ANNALES

DE

L'INSTITUT FOURIER

Richard AOUN

Transience of algebraic varieties in linear groups - applications to generic Zariski density

Tome 63, nº 5 (2013), p. 2049-2080.

<http://aif.cedram.org/item?id=AIF_2013__63_5_2049_0>

Ann. Inst. Fourier, Grenoble
63, 5 (2013) 2049-2080

TRANSIENCE OF ALGEBRAIC VARIETIES IN LINEAR GROUPS - APPLICATIONS TO GENERIC ZARISKI DENSITY

by Richard AOUN

ABSTRACT. — We study the transience of algebraic varieties in linear groups. In particular, we show that a “non elementary” random walk in $SL_2(\mathbb{R})$ escapes exponentially fast from every proper algebraic subvariety. We also treat the case where the random walk takes place in the real points of a semisimple split algebraic group and show such a result for a wide family of random walks.

As an application, we prove that generic subgroups (in some sense) of linear groups are Zariski dense.

RÉSUMÉ. — Nous étudions la transience des variétés algébriques dans les groupes linéaires. En particulier, nous montrons qu'une marche aléatoire sur un sous-groupe non élémentaire de $SL_2(\mathbb{R})$ évite toute sous-variété algébrique propre avec une probabilité convergeant vers 1 de façon exponentielle. Nous étudions aussi le cas où la marche aléatoire vit dans un sous-groupe Zariski dense du groupe des points réels d'un groupe algébrique semi-simple, défini et déployé sur $\mathbb{R}$.

Nous utilisons ces résultats pour montrer qu'un sous-groupe aléatoire (en un sens à préciser) d'un groupe algébrique est Zariski dense.

1. Introduction

One of the essential results in probability theory on groups is Kesten's theorem [23]: the probability of return to identity of a random walk on a group Γ decreases exponentially fast if and only if Γ is non amenable. A natural question is to extend this to other subsets: for which subsets does the random walk escape with exponential rate? Many authors have studied the case where the subset is a subgroup of Γ: see for example [15], [3] and in particular [2, Theorem 51] where it is shown that the probability that a

Keywords: transience, algebraic varieties, Zariski density, random matrix products, random walks, probability of return.
Math. classification: 20P05, 20G20, 60B15.

random walk on Γ returns to a subgroup H decreases exponentially fast to zero if and only if the Schreier graph of Γ/H is non amenable.

In this note we look at random walks on Zariski dense subgroups of algebraic groups (such as $SL_2(\mathbb{R})$) and we look at the escape from proper algebraic subvarieties. Such questions have an interest in their own right since they allow us to study the delicate behavior of the random walk but they have also been recently involved in other domains such as the theory of expander graphs. We are referring here among others to the works of Bourgain and Gamburd [11],[12], Breuillard and Gamburd [14] and Varju [32]. In [14] for instance it is shown that there is an infinite set of primes p of density one, such that the family of all Cayley graphs of $SL_2(\mathbb{Z}/p\mathbb{Z})$ is a family of expanders. A crucial part of the proof is to take a random walk on $SL_2(\mathbb{Z}/p\mathbb{Z})$ and to show that the probability of remaining in a subgroup decreases exponentially fast to zero and uniformly. In [12, Corollary 1.1.] the following statement was established: consider the group $SL_d(\mathbb{Z})$ ($d \geqslant 2$), the uniform probability measure on a finite symmetric generating set and $(S_n)_{n\in\mathbb{N}}$ the associated random walk, then for every proper algebraic variety $\mathcal{V}$ of $SL_d(\mathbb{C})$, $\mathbb{P}(S_n \in \mathcal{V})$ decreases exponentially fast to zero.

Kowalski [25] and Rivin [28] were interested in similar questions: for example they were able to estimate the probability that a random walk in $SL_d(\mathbb{Z})$ lies in the set of matrices with reducible characteristic polynomial. The techniques used by Kowalski and Rivin are arithmetic sieving ones.

In this article, we develop a more probabilistic approach allowing us to deal with random walks on arbitrary Zariski dense subgroups of semisimple algebraic groups. In the particular case of $SL_2(\mathbb{R})$, we obtain (see Theorem 1.1) that a random walk whose law generates a non-elementary subgroup escapes with probability tending to one exponentially fast from every algebraic variety. Our method relies on the theory of random matrix products developed in the 60's by Kesten and Furstenberg and in the 70's-80's by the French school: in particular Bougerol, Guivarc'h, Le Page and Raugi.

