Théorie des groupes / Group Theory

CYCLIC SUBGROUPS OF EXPONENTIAL GROWTH AND METRICS ON DISCRETE GROUPS

ALEXANDER LUBOTZKY, SHAHAR MOZES,
M.S. RAGHUNATHAN

ABSTRACT. Let G be a semisimple Lie group of rank ≥ 2 and Γ an irreducible lattice. A cyclic subgroup of Γ has exponential growth with respect to the generators of Γ if and only if it is virtually unipotent. This is used to prove that the word metric of Γ is Lipschitz equivalent to the metric induced by the Riemannian metric of G. This confirms a conjecture of D. Kazhdan (cf. Gromov [1]).

SOUS-GROUPES CYCLIQUES DE CROISSANCE EXPONENTIELLE ET MÉTRIQUES SUR LES GROUPES DISCRETS

RÉSUMÉ. Soit G un groupe de Lie semisimple de rang≥ 2, et Γ un réseau irréductible (dans G). Un sous groupe cyclique de Γ est de croissance exponentielle par rapport aux générateurs de Γ si et seulement si il est virtuellement unipotent. Ceci sert à montrer que la métrique des mots de Γ est équivalente, au sens Lipschitzien, à la métrique induite par la métrique Riemannienne de G. Ceci démontre une conjecture de D. Kazhdan (cf. Gromov [1]).

Version française abrégée. Soit G un groupe semisimple linéaire et d_R un distance Riemannienne invariante par translation à gauche sur G. Soit Γ un réseau dans G engendré par une partie finie Σ. Le graphe de Cayley de Γ par rapport à Σ induit sur Γ une métrique, la métrique des mots d_W. Bien sûr cette métrique dépend de Σ, mais sa classe d'équivalence au sens de Lipschitz n'en dépend pas. Si Γ est cocompact dans G, c'est un resultant facile et bien connu que la restriction de d_R est équivalente à d_W au sens Lipschitzien. Ce n'est pas toujours le cas si Γ est un réseau non uniforme (c-à-d de covolume fini mais non cocompact). Par éxample soient $G = SL_2(\mathbb{R})$ et $\Gamma = SL_2(\mathbb{Z})$ alors si $u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$, $d_W(u^n, 1)$ est de croissance linéaire en n tandis que $d_R(u^n, 1) = O(\log n)$.

$SL_2(\mathbb{R})$ est un groupe de rang un. D'autre part:

Théorème A. *Si G est un groupe de Lie semisimple de rang ≥ 2 est Γ un réseau irrèductible dans G, alors la réstriction à Γ de d_R est equivalente au sens Lipschitzien à d_W.*

Un réseau Γ dans G est irréductible si $N\Gamma/N$ n'est discret pour aucun sous-groupe fermé distingué infini de G. Le Théorème A à èté conjecturé par D. Kazhdan. M. Gromov [1 §3] le démontre pour $G = \underline{G}(\mathbb{R})$ et $\Gamma = \underline{G}(\mathbb{Z})$, où $\underline{G}$ est un groupe $\mathbb{Q}$-algébrique de $\mathbb{Q}$-rang un et $\mathbb{R}$-rang ≥ 2.

1991 *Mathematics Subject Classification.* 22E40, 20F32.

The authors acknowledge support from MSRI, University of Chicago, Hebrew University and Tata Institute for some mutual visits which enabled the work.

D'après le Théorème A, si nous considérons l'inclusion de SL_2 dans SL_3 au coin gauche supérieur, et u est comme ci-dessus alors $d_W(u^n, 1) = O(\log n)$ où d_W est la métrique des mots de $SL_3(\mathbb{Z})$, donc u^n est representé par un mot de longueur $O(\log n)$ dans les générateurs de $SL_3(\mathbb{Z})$.

Définition. *1) Un élément γ d'ordre infini dans un groupe Γ de génération fini est un élément U1 si $d_w(u^n, 1) = O(\log n)$.*
2) $\gamma \in \Gamma$ est élément U2 de Γ si $|B_n(1) \cap < \gamma >|$ est de croissance exponentielle, où $B_n(1)$ est la boule par rapport à d_W de rayon n et centre l'élément neutre 1 de Γ. En d'autre termes le groupe cyclique $< \gamma >$ engendré par γ est de croissance exponentielle par rapport aux générateurs de Γ.

