mathrm{B}) - \mu_v(g\mathrm{B})) + (\mu_v(g\mathrm{B}) - \mu_v(\mathrm{B})) + (\mu_v(\mathrm{B}) - \mu(\mathrm{B})) \leqslant 0 + 2\varepsilon + \varepsilon^2.$$

Since this is the case for arbitrary B, we actually have $|\mu(g\mathrm{B}) - \mu(\mathrm{B})| \leqslant 2\varepsilon + \varepsilon^2$. Finally, normalizing μ and using Claim 1 again, we get a probability measure $\nu = \mu/\mu(\mathrm{X})$, supported on $\mathrm{X} - \{0\}$, which satisfies for every Borel subset B and $g \in \{\mathrm{T}^{\pm}, \mathrm{S}^{\pm}\}$:

$$|\nu(g\mathrm{B}) - \nu(\mathrm{B})| \leqslant (2\varepsilon + \varepsilon^2)/(1 - \varepsilon^2) = 21/99 < 1/4 \qquad (\varepsilon = 1/10).$$

Next, notice that for every g as above we have $g\mathrm{X} \subsetneq (-\frac{1}{2}, \frac{1}{2})^2$ for the **ordinary linear action** of g on $\mathbf{R}^2$. Thus, if we now view ν as a measure defined naturally on $\mathbf{R}^2$, we obtain a contradiction to the following general result (whose proof therefore completes the proof of Theorem 2.1):

Lemma **2.2.** — *Let* ν *be a finitely additive probability measure defined on the Borel sets of* $\mathbf{R}^2 - \{0\}$. *Then there exists a Borel set* $\mathrm{Y} \subsetneq \mathbf{R}^2 - \{0\}$ *and* $g \in \{\mathrm{T}^{\pm}, \mathrm{S}^{\pm}\}$, *such that* $|\nu(g\mathrm{Y}) - \nu(\mathrm{Y})| \geqslant 1/4$.

Proof. — The result is proved in [Bur, §4]. For completeness, let us present briefly this nice and easy argument, simplified even further. The reader may benefit from keeping in mind the discussion here when we deal with the case of a general ring in the sequel (compare with Lemma 3.3 below).

Consider the disjoint partition of $\mathbf{R}^2 - \{0\}$ into 8 regions, formed by the lines $x=y$, $x=-y$, $x=0$, $y=0$. Starting from the positive x-axis and going counter clockwise, we denote the regions by A, B, C, D, and then, identifying each point p with $-p$, the regions A, B, C, D repeat. Let us agree that every region is half closed, half open, containing only its boundary going clockwise. It is then easy to check that:

$$\mathrm{T}^{+}(\mathrm{A}\cup\mathrm{B}) \subsetneq \mathrm{A} \qquad \mathrm{S}^{+}(\mathrm{A}\cup\mathrm{B}) \subsetneq \mathrm{B} \qquad \mathrm{T}^{-}(\mathrm{D}\cup\mathrm{C}) \subsetneq \mathrm{D} \qquad \mathrm{S}^{-}(\mathrm{D}\cup\mathrm{C}) \subsetneq \mathrm{C}$$

Now, if a measure ν exists, which contradicts the assertion of the lemma, we would get from the above inclusions that $\nu(\mathrm{B}), \nu(\mathrm{A}), \nu(\mathrm{C}), \mu(\mathrm{D}) < \frac{1}{4}$ respectively. However $\nu(\mathrm{A}) + \nu(\mathrm{B}) + \nu(\mathrm{C}) + \nu(\mathrm{D}) = \nu(\mathrm{A} \cup \mathrm{B} \cup \mathrm{C} \cup \mathrm{D}) = 1$, a contradiction. □

Corollary **2.3.** — *Let* $(\pi, \mathscr{H})$ *be a unitary representation of* $\mathrm{G} = \mathrm{SL}_2(\mathbf{Z}) \ltimes \mathbf{Z}^2$, *and* $\mathrm{F} \subseteq \mathrm{G}$ *be the subset of 8 elements as defined in Theorem 2.1. If* $v \in \mathscr{H}$ *is a unit vector which is* $(\mathrm{F}, \varepsilon/20)$*-invariant for some* $\varepsilon > 0$, *then for* **every** $g \in \mathbf{Z}^2$ *one has* $\|\pi(g)v - v\| \leqslant \varepsilon$.

Proof. — Let $\mathscr{H}_0 \subset \mathscr{H}$ be the subspace of $\mathbf{Z}^2$-invariant vectors and $\mathscr{H}_1$ its orthogonal complement. Since $\mathbf{Z}^2$ is normal in G, both subspaces are G-invariant. Write the corresponding (orthogonal) decomposition $v = v_0 + v_1$. For every $g \in \mathrm{F}$ we then have: $\|\pi(g)v - v\|^2 = \|\pi(g)v_0 - v_0\|^2 + \|\pi(g)v_1 - v_1\|^2 \leqslant \left(\frac{\varepsilon}{20}\right)^2$. However, since there are no non-zero $\mathbf{Z}^2$-invariant vectors in $\mathscr{H}_1$, it follows from Theorem 2.1 that for some $g_0 \in \mathrm{F}$: $(\|v_1\|/10)^2 \leqslant \|\pi(g_0)v_1 - v_1\|^2$. Therefore combining the last two inequalities yields $(\|v_1\|/10)^2 \leqslant (\varepsilon/20)^2$, or $\|v_1\| \leqslant \varepsilon/2$. Finally, for **every** $g \in \mathbf{Z}^2$ we have by the calculation above (recalling that v_0 is g-invariant): $\|\pi(g)v - v\|^2 = \|\pi(g)v_1 - v_1\|^2$, hence $\|\pi(g)v - v\| \leqslant 2\|v_1\| \leqslant \varepsilon$. □

To complete our discussion of $\mathrm{SL}_n(\mathbf{Z})$, we shall need to recall a basic structural fact, which will enable us to apply our foregoing analysis.

Lemma **2.4.** — *Fix an integer* $n \geqslant 3$. *Every elementary matrix* $E_{ij}(t) \in SL_n(\mathbf{Z})$ *(see Definition 1.2) belongs to some copy of a subgroup isomorphic to* $\mathbf{Z}^2$, *contained naturally in the semi-direct product* $SL_2(\mathbf{Z}) \ltimes \mathbf{Z}^2$, *itself embedded in* $SL_n(\mathbf{Z})$. *In fact, the asserted copy of* $SL_2(\mathbf{Z})$ *can always be found along the main diagonal (i.e. occupying the entries* (i, j) *with* $i, j = k, k+1$, *for some* $1 \leqslant k \leqslant n-1$*).*

The same result holds for any commutative ring replacing $\mathbf{Z}$.

Proof. — Although the claim is standard, we give the details of the proof, as properties of the construction will be used in the sequel. For $n = 3$ there are four natural embeddings of $SL_2(\mathbf{Z}) \ltimes \mathbf{Z}^2$ which together contain every elementary matrix. These are the (integral matrices of the) two upper maximal parabolic and two lower maximal parabolic subgroups. The upper parabolic subgroups are those defined by having third row (0, 0, 1), and first column (1, 0, 0). The two lower parabolics can be obtained from the first two by taking their adjoint images (namely, third column (0, 0, 1) and first row (1, 0, 0)). It is easy to check that these subgroups are isomorphic to $SL_2(\mathbf{Z}) \ltimes \mathbf{Z}^2$ and that they provide the copies required in the Lemma.