We also apply our techniques to generic Zariski density. Let Γ_1 and Γ_2 be two Zariski dense subgroups of $SL_d(\mathbb{R})$ ($d \geqslant 2$). We prove in Theorem 7.4 that one can exhibit a probability measure on each of the subgroups such that two independent random walks will eventually generate a Zariski dense subgroup. We have proved in [1] that the latter subgroup is also free. This gives consequently a "probabilistic" version of the Tits alternative [31].

All the random variables will be defined on a probability space $(\Omega, \mathcal{F}, \mathbb{P})$, the symbol $\mathbb{E}$ will refer to the expectation with respect to $\mathbb{P}$ and "a.s." to almost surely. If Γ is a topological group, μ a probability measure on Γ, we define a sequence of independent random variables $\{X_n; n \geqslant 0\}$ with the same law μ. We denote for every $n \in \mathbb{N}^*$ by $S_n = X_n \cdots X_1$ the n^{th} step of the random walk.

First let us present the result we obtain for $SL_2(\mathbb{R})$. We will say that a probability measure μ on $SL_2(\mathbb{R})$ is non elementary if the group generated by its support is non elementary, *i.e.*, Zariski dense in $SL_2(\mathbb{R})$ or equivalently non solvable.

Theorem 1.1. — *Let μ be a non elementary probability measure on $SL_2(\mathbb{R})$ having an exponential moment (see Section 5.1 for a definition of this notion). Then for every proper algebraic subvariety $\mathcal{V}$ of $SL_2(\mathbb{R})$,*

$$\limsup_{n\to\infty} \left[\mathbb{P}(S_n \in \mathcal{V})\right]^{\frac{1}{n}} < 1.$$

In particular, every proper algebraic subvariety is transient, that is a.s. S_n leaves $\mathcal{V}$ after some time.

More precisely, if P is a non constant polynomial equation in the entries of the 2×2 matrices of $SL_2(\mathbb{R})$, then there exists $\lambda > 0$ such that:

$$\frac{1}{n} \log |P(S_n)| \xrightarrow[n\to\infty]{a.s.} \lambda.$$

A large deviation inequality holds as well: for every $\epsilon > 0$:

$$\limsup_{n\to\infty} \left[\mathbb{P}\left(\left|\frac{1}{n} \log |P(S_n)| - \lambda\right| > \epsilon\right)\right]^{\frac{1}{n}} < 1. \tag{1.1}$$

Theorem 1.1 is in fact a particular case of a more general statement: Theorem 1.2 below. If G is the group of real points of an algebraic semisimple group $\mathbf{G}$, m a Cartan projection (see Section 4), μ a probability measure on G, then the Kingman subadditive ergodic theorem allows us to define a vector $\mathrm{Liap}(\mu)$ (see Definition / Proposition 5.7) in the Weyl chamber of G which is the almost sure limit of $\frac{1}{n} m(S_n)$.

Theorem 1.2. — *Let $\mathbf{G}$ be an algebraic semisimple group defined and split over $\mathbb{R}$*[1]*, $G = \mathbf{G}(\mathbb{R})$ its group of real points, Γ a Zariski dense subgroup of G, $\mathcal{V}$ a proper algebraic subvariety of $\mathbf{G}$ defined over $\mathbb{R}$, μ a probability on G with an exponential moment (see Section 5.1) such that its support generates Γ. Then, there exists a finite union of hyperplanes $H_1, \cdots, H_r$ in the Weyl chamber (see Section 4.1) depending only on $\mathcal{V}$ such that if* $\mathrm{Liap}(\mu) \notin H_1 \cup \cdots \cup H_r$ *then,*

$$\limsup_{n\to\infty} \left[\mathbb{P}(S_n \in \mathcal{V})\right]^{\frac{1}{n}} < 1. \tag{1.2}$$

(1) For example, $\mathbf{G} = \mathbf{SL}_d$, $d \geqslant 2$.

Probability measures, whose support generates Γ*, satisfying the condition* $\mathrm{Liap}(\mu) \notin H_1 \cup \cdots H_r$ *exist (See Lemma 5.10). A large deviation inequality similar to (1.1) holds as well.*

Theorem 1.2 clearly implies Theorem 1.1: indeed, everything we want to show is that the Lyapunov exponent associated to μ (see Definition 5.4) is non zero (positive). This is ensured by Furstenberg's theorem [17].