Il est évident que U1 entraine U2 - mais la réciproque est sans doute fausse pour un groupe arbitraire de génération fini. Si Γ est un groupe linéaire et γ est un élément U1 ou U2, il n'est pas difficile à voir que γ est virtuellement unipotent, c-à-d qu'il existe un puissance de γ qui est unipotente. L'élément $u \in SL_2(\mathbb{Z})$ montre que la réciproque n'est pas toujours vraie; mais le Théorème A montre que u est un élément U1 de $SL_3(\mathbb{Z})$. De façon plus générale, nous avons le résultat suivant:

Théorème B. *Soit G un groupe de Lie semisimple linéaire et Γ un réseau irréductible de G. Pour $\gamma \in \Gamma$ les conditions suivantes sont équivalentes.*

(i) *γ est un élément U1 de Γ.*
(ii) *γ est un élément U2 de Γ.*
(iii) *γ est virtuellement unipotent et rang $(G) \geq 2$.*

Le Théorème B montre en particulier que si rang $G = 1$, g ne contient pas d'élément U1; ce résultant est démontré par Gromov dans [1, §3], qui observe aussi que la conjecture de Kazhdan (Théorème A) entraine les autres affirmations du Théorème B. En revanche, nous prouvons d'abord qu'un élément unipotent de Γ est un élément U1 si rang $G \geq 2$, et ensuite nous utilisons ce résultat pour prouver le Théorème A.

Nos démonstrations font appel de manière essentielle au théorème d'arithméticité de Margulis [3], qui affirme que si rang $G \geq 2$ un réseau irréductible de G est arithmétique. Nous avons appris récemment que G.A. Margulis a trouvé une preuve différente, plus géométrique, que le Théorème B entraine le Théorème A, mais cette preuve repose , elle aussi, sur le Théorème d'arithméticité. Il serait intéréssant d'avoir une démonstration purement géométrique du Théorème A.

Les démonstrations complètes des Théorèmes A et B seront données dans [2], où les résultats sont énoncés et prouvés dans le contexte plus générale des groupes S-arithmétiques. Ici, nous nous contentins donner la demonstration complète pour le cas $G = SL_d(\mathbb{R})$, $\Gamma = SL_d(\mathbb{Z})$. La preuve contient la plus part des ingrédients principaux de la preuve du résultat général (mais pas tous); d'autre part, elle est beaucoup plus facile à suivre.

Introduction.

Let G be a semi-simple linear Lie group and d_R its Riemannian left invariant metric. Let Γ be a lattice in G generated by a finite set Σ. The Cayley graph of Γ with respect to Σ induces a metric - the word metric d_W - on Γ. Of course this metric depends on Σ, but only up to Lipschitz equivalence ("coarse"). If Γ is

cocompact in G, then it is well known and not difficult to see that d_R restricted to Γ is Lipschitz equivalent to d_W. This is not always the case if Γ is a non-uniform lattice (i.e. of finite covolume in G but not cocompact). For example let $G = SL_2(\mathbb{R})$ and $\Gamma = SL_2(\mathbb{Z})$ then for $u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$, $d_W(u^n, 1)$ grows linearly in n while $d_R(u^n, 1) = O(\log n)$.

$SL_2(\mathbb{R})$ is a group of rank one. On the other hand:

Theorem A. *If G is a semi-simple Lie group of rank ≥ 2 and Γ an irréducible lattice of G, then d_R restricted to Γ is Lipschitz equivalent to d_W.*

A lattice Γ in G is irreducible if $N\Gamma/N$ is not discrete for any infinite closed normal subgroup N of G.

Theorem A was posed as a conjecure by Gromov ([Gr, §3]), who attributed it to Kazhdan. Gromov proved it there [Gr, §3] for the case $G = \underline{G}(\mathbb{R})$ and $\Gamma = \underline{G}(\mathbb{Z})$ where $\underline{G}$ is a $\mathbb{Q}$-algebraic group of $\mathbb{Q}$-rank one and $\mathbb{R}$-rank ≥ 2.

Theorem A implies that if we embed SL_2 in SL_3 at the left upper corner, and u is as above, then $d_W(u^n, 1) = O(\log n)$ where now d_W is the word metric of $SL_3(\mathbb{Z})$. This means that u^n can be written as a word of length $O(\log n)$ using generators of $SL_3(\mathbb{Z})$.