For a general n we proceed by induction. Given an elementary matrix $E_{ij}(t)$, it is easy to see that if $(i, j) \neq (1, n)$ and $(i, j) \neq (n, 1)$, then $E_{ij}(t)$ is contained in a copy of $SL_{n-1}(\mathbf{Z})$ occupying either the upper or lower $(n-1) \times (n-1)$ principal minor. To deal with the case $(i, j) = (1, n)$ take the natural embedding of $SL_2(\mathbf{Z})$ in the upper left corner of $SL_n(\mathbf{Z})$, and the subgroup generated by $E_{1,n}(t)$, $E_{2,n}(t)$ $(t \in \mathbf{Z})$, which is isomorphic to $\mathbf{Z}^2$. Together they generate a copy of $SL_2(\mathbf{Z}) \ltimes \mathbf{Z}^2$ as required. The case $(i, j) = (n, 1)$ is dealt with similarly (or one can take the adjoint image of the previous construction).

It is clear that the above proof works for any ring replacing $\mathbf{Z}$. □

Finally, we shall need the following general result:

Lemma **2.5.** — *Let* $(\pi, \mathcal{H})$ *be a unitary representation of a group* G. *Suppose that for some unit vector* $v \in \mathcal{H}$, *one has for all* $g \in G$: $\|\pi(g)v - v\| \leqslant 1$. *Then there exists a non-zero* G*-invariant vector in* $\mathcal{H}$.

Proof. — The result follows from [HV, Ch. 3, Cor. 11] (actually, with 1 replaced by any value smaller than $\sqrt{2}$), but we include a proof for completeness. Recall the following well known geometric property of a Hilbert space (in fact, any CAT(0) metric space): For any bounded set $Q \subset \mathcal{H}$ there is a unique point $v_Q \in \mathcal{H}$ ("center of mass"), minimizing the function $f_Q(v) = \sup\{\|v - q\| \mid q \in Q\}$ (see e.g. [HV, 3.8]). Notice that if G acts on $\mathcal{H}$ by isometries then G-invariance of Q implies, by uniqueness, that v_Q is G-invariant as well. With these preliminaries, and the notations of the Lemma, denote $Q = \pi(G)v$. As v_Q is G-invariant, we only need to show that $v_Q \neq 0$. However, this is clear as $f_Q(0) = 1$ and $f_Q(v) \leqslant 1$, so in any case 0 cannot be the unique vector minimizing the function f_Q. □

We are now ready to complete our discussion of $SL_n(\mathbf{Z})$.

Theorem **2.6.** — *Suppose that* $n \geqslant 3$ *and let* $F \subset SL_n(\mathbf{Z})$ *be the set of all* $(n^2 - n)$ *elementary matrices with 1 off the diagonal. Let* $\nu_n = \nu_n(\mathbf{Z})$ *be as in Definition 1.2. (By [CK]:* $\nu_n \leqslant \frac{1}{2}(3n^2 - n) + 51$.*) Then the group* $SL_n(\mathbf{Z})$ *has property* (T)*, with* $(20\nu_n)^{-1}$ *as a Kazhdan constant for the set* F.

Proof. — Since $\|\pi(g)v - v\| = \|\pi(g^{-1})v - v\|$ it is enough to prove the same result when F consists of the elementary matrices with ± 1 off the diagonal, namely, replacing F by $F \cup F^{-1}$. Suppose now that $v \in \mathscr{H}$ is $(F, (20\nu_n)^{-1})$-invariant, and let $g \in SL_n(\mathbf{Z})$ be **any** elementary matrix. By Lemma 2.4 we can find a copy of $SL_2(\mathbf{Z}) \ltimes \mathbf{Z}^2$ inside $SL_n(\mathbf{Z})$ such that $g \in \mathbf{Z}^2$. Furthermore, the proof of Lemma 2.4 shows that such copy can be found intersecting F with a generating set of 8 elements, exactly as in the situation of Corollary 2.3. It then follows from 2.3 that $\|\pi(g)v - v\| \leqslant \nu_n(\mathbf{Z})^{-1}$.

We shall be done by showing that the assumption of Lemma 2.5 holds. Indeed, given any $A \in SL_n(\mathbf{Z})$, write $A = g_0 g_1 \dots g_{\nu_n}$, where $g_0 = I$ is the unit matrix, and all g_i's are elementary. We then have:

$$\pi(A)v - v = \sum_{i=0}^{\nu_n - 1} \pi(g_0 g_1 \dots g_{\nu_n - i})v - \pi(g_0 g_1 \dots g_{\nu_n - i - 1})v$$

$$\|\pi(A)v - v\| \leqslant \sum_{i=0}^{\nu_n - 1} \|\pi(g_0 \dots g_{\nu_n - i})v - \pi(g_0 \dots g_{\nu_n - i - 1})v\| = \sum_{j=1}^{\nu_n} \|\pi(g_j)v - v\| \leqslant \nu_n \cdot \nu_n^{-1} = 1$$

as required. □

3. PROOF OF THE MAIN THEOREM

We now proceed to consider the case of a general finitely generated ring, aiming at the Main Theorem. Our strategy will be similar to that in the case of **Z**, only the details are technically more involved. All the rings discussed hereafter will be assumed commutative and with unit. In order to study the relative property (T) for general finitely generated rings, the following auxiliary, inductive-type result, will be essential.

Theorem **3.1.** — *Suppose that* R *is a discrete ring and that for some finite set* $F \subset SL_2(R) \ltimes R^2$ *and some* $\varepsilon > 0$, (F, ε) *form Kazhdan constants for the relative property* (T)*, namely, for every unitary representation of* $SL_2(R) \ltimes R^2$ *with* (F, ε)*-invariant vector, there is a non-zero* R^2*-invariant vector. Assume also that* F *contains the four elementary matrices of* $SL_2(R)$ *with* ± 1 *off the diagonal. Let* $R[t]$ *denote the ring of polynomials over* R *with variable* t. *The ring* R *is embedded naturally as a subring of* $R[t]$*, which induces an embedding of* $SL_2(R) \ltimes R^2$

in $SL_2(R[t]) \ltimes R[t]^2$. *Let* $0 < \delta < \varepsilon$ *be a real number such that* $(\delta + 2\delta/\varepsilon)/(1 - \delta/\varepsilon) \leqslant \frac{1}{10}$. *Then* (F_t, δ) *form Kazhdan constants for a relative property* (T) *of* $SL_2(R[t]) \ltimes R[t]^2$ *with respect to* $R[t]^2$, *where* F_t *is the union of* F *and the set of four elementary matrices in* $SL_2(R[t])$ *having* $\pm\, t$ *off the diagonal.*

To prove Theorem 3.1 we shall first need to obtain a presentation of the dual group of $R[t]$ (viewed as a discrete abelian group) in a form suitable for our analysis. We thus preface the proof with some general discussion concerning rings of this type.

3.2. The ring $R[t]$ and its dual

Any discrete commutative ring R may be regarded as a discrete abelian (additive) group. Its dual $\widehat{R}$ is defined as the set of all characters $\chi : R \to \mathbf{R}/\mathbf{Z}$ satisfying $\chi(r+s) = \chi(r) + \chi(s)$. Recall that the dual of a discrete group is compact (abelian group) for the topology of pointwise congruence: $\chi_i \to \chi$ iff for all $r \in R$ one has $\chi_i(r) \to \chi(r)$.

Starting with any ring R as above, consider the group K of all formal series $\sum_{n=0}^{\infty} \chi_n t^{-n}$, $\chi_n \in \widehat{R}$. This is an abelian group under the natural "coordinate" addition operation. We put the topology of "coordinate convergence" on K, which is just the product topology coming from its natural identification with $\widehat{R}^{\infty}$. This makes K a compact abelian topological group.

We wish to show that K may be identified with $\widehat{R[t]}$. First we embed it in $\widehat{R[t]}$ by defining

$$(1) \qquad \langle \bar{\chi}, \bar{r} \rangle = \sum_n \langle \chi_n, r_n \rangle \in \mathbf{R}/\mathbf{Z} \qquad \bar{r} = \sum r_n t^n \in R[t], \quad \bar{\chi} = \sum \chi_n t^{-n} \in K$$

where for $r \in R$ and $\chi \in \widehat{R}$, $\langle \chi, r \rangle$ stands for the action of χ on r. Notice that for only finitely many n's one has $r_n \neq 0$, so the sum in (1) is actually a finite sum and hence always defined.

That the above homomorphism into $\widehat{R[t]}$ is indeed an embedding is easy to see: if $\bar{\chi}_0 = \sum \chi_n t^{-n}$ satisfies $\langle \bar{\chi}_0, \bar{r} \rangle = 0$ for all $\bar{r} \in R[t]$, then taking $\bar{r} = r_n t^n$ gives $\langle \chi_n, r \rangle = 0$ for all $r \in R$, i.e. $\chi_n = 0$ for all n. It is also easy to verify that this embedding is continuous (namely, if $\bar{\chi}_n \to 0$ in the topology of K then for every $\bar{r} \in R[t]$ one has $\langle \bar{\chi}_n, \bar{r} \rangle \to 0$), so the image is a (compact and hence) closed subgroup of $\widehat{R[t]}$. Finally, to show that it is actually surjective, and hence an isomorphism, it is enough by Pontrjagin duality, to show that if $\bar{r} \in R[t]$ satisfies $\langle \bar{\chi}, \bar{r} \rangle = 0$ for all $\bar{\chi} \in K$ then $\bar{r} = 0$. Indeed, if $\bar{r}_0 = \sum r_n t^n$ and for all $\bar{\chi}$ of the form $\bar{\chi} = \chi_n t^{-n}$ we have $\langle \bar{\chi}, \bar{r} \rangle = \langle \chi_n, r_n \rangle = 0$, then necessarily $r_n = 0$. Since this holds for all n, necessarily $\bar{r}_0 = 0$.

We thus have an "explicit" description of $\widehat{R[t]}$, which we identify with K. However it will be more convenient to work with a larger group $\tilde{K}$. One may think heuristically of the relation between $\tilde{K}$ and K as that between $\mathbf{R}$ and $\mathbf{R}/\mathbf{Z}$, when the ring R is $\mathbf{Z}$. This point of view will actually be of help in the sequel. $\tilde{K}$ is defined as the group of all "Laurent" (rather than "Taylor") series in t^{-1}, with coefficients in $\hat{R}$, namely, the formal series of the form $\sum_{n=m}^{\infty} \chi_n t^{-n}$, where $m \in \mathbf{Z}$ is **any** integer. K is naturally embedded in $\tilde{K}$, and declaring it an open subgroup makes $\tilde{K}$ a topological abelian group as well. The same formula as in (1) defines a homomorphism of $\tilde{K}$ onto $\widehat{R[t]}$ which, when the latter is identified with K as above, is just truncating the negative components ($n < 0$). Thus, we may identify $\widehat{R[t]}$ with $\tilde{K}$, once two elements of $\tilde{K}$ are identified if their difference has only "negative components".

Next, recall that for any commutative ring S, the abelian group $\hat{S}$ carries a structure of S-module: for $\chi \in \hat{S}$ and $s \in S$ set $s \cdot \chi = \chi \circ s$, where $\chi \circ s(t) = \chi(st)$. The point of the above description of $\widehat{R[t]}$ is that if we know the "R-multiplication" on $\hat{R}$, then we can describe the same for the ring $R[t]$. Indeed, the $R[t]$ multiplication operation on $\widehat{R[t]}$ is given by a natural product formula: for $\overline{r} = \sum r_n t^n$, $\overline{\chi} = \sum \chi_m t^{-m}$, set: $\overline{r} \cdot \overline{\chi} = \sum_{n,m} (r_n \cdot \chi_m) t^{n-m}$ (where $r_n \cdot \chi_m \in \hat{R}$ is the original R-multiplication operation on $\hat{R}$). Here one sees that working in $\tilde{K}$ rather than K is more convenient, as we may have $n - m > 0$. Again, since $r_n \neq 0$ for only finitely many n's, there is no convergence issue in the above expression. To prove that this formula indeed describes the $R[t]$-module structure on $\widehat{R[t]}$, we need to show that for all $\overline{\chi} \in \tilde{K}$ and $\overline{r}, \overline{p} \in \overline{R[t]}$: $\langle \overline{\chi}, \overline{r}\,\overline{p} \rangle = \langle \overline{r}\,\overline{\chi}, \overline{p} \rangle$. By linearity it is enough to check it when $\overline{\chi} = \chi_0 t^{-n}$, $\overline{r} = r_0 t^k$, $\overline{p} = p_0 t^m$. Indeed, then we have

$$\langle \overline{\chi}, \overline{r}\,\overline{p} \rangle = \overline{\chi}(r_0 p_0 t^{k+m}) = \begin{Bmatrix} \chi_0(r_0 p_0) & \text{if } n = k + m \\ 0 & \text{otherwise} \end{Bmatrix}$$

$$\langle \overline{r}\,\overline{\chi}, \overline{p} \rangle = \langle r_0 \chi_0 t^{k-n}, p_0 t^m \rangle = \begin{Bmatrix} r_0\chi_0(p_0) & \text{if } n - k = m \\ 0 & \text{otherwise} \end{Bmatrix} = \langle \overline{\chi}, \overline{r}\,\overline{p} \rangle.$$

Having this established, let us return to the general framework of a commutative discrete ring S with unit. The group $SL_2(S)$ acts by automorphisms on S^2, which induces an action on the dual $\hat{S}^2$: $A \cdot \overline{\chi} = \overline{\chi} \circ A^{-1}$ ($A \in SL_2(S)$, $\overline{\chi} \in \hat{S}^2$). It is a general fact that the dual action of $SL_2(S)$ on $\hat{S}^2$ is given by the adjoint operation: If $A \in SL_2(S)$ and $\overline{\chi} = {}^t(\chi_1, \chi_2) \in \hat{S}^2$ then $A \cdot \overline{\chi} = {}^t A^{-1} \overline{\chi}$, where the multiplication of a matrix in $SL_2(S)$ and a vector in $\hat{S}^2$ is defined by the S-module structure on $\hat{S}^2$. We leave the verification of this easy general fact to the reader. This ends our general discussion of $\widehat{R[t]}$.

With these preliminaries we can now return to the proof of Theorem 3.1.