Definition. *1) An element γ of infinite order in a finitely generated group Γ is called a U1-*element of Γ *if $d_W(\gamma^n, 1) = O(\log n)$.*
*2) $\gamma \in \Gamma$ is a U2-*element *of Γ if $|B_n(1) \cap \langle\gamma\rangle|$ grows exponentially, where $B_n(1)$ is the ball with respect to d_W of radius n around the identity element 1 of Γ. In other words, the cyclic group $\langle\gamma\rangle$ generated by γ has exponential growth with respect to the generators of Γ.*

Clearly U1 implies U2 - but the converse is probably not true for general finitely generated groups. If Γ is a linear group and $\gamma \in \Gamma$ is a U1 or U2 element, then it is not difficult to show that γ is virtually unipotent, i.e., some power of γ is unipotent. The element $u \in SL_2(\mathbb{Z})$ above show that the converse is not always true - but we also saw that u is a U1 element of $SL_3(\mathbb{Z})$. More generally we have:

Theorem B. *Let G be a semi-simple linear Lie group and Γ an irreducible lattice of G. For $\gamma \in \Gamma$ the following conditions are equivalent.*

(i) *γ is a U1-element of Γ.*
(ii) *γ is a U2-element of Γ.*
(iii) *γ is virtually unipotent and rank $(G) \geq 2$.*

The part of Theorem B, asserting that if rank $(G) = 1$, then there are no U-elements is proved by Gromov in [Gr, §3]. He also mentioned there that Kazhdan's conjecture above (Theorem A) would imply the other assertions. Our approach is different - we first prove that unipotent elements of Γ are U1-elements if rank $(G) \geq 2$, hence proving the missing half of Theorem B. Then we use it, to prove Theorem A.

Our proofs make an essential use of Margulis arithmeticity theorem ([3]) stating that when rank $(G) \geq 2$, an irreducible lattice of G is arithmetic. We recently learnt that G. A. Margulis has a different (more geometric) way to deduce Theorem A from Theorem B. His proof however is also based on the arithmeticity of the lattice. It will be interesting to find a purely geometric proof for Theorem A.

The complete proofs of Theorem A and B can be found in [2]. In fact the results there are stated and proved in the more general context of S-arithmetic groups. Here we limit ourselves to giving a complete proof for the special cases $G = SL_d(\mathbb{R})$ and $\Gamma = SL_d(\mathbb{Z})$. The proof contains most (but not all) of the essential ingredients for the proof of the general theorems, but it is much easier to digest.

2. Proofs.

Throughout this section d is a fixed integer ≥ 3.

Lemma 1. *For any $1 \leq i \neq j \leq d$, $\gamma = E_{ij}(1)$ is a U1-element in $SL_d(\mathbb{Z})$ where $E_{ij}(t)$ denotes the elementary matrix having t at the ij entry, ones on the diagonal and zeros elsewhere.*

Proof. As all the elements $E_{ij}(1)$, $1 \leq i \neq j \leq d$, are conjugate to each other in $SL_d(\mathbb{Z})$ it suffices to prove the lemma for, say, $E_{1,3}(1)$. Moreover, it suffices to consider $SL_3(\mathbb{Z})$ and show that $E_{1,3}(1)$ is a U1-element in $SL_3(\mathbb{Z})$. Let $A = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $V = \left\{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; x, y \in \mathbb{R} \right\}$, $V \supset L = V \cap SL_3(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & 0 & k \\ 0 & 1 & l \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; k, l \in \mathbb{Z} \right\}$. The abelian group V is isomorphic to the vector space $\mathbb{R}^2$. The action of A on V by conjugation corresponds under this isomorphism to the linear action of $\overline{A} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ on $\mathbb{R}^2$. Clearly it preserves L which is identified with the integer lattice $\mathbb{Z}^2 \subset \mathbb{R}^2$. Henceforth we shall consider V as the vector space $\mathbb{R}^2$ and write the multiplication in it as addition and for $v \in V$ we shall write Av meaning the conjugation of v by A. Let W_1 be the eigenspace of V corresponding to the eigenvalue $\lambda = \frac{3+\sqrt{5}}{2} > 1$ of A and W_2 be the eigenspace corresponding to the eigenvalue $\lambda^{-1} = \frac{3-\sqrt{5}}{2} < 1$ of A.