Proof of Theorem **3.1.** — Let $(\pi, \mathscr{H})$ be a unitary representation of $SL_2(R[t]) \ltimes R[t]^2$ and $v \in \mathscr{H}$ a unit vector which is (F_t, δ)-invariant (see the Theorem for notations). Let $\mathscr{H}_0 \subset \mathscr{H}$ be the subspace of R^2-invariant vectors and $\mathscr{H}_1$ its orthogonal complement. $\mathscr{H}_0$ and $\mathscr{H}_1$ are $SL_2(R) \ltimes R^2$-invariant. Write the corresponding decomposition $v = v_0 + v_1$. Then for all $g \in F$ we have

$$\|\pi(g)v - v\|^2 = \|\pi(g)v_0 - v_0\|^2 + \|\pi(g)v_1 - v_1\|^2 \leqslant \delta^2$$

whereas, since in $\mathscr{H}_1$ there are no R^2-invariant vectors, there exists, by the assumption on F and ε, some $g_0 \in F$ with $\varepsilon^2\|v_1\|^2 \leqslant \|\pi(g_0)v_1 - v_1\|^2$. It follows that $\|v_1\|^2 \leqslant (\delta/\varepsilon)^2$ which implies that $\|v_0\|^2 = \|v\|^2 - \|v_1\|^2 \geqslant 1 - \left(\frac{\delta}{\varepsilon}\right)^2$, and so $\|v_0\| > 1 - \delta/\varepsilon$.

Now, writing $v_0 = v - v_1$ and using the triangle inequality, we get for every $g \in F_t$:

$$\|\pi(g)v_0 - v_0\| \leqslant \|\pi(g)v - v\| + \|\pi(g)v_1 - v_1\| \leqslant \delta + 2\delta/\varepsilon.$$

Normalizing v_0 yields a unit vector $u_0 = v_0/\|v_0\|$ which, by the foregoing discussion, is $(\delta + 2\delta/\varepsilon)/(1 - \delta/\varepsilon)$-invariant, so by the choice of δ: $\|\pi(g)u_0 - u_0\| < 1/10$ for all $g \in F_t$.

Henceforth we shall use freely the results and notations in Section 3.2 above. Consider the restriction of π to $R[t]^2$ and let P denote the associated spectral measure on $\widehat{R[t]}^2$ (see the proof of Theorem 2.1 above). Let $X \subset K^2 \cong \widehat{R[t]}^2$ be the subgroup of elements with no "free component":

$$X = \{ (\overline{\chi}_1, \overline{\chi}_2) \in K^2 \mid \overline{\chi}_i = \chi_1^i t^{-1} + \chi_2^i t^{-2} + \dots \quad (i = 1, 2) \}$$

It is easily verified that P(X) is the orthogonal projection onto the subspace of R^2-invariant vectors (with the natural embedding of R in $R[t]$), so $P(X)u_0 = u_0$. It follows that the measure $\mu_0(B) = \langle P(B)u_0, u_0\rangle$, defined on K, is supported on X. The reader may find it helpful at this point to compare the role played by $X \subset K \subset \widetilde{K}$, and $(-\frac{1}{4}, \frac{1}{4})^2 \subset (-\frac{1}{2}, \frac{1}{2}]^2 \subset \mathbf{R}^2$ respectively, in the proof of Theorem 2.1. Assuming that there are no $R[t]^2$-invariant vectors in $\mathscr{H}$, which implies that $\mu_0\{0\} = 0$, we shall argue to obtain a contradiction.

As in the proof of Claim 2 in Theorem 2.1, the fact that u_0 is $1/10$-invariant implies that for every $g \in F_t \cap SL_2(R[t])$ and every Borel set $B \subset K^2$ one has: $|\mu_0(gB) - \mu_0(B)| < 2 \cdot 1/10 = 1/5$. (The action here is through the adjoint, but again notice that all our sets are invariant under this operation.) Also, similarly to the proof of Theorem 2.1, the action of $SL_2(R[t])$ on K^2 extends naturally to a "linear" action on $\widetilde{K}^2$ (i.e., matrix multiplication over the ring $R[t, t^{-1}]$). If g is any elementary matrix with ± 1 or $\pm t$ off the diagonal, then for this extended action on $\widetilde{K}^2$ we have $gX \subset K^2$. Hence, if we view μ_0 naturally as a measure on $\widetilde{K}^2$ (actually, $\widetilde{K}^2 - \{0\}$), the discussion above and the following claim yield together the required contradiction:

Lemma **3.3.** — *Let*

$$E = \left\{ T^{\pm} = \begin{pmatrix} 1 & \pm t \\ 0 & 1 \end{pmatrix} \quad S^{\pm} = \begin{pmatrix} 1 & 0 \\ \pm t & 1 \end{pmatrix} \right.$$
$$\left. N_u^{\pm} = \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix} \quad N_d^{\pm} = \begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix} \right\}$$

and consider the natural E*-action on* $\tilde{K}^2$ *by matrix multiplication. Then for every finitely additive probability measure* ν *on* $\tilde{K}^2 - \{0\}$, *there is a Borel subset* $Y \subset \tilde{K}^2 - \{0\}$, *and* $g \in E$, *satisfying* $|\nu(gY) - \nu(Y)| \geqslant 1/5$.

Proof. — For an element $0 \neq \chi = \sum_{n=m}^{\infty} \chi_n t^{-n}$ define the "valuation" $v(\chi)$ to be the minimal n for which $\chi_n \neq 0$ (for instance, $v(\chi t^{-2} + \ldots) = 2$). It is easily verified that $v(t\chi) = v(\chi) - 1$ and that $v(\chi_1 + \chi_2) \geqslant \min\{v(\chi_1), v(\chi_2)\}$, with equality if $v(\chi_1) \neq v(\chi_2)$.

Partition $\tilde{K}^2 - \{0\}$ into three disjoint regions:

$$A = \{(\chi_1, \chi_2) | v(\chi_1) > v(\chi_2)\}$$
$$B = \{(\chi_1, \chi_2) | v(\chi_1) = v(\chi_2)\}$$
$$C = \{(\chi_1, \chi_2) | v(\chi_1) < v(\chi_2)\}.$$

Using the above "valuation" properties of v it is now easy to check that:

(i) $T^+(A \cup B) \subseteq C$ (ii) $S^+(C \cup B) \subseteq A$ (iii) $N_u^+(A) \subseteq B$

For instance, let us check (i) (abusing notation, we identify rows and columns through the transpose operation). We have:

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \chi_1 \\ \chi_2 \end{pmatrix} = \begin{pmatrix} \chi_1 + t\chi_2 \\ \chi_2 \end{pmatrix}$$

so if $v(\chi_2) \leqslant v(\chi_1)$ then $v(t\chi_2) = v(\chi_2) - 1 < v(\chi_1)$ and hence $v(\chi_1 + t\chi_2) = v(t\chi_2) < v(\chi_2)$. Similarly, one can easily verify (ii) and (iii).

Suppose now that a measure ν exists, which violates the conclusion of Lemma 3.3. By (ii) we would then have $\nu(C) + \nu(B) < \nu(A) + 1/5$ and since by (iii) $\nu(A) < \nu(B) + 1/5$ we have $\nu(C) + \nu(B) < \nu(B) + 2/5$ or, $\nu(C) < 2/5$. By (i) we deduce: $\nu(A) + \nu(B) < \nu(C) + 1/5 < 3/5$ so altogether we get $\nu(A) + \nu(B) + \nu(C) < 3/5 + 2/5 = 1$, a contradiction. This completes the proof of Theorem 3.1. □

Using Theorem 3.1 we can now establish explicit Kazhdan constants for the relative property (T) of $SL_2(R) \ltimes R^2$, for a general finitely generated ring R.

Theorem **3.4.** — *Fix some integer* $m \geqslant 0$ *and denote by* R_m *the ring* $\mathbf{Z}[x_1, \ldots, x_m]$ *of polynomials over* $\mathbf{Z}$ *with* m *variables. Let* $F \subset SL_2(R_m) \ltimes R_m^2$ *be the subset consisting of the* *four elements* $\{(\pm 1, 0), (0, \pm 1)\} \subseteq R_m^2$ *and the* $4(m+1)$ *elementary matrices of* $SL_2(R_m)$ *with* $\pm 1, \pm x_1, \ldots, \pm x_m$ *off the diagonal. Then every unitary representation of* $SL_2(R_m) \ltimes R_m^2$ *with an* $(F, 2 \cdot (22)^{-m-1})$*-invariant vector, contains a non-zero* R_m^2*-invariant vector.*

Proof. — For $m = 0$ apply Theorem 2.1. To proceed by induction we invoke Theorem 3.1. The only calculation to be verified is that the recursive relation $\dfrac{\delta + 2\delta/\varepsilon}{1 - \delta/\varepsilon} < 1/10$ is satisfied, where $\varepsilon = 2 \cdot 22^{-m}$ and $\delta = 2 \cdot 22^{-m-1}$. □

Corollary **3.5.** — *Let* R *be any topological commutative ring with unit, and* $\alpha_0 = 1, \alpha_1, \ldots, \alpha_m \in R$ *elements which generate a dense subring* $S \subset R$. *Let* $F \subset SL_2(R) \ltimes R^2$ *be the subset described in Theorem 3.4 when replacing the variables* x_i *with the* α_i*'s. Suppose that* $(\pi, \mathscr{H})$ *is a unitary representation of* $G = SL_2(R) \ltimes R^2$, *and* $v \in \mathscr{H}$ *is a unit vector which is* $(F, \varepsilon \cdot 22^{-m-1})$*-invariant for some* $\varepsilon > 0$. *Then, for* **every** $g \in R^2$ *one has* $\|\pi(g)v - v\| \leqslant \varepsilon$.

Proof. — The map which sends $1, x_1, \ldots, x_m \in R_m$ to $1, \alpha_1, \ldots, \alpha_m \in S \subset R$ resp., extends canonically to a surjective ring homomorphism $R_m \to S$, which induces a group homomorphism:

$$\varphi \colon SL_2(R_m) \ltimes R_m^2 \to SL_2(S) \ltimes S^2 \subseteq SL_2(R) \ltimes R^2.$$

Let $\mathscr{H}_0 \subset \mathscr{H}$ denote the subspace of R^2-invariant vectors and $\mathscr{H}_1 \subset \mathscr{H}$ its orthogonal complement. Write $v = v_0 + v_1$, the corresponding decomposition. Notice that by the density of S in R there are no non-zero S^2-invariant vectors for the representation of $SL_2(S) \ltimes S^2$ on $\mathscr{H}_1$, and hence also for that of $SL_2(R_m) \ltimes R_m^2$ acting through φ. Therefore, from Theorem 3.4 it follows that there exists some $g_0 \in F$ for which $2 \cdot 22^{-m-1}\|v_1\| \leqslant \|\pi(g_0)v_1 - v_1\|$. On the other hand, by the assumption:

$$\|\pi(g_0)v - v\|^2 = \|\pi(g_0)v_0 - v_0\|^2 + \|\pi(g_0)v_1 - v_1\|^2 \leqslant (\varepsilon \cdot 22^{-m-1})^2$$

hence

$$(2 \cdot 22^{-m-1} \cdot \|v_1\|)^2 \leqslant (\varepsilon \cdot 22^{-m-1})^2 \quad \text{or} \quad \|v_1\| \leqslant \varepsilon/2.$$

Finally, repeating the calculation above for any $g \in R^2$ and using the fact that v_0 is g-invariant, yields $\|\pi(g)v - v\| = \|\pi(g)v_1 - v_1\| \leqslant 2\|v_1\| \leqslant \varepsilon$, as required. □

We can now easily prove the Main Theorem, stated in the introduction.

Proof of the Main Theorem. — The proof is similar to that of Theorem 2.6. The main auxiliary result here is Corollary 3.5, which replaces Corollary 2.3. Lemma 2.4 applies to any ring R, and its proof shows that the matrices involved in the copies of $SL_2(R) \ltimes R^2$, which together contain every elementary matrix, are exactly those of the set $F_1 \cup F_2$ in the theorem. As for the final assertion of the theorem, if

$(\pi, \mathscr{H})$ is a continuous representation of $SL_n(R)$, and $v \in \mathscr{H}$ is a unit vector, take a neighborhood U of $0 \in R$ such that for any elementary matrix $E_{i,j}(t)$ with $t \in U$: $||\pi(E_{i,j}(t))v - v|| < \varepsilon = \nu_n(R)^{-1}22^{-m-1}$. Then, if π has no non-zero fixed vector, by the first part of the Main Theorem there must be some $g \in F_1$ with $||\pi(g)v - v|| \geqslant \varepsilon$, as required. □

4. APPLICATIONS OF THE MAIN THEOREM

In this section we establish the corollaries to the Main Theorem, stated in the introduction. In light of the Main Theorem, their proof relies on a bound on ν_n. Corollary 1 follows, as indicated in the introduction, from the results of [CK], whereas Corollary 5 is a straightforward application of the Main Theorem, so we only need to discuss Corollaries 2, 3 and 4. To prove Corollaries 2 and 3 it clearly suffices to show the following:

Theorem **4.1.** — *If* R *is a ring as in Corollary 2 or 3, then* $\nu_n(R) \leqslant 5n^2$.

We preface the proof of 4.1 by considering first the simplest example of a ring for which SL_n is boundedly elementary generated, namely, a field. That $SL_n(F)$, where $n \geqslant 2$ and F is any (abstract) field, has this property, is a completely elementary fact which follows from the Gauss elimination process. In fact we shall need the following:

Lemma **4.2.** — *Let* $\{F_\alpha\}_{\alpha \in I}$ *be a set of (abstract) fields. Consider their direct product:* $R = \prod_\alpha F_\alpha$ *(with the pointwise operations). Then* $\nu_n(R) \leqslant \frac{1}{2}(3n^2 - n)$.

Proof. — We shall prove that any field F satisfies $\nu_n(F) \leqslant \frac{1}{2}(3n^2 - n)$. In fact, the actual value is less than this estimate, and our proof will be somewhat expensive. However, the point of this proof is that the order and type of elementary matrices E (i.e. the (i, j) such that $E = E_{ij}(t)$) which appear in the decomposition of a general matrix, **do not** depend on the given matrix, only the values of the entries t. We will actually consider the elementary operations on the rows and columns needed to transform a general matrix to the identity one. Then, for a general ring R of the above type we have $SL_n(R) \cong \prod_\alpha SL_n(F_\alpha)$, and we can transform any matrix to the identity by performing simultaneously the elementary operations in all the $SL_n(F_\alpha)$ (where the value of the entry t_α will of course depend on α).

Given a matrix $A \in SL_n(F)$, add to the last row a multiple of the first one, then a multiple of the second, and so on, until the $n-1$ row. Since the first column is not all zeros we can always find scalars such that this process yields a non-zero element in the entry $(n, 1)$ (notice that the type and order of operations do not depend on A, only the scalars). Using one more elementary operation: adding a multiple of the first column to the last one, we can arrange to have 1 in the entry (n, n). Using this we now perform $n-1$ elementary operations which annihilate the first $n-1$ elements in the last row, and then $n-1$ operations which do the same for the last column. Altogether, we have used $(n-1)+1+(n-1)+(n-1)=3n-2$ operations in a fixed type and order, to get a matrix with zero entries in the last row and column, except for the entry (n, n) which is 1. Now continue the process by induction to get the identity matrix. The number of operations used is at most $\Sigma_{k=n}^{1}(3k-2)=\frac{1}{2}(3n^2-n)$, thereby proving Lemma 4.2. □

Aiming at Corollary 2, we shall also need the following:

Proposition **4.3.** — *Let* R *be a compact topological commutative ring with unit. Suppose that* R *contains a finitely generated dense subring* S. *Then every non invertible element* $x \in \mathrm{R}$ *is contained in a (proper) maximal ideal, which is* **closed**.