Let $Y_0 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in V$. Define the following sets in L.

$$S_1 = \left\{ \pm \sum_{i=0}^{m} a_i A^i Y_0 \;\middle|\; m \in \mathbb{N} \quad 0 \leq a_i < \lambda,\ a_i \in \mathbb{Z} \right\}$$

$$S_2 = \left\{ \pm \sum_{j=0}^{n} b_j A^{-j} Y_0 \;\middle|\; n \in \mathbb{N} \quad 0 \leq b_j < \lambda,\ b_j \in \mathbb{Z} \right\}$$

It is easy to check that for each $i = 1, 2$, $\quad S_i$ is contained in a strip of bounded width around W_i and is syndetic in that strip (i.e., every point in that strip is at a bounded distance from some point of S_i).

It follows that the set $S = S_1 + S_2$ is a syndetic subset of L.

Next, observe that

(1) There exist some constants C_1, C_2 such that if $v \in S$ is of the form

$$v = \pm \sum_{i=0}^{m} a_i A^i Y_0 \pm \sum_{j=0}^{n} b_j A^{-j} Y_0$$

where $0 \leq a_i,\, b_j < \lambda$ and $a_m,\, b_n \neq 0$ then $C_1\lambda^k \leq \|V\| \leq C_2\lambda^k$ where $k = \max(m,n)$, and $\|\cdot\|$ is the usual norm on $\mathbb{R}^2$.

(2) The expression $v = \pm\sum_{i=0}^{m} a_i A^i Y_0 \pm \sum_{j=0}^{n} b_j A^{-j} Y_0$ may be rewritten in Hörner form as

$$v = \pm\big(a_0 Y_1 + A\big(a_1 Y_0 + (a_{m-1}Y_0 + Aa_m Y_0)\dots\big)\big) \pm \big(b_0 Y_0 \pm A^{-1}(b_1 Y_0 + \dots)\dots\big)$$

which, in turn, may be translated into a word (written multiplicatively) in the elements $\begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ in $SL_3(\mathbb{Z})$ of length at most $C_3(m+n) \leq 2C_3\, k$, C_3 some fixed constant and $k = \max(m,n)$.

i) and ii) imply that any element v of S may be expressed as a word of length $O(\log\|v\|)$ in the generators of $SL_3(\mathbb{Z})$. As S is syndetic in L the same (for a slightly different constant) holds for L. Since $\|E_{13}(1)^n\| = O(n)$ it follows that $E_{13}(1)$ is a U1-element. □

We remark that one can deduce from this lemma that any unipotent element in $SL_d(\mathbb{Z})$ is a U1-element in $SL_d(\mathbb{Z})$, thus proving Theorem A in this case. This would however follow in a stronger uniform way from our main result theorem 6 below.

Lemma 2. *Let* $x = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} \in \mathbb{Z}^d$ *be a unimodular vector and* $SL_2^{1,i}(\mathbb{Z})$, $2 \leq i \leq d$, *is the copy of* $SL_2(\mathbb{Z})$ *in* $SL_d(\mathbb{Z})$ *fixing the basis vectors* $e_j,\ j \neq i, 1$. *There exists* $\gamma_i \in SL_2^{1,i}(\mathbb{Z})$, $2 \leq i \leq d$ *and an element* $\gamma_1 \in \{E_{1i}(1) \mid\ i \neq 1\} \cup \{id\}$ *such that* $\gamma_d\gamma_{d-1}\dots\gamma_2\gamma_1 x = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ *and the entries of each* γ_i, $2 \leq i \leq d$, *are bounded by some fixed polynomials* p_i *in the* x_j*'s* $1 \leq j \leq d$.

Proof. Step 1: Applying some $\gamma_1 \in \{E_{1j}(1) \mid 2 \leq j \leq d\} \cup \{id\}$ we can assume $x_1 \neq 0$.

Step 2: For $i = 2, 3, \dots d$ we have a vector $y = (y_1, \dots, y_d)^{tr} = \gamma_{i-1}\dots,\gamma_1 x$ where $y_1 \neq 0$ and $y_j = 0$ for $1 < j < i$. Let $d = g.c.d.(y_1, y_i)$. There exist $u, v \in \mathbb{Z}$ such that $uy_1 + vy_i = d$ and $|u| < y_i,\ |v| < y_1$. There exist $w, z \in \mathbb{Z}$ such that $\begin{pmatrix} u & v \\ w & z \end{pmatrix} \in SL_2(\mathbb{Z})$ and $\begin{pmatrix} u & v \\ w & z \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$ moreover $|w|, |z| < y_1^2 + y_i^2$. Let γ_i be the element $\begin{pmatrix} u & v \\ w & z \end{pmatrix} \in SL^{1,i}(\mathbb{Z})$.