The proof of Proposition 4.3 is based on the following:

Lemma **4.4.** — *With the notations of 4.3, let* $\mathrm{I} \lhd \mathrm{R}$ *be a closed ideal, and* $x \in \mathrm{R}$ *with* $\mathrm{I}+\mathrm{R}x \neq \mathrm{R}$. *Then there exist finitely many elements* $s_1, \dots, s_n \in \mathrm{S}$ *such that* $\mathrm{I}+\mathrm{R}x \subseteq \mathrm{I}+\mathrm{R}s_1+\dots+\mathrm{R}s_n \neq \mathrm{R}$.

Proof of **4.4.** — Denote $\mathrm{I}_0=\mathrm{I}+\mathrm{R}x$ and $\pi_0 : \mathrm{R} \to \mathrm{R}/\mathrm{I}_0$ the canonical projection. Let $\{\mathrm{U}_n\}$ form a base for the neighborhoods of x in R (by the assumption on S, R is second countable). There exists some $s_1 \in \mathrm{U}_1 \cap \mathrm{S}$ such that $\pi_0(s_1)$ is not invertible. Indeed, otherwise, we would get a sequence $s_i \to x$ such that $\pi_0(s_i)$ are invertible, but $\pi_0(s_i) \to \overline{0}$, so then any limit point $\overline{r}$ of the sequence of elements $\overline{r_i} \in \mathrm{R}/\mathrm{I}_0$ satisfying $\overline{r_i}\,\pi_0(s_i)=\overline{1}$, satisfies $\overline{r}\,\overline{0}=\overline{1}$, a contradiction. Denote $\mathrm{I}_1=\mathrm{I}_0+\mathrm{R}s_1 \neq \mathrm{R}$ and let $\pi_1 : \mathrm{R} \to \mathrm{R}/\mathrm{I}_1$. As before, we may find $s_2 \in \mathrm{U}_2 \cap \mathrm{S}$ such that $\mathrm{I}_2=\mathrm{I}_0+\mathrm{R}s_1+\mathrm{R}s_2 \neq \mathrm{R}$, and continuing this process yields a sequence $s_n \in \mathrm{S}$, $s_n \to x$, satisfying $\mathrm{I}_0+\mathrm{R}s_1+\dots+\mathrm{R}s_n \neq \mathrm{R}$ for every n. Recall that by Hilbert's basis theorem S is Noetherian, namely, every ideal is finitely generated. In particular, the ideal $\mathrm{S}s_1+\mathrm{S}s_2+\dots \lhd \mathrm{S}$ is finitely generated, say, by $s_1, \dots, s_k$. It follows that the ideal $\mathrm{J}=\mathrm{R}s_1+\mathrm{R}s_2+\dots=\mathrm{R}s_1+\dots+\mathrm{R}s_k$ is closed (as each $\mathrm{R}s_i$ is compact). Also, $\mathrm{J} \neq \mathrm{R}$ by the construction of the s_i's. On the other hand, since $s_i \to x$ clearly $x \in \overline{\mathrm{J}}=\mathrm{J}$. Therefore $\mathrm{I}+\mathrm{J}$ is the required ideal. □

Proof of **4.3.** — It follows from lemma 4.4, taking $\mathrm{I}_0=0$, that there exist $s_1, \dots, s_k \in \mathrm{S}$ such that $x \in \mathrm{J}=\mathrm{R}s_1+\dots\ \mathrm{R}s_k \neq \mathrm{R}$. Consider now increasing chains of proper ideals containing J and generated by elements of S, and take, by Zorn's lemma, a maximal element I. As S is Noetherian, I is finitely generated, and hence closed. We claim that I is maximal. Indeed, otherwise there exists some $y \in \mathrm{R}$ with $\mathrm{I}+\mathrm{R}y \neq \mathrm{R}$, but then Lemma 4.4 contradicts the maximality of I. □

With these preliminaries, we can now prove Theorem 4.1.

4.5. *Proof of Theorem 4.1 for the case* R *compact.* — First notice that we may assume that R contains a finitely generated dense subring (in fact, a ring generated by n^2 elements). This is so since for any $A \in SL_n(R)$ it is enough to consider the ring S generated by the n^2 entries of A, and replace R by $\overline{S}$.

Next, let $\{I_\alpha\}$ denote the set of all maximal closed ideals in R, and $I = \cap I_\alpha$. Then for every α the quotient R/I_α is a field F_α, and we have a canonical continuous ring homomorphism $\varphi: R \to \Pi F_\alpha$. By the Chinese remainder theorem the image of R is dense in ΠF_α (for the product topology). However, as R is compact, the image is also closed, hence φ is onto, and induces an isomorphism $\tilde{\varphi}: R/I \to \Pi F_\alpha$.

Now, given any $A \in SL_n(R)$ we use the discussion above and Lemma 4.2 to transform A, using $\frac{1}{2}(3n^2 - n)$ elementary operations, into a matrix B which satisfies $B \equiv I_n \bmod I$ (I_n stands for the unit $n \times n$ matrix). In particular, the diagonal of B has entries of the form $1 + u$, with $u \in I$. However such a diagonal element is invertible, for if it weren't, by Proposition 4.3 we could find a closed maximal proper ideal $J \lhd R$ containing $1 + u$. But by definition $u \in J$, so $1 \in J$, a contradiction. Thus, the matrix B has invertible elements in its diagonal, so $n - 1$ elementary operations in each of the n rows transform it into a diagonal matrix. It is an easy exercise to check that every diagonal $n \times n$ (determinant one) matrix is a product of $4(n-1)$ elementary matrices (4 are needed for SL_2, repeat the process $n - 1$ times). This shows that $\nu_n(R) \leqslant \frac{1}{2}(3n^2 - n) + n(n-1) + 4(n-1) < 5n^2$. □

4.6. *Proof of Theorem 4.1 for the ring* $R((t))$. — The idea here is similar to that in 4.5, only the proof is technically much more simple. This is because the ring $R((t))$ has only finitely many maximal ideals (all closed), which are actually easy to describe: these are exactly the ideals of the form $I((t))$, where I is a maximal ideal of R. Indeed, on one hand, for an ideal of this form one has $R((t))/I((t)) \cong (R/I)((t))$, which is a field since R/I is, hence $I((t))$ is maximal. In the other direction, let $J \lhd R((t))$ be a maximal ideal, and $\varphi: R((t)) \to R((t))/J \cong F$ be the projection from $R((t))$ to a field F. $\varphi(R)$ is a finite subring of a field, hence a subfield, so for some maximal ideal $I \lhd R$ we have $J \supseteq I$. Since J is an ideal we must have $J \supseteq I((t))$. However we saw that $I((t))$ is already maximal, so $J = I((t))$ as required.

At this point we may repeat the whole argument as in 4.5 above. Since there are only finitely many maximal ideals I_α, we do not need the compactness of R to deduce that $R/\cap I_\alpha$ is isomorphic to a direct sum of fields, the Chinese remainder theorem suffices. The rest of the proof in 4.5 goes through, hence our result. □

Let us now discuss Corollary 4. First, notice that if X is any topological space and $G = SL_n(\mathbf{C})$, then G^X, the group of continuous maps from X to G, is naturally isomorphic to the group $SL_n(R)$, where R is the ring of continuous functions $f: X \to \mathbf{C}$ (with the pointwise addition and multiplication operations). For Corollary 4 we are interested in the case $X = S^1$ (later we will also discuss the case where X is totally disconnected). Let us denote this ring by R. First notice that R has a finitely generated dense subring, namely, the ring generated by $\sin 2\pi x$, $\cos 2\pi x$ and, say, $\sqrt{2}+i$ (that the first two, together with $\mathbf{C}$, generate a dense subring, is just the Stone-Weierstrass theorem, but the ring generated by $\sqrt{2}+i$ is dense in $\mathbf{C}$). In fact, considering $\frac{sin 2\pi x}{n}, \frac{cos 2\pi x}{n}, \frac{\sqrt{2}+i}{n}$, we see that the condition in the last assertion of the Main Theorem holds as well (with $m=3$). Thus, in order to complete the proof of Corollary 4 it suffices to show the following:

Proposition **4.7.** — *For $n \geqslant 2$ and the ring* R *above, one has* $v_n(\mathrm{R}) \leqslant \frac{3}{2}n^2$.

Proof. — The proof of Proposition 4.7 is based on the following topological fact:

Lemma **4.8.** — *Let $f, h\colon \mathrm{S}^1 \to \mathbf{C}$ be two continuous functions with no common zero. Then there exists a continuous function $\varphi\colon \mathrm{S}^1 \to \mathbf{C}$ such that $h+\varphi f$ has no zero.*

Let us first see how 4.7 follows from 4.8. Let $\mathrm{A} \in \mathrm{SL}_n(\mathrm{R})$ be any matrix (R as above) and $f_1, \dots, f_n$ its first row. Because $\det \mathrm{A} = 1$, the f_i's have no common zero. Therefore, also the functions $f = |f_1|^2 + \dots + |f_{n-1}|^2$ and $h = f_n$ have no common zero. Let $\varphi\colon \mathrm{S}^1 \to \mathbf{C}$ be as in 4.8 for the functions f and h above. Now perform the following $n-1$ elementary operations on A: first add to the last column the first column multiplied by $\varphi \cdot \bar{f}_1$, then add to it the second multiplied by $\varphi \cdot \bar{f}_2$ and so on, until the $n-1$ column. After these $n-1$ operations we obtain a non vanishing, hence invertible, continuous function on S^1 as the entry $(1, n)$, so by one more elementary operation we can generate the constant function 1 in the entry (n, n). Using $(n-1)+(n-1)$ more operations we then annihilate the rest of the last row and last column, so altogether we have used $(n-1)+1+(n-1)+(n-1) = 3n-2$ operations to reduce the problem from a general $n \times n$ matrix to a $(n-1) \times (n-1)$ matrix. Thus, to transform A to I at most $\sum_{k=n}^{1} 3k-2 \leqslant \frac{3}{2}n^2$ operations are required.

Thus, to complete the proof of 4.7, and hence of Corollary 4, we are left with the proof of 4.8.

Proof of Lemma **4.8.** — The claim is a rather easy exercise and thus we only sketch here the proof. Consider the function $\psi = -h/f$. If f does not vanish then ψ is defined everywhere, so any φ which is different from ψ for all x will do (e.g. $\varphi = \psi + 1$). Of course, f may vanish, but since it does not vanish together with h, it is easy to see that as a function to the one point compactification $\mathbf{C} \cup \{\infty\} \cong \mathrm{S}^2$ (where $\frac{a}{0} = \infty$), ψ is well defined and continuous. Thus, we need only to verify the following fact: Let S^2 be the two dimensional sphere, and $\infty \in \mathrm{S}^2$ a point. Then for every continuous $\psi\colon \mathrm{S}^1 \to \mathrm{S}^2$ there exists a continuous $\varphi\colon \mathrm{S}^1 \to \mathrm{S}^2$ such that for every x both

$\varphi(x) \neq \infty$ and $\varphi(x) \neq \psi(x)$. We sketch the idea of proof. Fix two points $p, q \in S^2 - \{\infty\}$ and suppose their distance from each other, from ∞, and from $\psi(0) = \psi(1)$ is greater than 2. Let B_p, B_q denote the balls of radius 1 around p, q resp. The idea of the construction of φ is as follows: For most of the time the path φ will be fixed at p or q, and will move rapidly between p and q whenever ψ gets close to one of them. More precisely, at $t = 0$ we put $\varphi = p$ and wait until ψ "touches" B_p for the first time. It then takes ψ a certain time, in which it must stay within a ball of radius $\frac{1}{2}$ around the touching point, and in that time φ will escape quickly to q, avoiding that ball and ∞. Based on the uniform continuity of ψ, this process repeats finitely many times and may easily be used to define a continuous function φ as required. The details are left to the reader. □

Notice that the above proof does not apply if we replace $\mathbf{C}$ by $\mathbf{R}$, and Lemma 4.8 is false in that case. In fact, if we replace $\mathbf{C}$ by $\mathbf{R}$ it is no longer true that every matrix in $SL_n(R)$ is a product of elementary matrices, since $\pi_1(SL_n(\mathbf{R})) \neq \{e\}$ and it is not difficult to see that every $\psi: S^1 \to SL_n(\mathbf{R})$ which is a product of elementary matrices must be null homotopic. Put in a different language, the loop group associated with $SL_n(\mathbf{R})$ is not connected, and the connected component is exactly the subgroup generated by the elementary matrices. A different phenomenon occurs with the Lie group $SO(n, 2)$ for $n \geqslant 3$. This group has property (T) and an infinite (abelian) fundamental group. Thus, its Loop group cannot have property (T), as its quotient by the connected component is isomorphic to $\pi_1(SO(n, 2))$. In both of the above examples it would be interesting to see whether the connected component of the Loop group has property (T). One may also study in general the case where S^1 is replaced by other manifolds, say, a higher dimensional sphere S^d (here higher homotopy groups form obstructions to elementary generation).

We conclude with a brief discussion of the group G^X when $G = SL_n(\mathbf{Q}_p)$, and X is a Cantor set ($\mathbf{Q}_p$-the field of p-adic numbers, may be replaced here by any non-archimedean local field).

Theorem **4.9.** — *With the above notations, the group* G^X *satisfies the assumptions of the Main Theorem, and hence has property* (T).

Proof. — As in the foregoing discussion we may identify G^X with $SL_n(R)$, where R is the ring of continuous functions $\varphi: X \to \mathbf{Q}_p$. We identify X with $\mathbf{Z}_p \subseteq \mathbf{Q}_p$, the ring of p-adic integers. By an elementary fact (attributed in [Sch, p. 127] to Kaplansky, but was apparently proved first by Dieudonné [Di], as was pointed out to us by J.-P. Serre), the subring of polynomials with coefficients in $\mathbf{Q}_p$ is dense in R (for the uniform convergence topology). Thus, the subring $S \subset R$ generated by the function $f(x) = x$ and the constant function $1/p$ is dense. Hence we only need to verify bounded elementary generation. For this we first need to show that Lemma 4.8 holds if S^1 is replaced by X, and $\mathbf{C}$ by $\mathbf{Q}_p$. The proof of this elementary fact is easier than that of 4.8 and is left to the reader. Let us indicate how it implies $\nu_n(\mathrm{R}) \leqslant \frac{3}{2}n^2$, which then completes the proof.