We obtain $\gamma_1 \dots \gamma_n$ such that $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \gamma_d\gamma_{d-1}\dots\gamma_1 x$. It follows also that the entries of the γ_i's are bounded by some polynomials in the entries of x. □

Corollary 3. *Let $\gamma \in SL_d(\mathbb{Z})$ then γ may be written as a product $\gamma = \delta_1\delta_2\dots\delta_{d^2}$ where each δ_i belongs to some $SL_2^{t,s}(\mathbb{Z}) \subset SL_d(\mathbb{Z})$ $1 \le t \ne s \le d$ where $SL_2^{t,s}(\mathbb{Z})$ is the copy of $SL_2(\mathbb{Z})$ in $SL_d(\mathbb{Z})$ fixing all the basis vectors e_j, $j \ne t, s$. Moreover the entries of these δ_i, $1 \le i \le d^2$ are bounded by fixed polynomials in the entries of γ.*

Proof. We prove the corollary by induction. If $d = 2$ there is nothing to prove. If $d \ge 3$ let $x \in \mathbb{Z}^d$ be the first column of γ. By Lemma 2 there exist elements $\gamma_1, \dots, \gamma_d$ belonging to various copies of $SL_2(\mathbb{Z})$ in $SL_d(\mathbb{Z})$ such that $\gamma_d \dots \gamma_1 x = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. Hence $\gamma' = \gamma_d \dots \gamma_1 \gamma$ is an element of $SL_d(\mathbb{Z})$ whose first column is $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. By multiplying on the right by (unipotent) elements from $SL_2^{1j}(\mathbb{Z})$ $j = 2, \dots, d$ we can make sure that the first row is $(1\ 0 \dots 0)$. Hence the resulting element γ'' belongs to $SL_{d-1}(\mathbb{Z})$ embedded as the lower right corner of $SL_d(\mathbb{Z})$. Thus we may apply the induction hypothesis to this γ'', and conclude that γ may be expressed as a product of the required form (note that the entries of γ'' are bounded by polynomials in the entries of γ). $\square$

Proposition 4. *Any $\gamma \in SL_2(\mathbb{Z})$ may be written as a product of the form $\gamma = r_1 \dots r_m$ so that*

i) *Each r_j, $1 \le j \le m$, is either $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ or $\begin{pmatrix} 1 & n_j \\ 0 & 1 \end{pmatrix}$ for some $n_j \in \mathbb{Z}$.*

ii) $\sum_{j=1}^{m} f(r_j) = O\big(d(p_0, \gamma p_0)\big)$ *where* $f(\delta) = \begin{cases} 1 & \delta = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ \log(|n|+1) & \delta = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \end{cases}$,
$p_0 = 2i \in \mathbb{H}^2$ - the upper half plane and $d(\ ,\ )$ is the hyperbolic metric on $\mathbb{H}^2$.

Proof. Consider the action of $SL_2(\mathbb{Z})$ on the upper half plane $\mathbb{H}^2$ as hyperbolic isometries given by Möbius transformations. $\mathbb{H}^2$ is tesselated by fundamental domains $\mathcal{F}_\theta$ $\theta \in PSL_2(\mathbb{Z})$ where $\mathcal{F}_\theta = \theta\mathcal{F}_{id}$ and $\operatorname{int}\mathcal{F}_{id} = \{x + yi \mid -\frac{1}{2} < x < \frac{1}{2},\ x^2 + y^2 > 1\}$. Note that $p_0 \in \mathcal{F}_{id}$. $\mathcal{F}_\theta$ and $\mathcal{F}_{\theta'}$ are adjacent if and only if $\theta^{-1}\theta' \in \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$. Denote $u(n) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, $n \in \mathbb{Z}$. Let $B_0 = \{x + yi \mid y > 3\}$ be a horoball and $\mathbb{B} = \{\theta B_0 \mid \theta \in SL_2(\mathbb{Z})\}$. $\mathbb{B}$ is a collection of disjoint horoballs. Let $X_0 = \mathbb{H}^2 \setminus \bigcup_{B \in \mathbb{B}} B$. $SL_2(\mathbb{Z})\backslash X_0$ is compact. If $\mathcal{F}_\theta$ and $\mathcal{F}_{\theta'}$ are two fundamental domains intersecting B_0 then $\theta^{-1}\theta' = u(n)$ for some $n \in \mathbb{Z}$. For $\theta \in SL_2(\mathbb{Z})$ let $\mathcal{F}'_\theta = \mathcal{F}_\theta \cap X_0$, $\{\mathcal{F}'_\theta \mid \theta \in SL_2(\mathbb{Z})\}$ form a tesselation of X_0.