First, notice that the above modification of Lemma 4.8 implies that for **any** two continuous functions $f, h\colon \mathrm{X} \to \mathbf{Q}_p$, there exists a continuous φ such that $h+\varphi f$ vanishes **exactly** in the set of common zeroes of h and f. Indeed, denote by $\mathrm{Y} \subseteq \mathrm{X}$ the closed set of common zeroes and let $\mathrm{Y} \subseteq \ldots \mathrm{U}_2 \subset \mathrm{U}_1 \subset \mathrm{U}_0 = \mathrm{X}$ be a decreasing sequence of open-closed subsets with $\cap \mathrm{U}_n = \mathrm{Y}$. Then for every $n \geqslant 0$, h and f have no common zero in $\mathrm{U}_n - \mathrm{U}_{n+1}$ (which is closed and open) and hence there is a continuous function φ_n on $\mathrm{U}_n - \mathrm{U}_{n+1}$ such that $h + \varphi_n f$ has no zero there. Extending φ_n to be zero outside $\mathrm{U}_n - \mathrm{U}_{n+1}$, $\varphi(x) = \sum \varphi_n(x)$ is a function as required.

Now let $\mathrm{A} \in \mathrm{SL}_n(\mathrm{R})$ and denote by $f_1, \ldots, f_n$ its first row. By the above there exists a continuous function $\varphi_1\colon \mathrm{X} \to \mathbf{Q}_p$ such that $f_2 + \varphi_1 f_1$ vanishes exactly in the common zeroes of f_1 and f_2. Correspondingly, add the first column multiplied by φ_1 to the second. Now let φ_2 be such that $f_3 + \varphi_2(f_2 + \varphi_1 f_1)$ vanishes exactly on the set of common zeroes of f_1, f_2 and f_3. Correspondingly, add the second column multiplied by φ_2 to the third one. Continuing this process and using $\det \mathrm{A} = 1$, we get after $n-1$ elementary operations an invertible function in the n-th entry of the first row. One more operation yields the constant 1 in the (n, n) entry, and the rest of the argument is identical to that in Proposition 4.7. □

REFERENCES

[AM] S. I. Adian and J. Mennicke, On bounded generation of $\mathrm{SL}_n(\mathbf{Z})$, *Inter. Jour. Alg. and Comp.*, Vol. 2, No. **4** (1992), 357-365.

[BMS] H. Bass, J. Milnor and J. P. Serre, Solution of the congruence subgroup problem for SL_n $(n \geqslant 3)$ and Sp_{2n} $(n \geqslant 2)$, *IHES Publ.*, **33** (1967), 59-137.

[Bur] M. Burger, Kazhdan constants for $\mathrm{SL}_3(\mathbf{Z})$, *J. Reine Angew. Math.*, **413** (1991), 36-67.

[CK] D. Carter and G. Keller, Bounded elementary generation of $\mathrm{SL}_n(\mathcal{O})$, *Amer. J. Math.*, **105** (1983), 673-687.

[CW] G. Cooke and P. Weinberger, On the constructions of division chains in algebraic number fields, with applications to SL_2, *Comm Alg*, **3** (1975), 481-524.

[Di] J. Dieudonné, Sur les fonctions continues p-adiques, *Bull. Sci. Math.* (2), **68** (1944), 79-95.

[HRV] P. de La Harpe, A. G. Robertson, A. Valette, On the spectrum of the sum of generators for a finitely generated group, *Israel J. of Math.*, **81** (1993), No. 1-2, 65-96.

[HV] P. de La Harpe and A. Valette, La Propriété (T) de Kazhdan pour les Groupes Localement Compacts, *Astérisque*, **175**, Société Math. de France (1989).

[Is] R. S. Ismagilov, Representations of Infinite-Dimensional Groups, Translations of Mathematical Monographs, **152**, *Amer. Math. Soc.*, Providence (1996).

[Kal] W. van der Kallen, $\mathrm{SL}_3(\mathbf{C}[x])$ does not have bounded word length. Proceedings of the conference on Algebraic K-theory (Oberwolfach, 1980), *Lecture Notes in Math.*, **966** (1982), 357-361.

[Kaz] D. A. Kazhdan, On a connection between the dual space of a group and the structure of its closed subgroups, *Func. Anal. Appl. 1* (1967), 63-65.

[Lub1] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Birkhäuser, 1994.

[Lub2] A. Lubotzky, Subgroup growth and congruence subgroups, *Invent. Math.*, **119** (1995), 267-295.

[Mok] N. MOK, Harmonic forms with values in locally constant Hilbert bundles, *Proceeding of the conference in honor of J. P. Kahane (Orsay 1993), J. Fourier Anal. Appl.* (special issue), (1995), 433-453.

[Mu] V. K. MURTY, Bounded and finite generation of arithmetic groups, *Canadian Mathematical Society Conference Proceedings*, Vol. **15** (1995), 249-261.

[MSY] N. MOK, Y. T. SIU and S.-K. YEUNG, Geometric superrigidity, *Invent. Math.*, **113** (1993), 57-83.

[Pa] P. PANSU, Formules de Matsushima, de Garland et propriété (T) pour des groupes agissant sur des espaces symétriques ou des immeubles, *Bull. Soc. Math. France*, **126** (1998), 107-139.

[PR] V. PLATONOV and A. RAPINCHUK, Abstract properties of S-arithmetic subgroups and the congruence subgroup problem, *Izve. R. Acad. Sci. Ser. Math. (former Math. USSR Izvestiya)*, **56** (1992), 483-508.

[PS] A. PRESSLEY and G. SEGAL, Loop Groups, *Oxford Mathematical Monographs*, 1988.

[Rag] M. S. RAGHUNATHAN, On the congruence subgroup problem, *IHES Publ.*, **46** (1976), 107-161.

[Rap1] A. RAPINCHUK, Congruence subgroup problem for algebraic groups: old and new, *Astérisque*, **209** (1992), 73-84.

[Rap2] A. RAPINCHUK, On the finite dimensional unitary representations of Kazhdan groups, *Proc. of AMS*, **127**, No. 5 (1999), 1557-1562.

[Rap3] A. RAPINCHUK, On SS-rigid groups and A. Weil's criterion for local rigidity I, *Manuscripta Math.*, **97** (1998), 529-543.

[Sch] W. H. SCHIKHOF, Ultra Calculus: An Introduction to p-Adic Analysis, *Cambridge Studies in Advanced Mathematics 4*, 1984.

[Sh1] Y. SHALOM, Explicit Kazhdan constants for representations of semisimple and arithmetic groups, *Ann. Inst. Fourier (Grenoble)*, **50** (2000) No 3, 833-863.

[Sh2] Y. SHALOM, Harmonic maps, superrigidity, and property (T), preprint.

[Su] A. A. SUSLIN, On the structure of the special linear group over polynomial rings, *Math. USSR Izv.*, Vol. **11** (1977), 221-238.

[Tav] O. I. TAVGEN, Bounded generation of Chevalley groups over rings of algebraic S-integers, *Math. USSR Izv.*, **36** (1991), 101-128.

[VGG] A. M. VERSHIK, M. I. GRAEV and I. M. GELFAND, Representations of the group SL(2,R), where R is a ring of continuous functions, *Russ. Math. Surv.*, **28** (5) (1973), 87-132.

Department of Mathematics,
Princeton University.
Current Address: Department of Mathematics,
Yale University.
E-mail address: yshalom@math.yale.edu
Current address:
Department of Mathematics,
The Hebrew University
E-mail address: yehuda@math.huji.ac.il

Manuscrit reçu le 23 février 1999.