Given $\gamma \in SL_2(\mathbb{Z})$ look at the geodesic $[p_0, \gamma p_0]$ connecting p_0 and γp_0 in $\mathbb{H}^2$. Its intersection with X_0 passes through a sequence of fundamental domains $\mathcal{F}'_{\theta_j}$ $0 \le j \le m$ such that $\theta_0 = id$, $\theta_m = \gamma$. Let $r_j = \theta_{j-1}^{-1}\theta_j$, $1 \le j \le m$. Thus we obtain $\gamma = r_1 r_2 \dots r_m$. Notice that two consecutive fundamental domains $\mathcal{F}'_{\theta_{j-1}}, \mathcal{F}'_{\theta_j}$ along this sequence are either (i) adjacent in X_0, or (ii) both border some horoball $B \in \mathbb{B}$ containing the part of the geodesic between them. In case (i), $r_j = \theta_{j-1}^{-1}\theta_j \in \left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \right\}$. In case (ii), $r_j = \theta_{j-1}^{-1}\theta_j = u(n_j)$ for some

$0 \neq n_j \in \mathbb{Z}$.

Let $p_j = \theta_j p_0$ for $1 \leq j \leq m$, and consider the path α made of the geodesics $[p_{j-1}, p_j]$, $1 \leq j \leq m$, in $\mathbb{H}^2$. It is not difficult to see that

$d(p_0, \gamma p_0) = \text{length}([p_0, \gamma p_0] \approx \text{length}(\alpha) = \sum_{j=1}^{m} d(p_{j-1}, p_j) = \sum_{j=1}^{m} d(\theta_{j-1} p_0,\, \theta_j p_0) =$

$\sum d(p_0, \theta_{j-1}^{-1} \theta_j p_0) \approx \sum f(r_j)$, where $\approx$ means Lipschitz equivalent. This proves the proposition. $\square$

Corollary 5. *Let $1 \leq s \neq t \leq d$. Any $\gamma \in SL_2^{s,t}(\mathbb{Z}) \subset SL_d(\mathbb{Z})$ may be written as a word of length $O(\log \|\gamma\|)$ in a fixed set of generators of $SL_d(\mathbb{Z})$.*

Proof. Let $\gamma = r_1, r_2 \ldots r_m$ be an expression of γ as in Proposition 4. By Lemma 1 each of the r_j, $1 \leq j \leq m$, such that $r_j = \begin{pmatrix} 1 & n_j \\ 0 & 1 \end{pmatrix}$ for some $n_j \in \mathbb{Z}$ may be written as $r_j = w_j$ where w_j is a word of length $\leq C' \log n_j \leq C f(r_j)$ with respect to some fixed set of generators and some fixed constants C' and C. Substituting these words for each such r_j and expressing $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ as a word in our generators we obtain a word w in the generators expressing γ such that its length is $\leq D \cdot \sum_{j=1}^{m} f(m_j) = O\big(d(p_0, \gamma p_0)\big)$ where D is a constant. The corollary follows since $d(p_0, \gamma p_0) = O(\log \|\gamma\|)$. (Recall that for $SL_d(\mathbb{R})$, $d_R(g, id)$ is Lipschitz equivalent to $\log(\|\gamma - id\| + 1)$.) $\square$

Combining Corollary 4 and Lemma 5, we have:

Theorem 6. *The word metric on $SL_d(\mathbb{Z})$ for $d \geq 3$ is equivalent to the restriction of the Riemannian metric of $SL_d(\mathbb{R})$ to $SL_d(\mathbb{Z})$.* $\square$

Corollary 7. *For $d \geq 3$, a cyclic subgroup of $SL_d(\mathbb{Z})$ has a relative exponential growth if and only if it is virtually unipotent.* $\square$

References

[1] M. Gromov, *Asymptotic invariants of infinite groups*, to appear in the proceedings of the Isle of Thorns conference on group theory.

[2] A. Lubotzky, S. Mozes, M.S. Raghunathan, *The word and Riemannian metrics on lattices of semi-simple groups*, in preparation.

[3] G. Margulis, *Discrete Subgroups of Semisimple Lie Groups*, Springer-Verlag, 1990.

Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel

Department of Mathematics, The University of Chicago, Chicago IL 60637, U.S.A.

School of Mathematics, Tata Institute of Fundamental Research, Bombay 400-005, India