Remark 1.3. — The number λ that appears in Theorem 1.1 or 1.2, should be seen as a generalization of the classical Lyapunov exponent (see Definition 5.4). In fact, it will be the Lyapunov exponent relative to the probability measure $\rho(\mu)$ where ρ is some rational representation of $\mathbf{G}$.

Remark 1.4. — Our method doesn't allow us to estimate $\mathbb{P}(S_n \in \mathcal{V})$ when $\mathrm{Liap}(\mu)$ belongs to the finite union of hyperplanes H_i defined by the variety $\mathcal{V}$. Example 2 of Section 2 illustrates this.

Let us justify why we will look at the escape from algebraic subvarieties and not from C^1 submanifolds for instance. Kac and Vinberg proved in [33] (see also [6]) that there exist discrete Zariski dense subgroups of $SL_3(\mathbb{R})$ preserving a C^1 (but not algebraic) manifold on the projective plane (in fact, such manifolds are obtained as the boundary of a divisible convex in $P^2(\mathbb{R})$). Let Γ be such a group, $\mathcal{C}$ such a manifold and $\mathcal{V} = \{x \in \mathbb{R}^3 \setminus \{0\}; [x] \in \mathcal{C}\} \cup \{0\}$ where $[x]$ denotes the projection of $x \neq 0$ on $P^2(\mathbb{R})$. Note that $\mathcal{V}$ is differentiable outside 0. Then, for every $x \in \mathcal{V}$, every $n \in \mathbb{N}$, $\mathbb{P}(S_n x \in \mathcal{V}) = 1$. By way of contrast, we show in the following statement that for proper algebraic subvarieties the latter quantity decreases exponentially fast to zero.

Theorem 1.5. — *Let* Γ *be a Zariski dense subgroup of* $SL_d(\mathbb{R})$ $(d \geqslant 2)$*,* μ *a probability measure with an exponential moment whose support generates* Γ*. Then for every proper algebraic subvariety* $\mathcal{V}$ *of* $\mathbb{R}^d$*, every non zero vector* x *of* $\mathbb{R}^d$ *we have:*

$$\limsup_{n\to\infty} \left[\mathbb{P}(S_n x \in \mathcal{V})\right]^{\frac{1}{n}} < 1.$$

As discussed at the beginning of the introduction, it is interesting to study the transience of proper subgroups. It follows from Varju's paper (see [32, Propositions 8 and 9]) that if $\mathbf{E}$ is a simple algebraic group defined over $\mathbb{R}$, $\mathbf{G}$ the direct product of r copies of $\mathbf{E}$ (with $r \in \mathbb{N}^*$), Γ a Zariski dense subgroup of $G = \mathbf{G}(\mathbb{R})$, then there exists a symmetric probability measure μ on Γ whose support generates Γ such that the probability that the associated random walk escapes from a proper algebraic subgroup decreases exponentially fast to zero.

We will show that this in fact holds for all probability measures with an exponential moment whose support generates Γ and for every semisimple algebraic group $\mathbf{G}$, namely:

THEOREM 1.6. — *Let $\mathbf{G}$ be a semisimple algebraic group defined over $\mathbb{R}$, G its group of real points assumed without compact factors, Γ a Zariski dense subgroup of G and μ a probability measure with an exponential moment whose support generates Γ. Then for every proper algebraic subgroup $\mathbf{H}$ of $\mathbf{G}$,*

$$\limsup_{n\to\infty} \left[\mathbb{P}(S_n \in H)\right]^{\frac{1}{n}} < 1$$

where H is the group of real points of $\mathbf{H}$.

The bound obtained by Varju is uniform over the subgroups. Unfortunately our bound in Theorem 1.6 is not.

Our estimates will be applied to show that Zariski density in linear groups is generic in the following sense:

THEOREM 1.7. — *Let G be the group of real points of a semisimple algebraic group split over $\mathbb{R}$. Let Γ_1, Γ_2 be two Zariski dense subgroups of G. Then there exist probability measures μ_1 and μ_2 with an exponential moment whose support generate respectively Γ_1 and Γ_2 such that for some $c \in]0,1[$ and all large n,*

$$\mathbb{P}(\langle S_{1,n}, S_{2,n}\rangle \text{ is Zariski dense and free}) \geqslant 1 - c^n$$

where $\{S_{2,n}; n \geqslant 0\}$ and $\{S_{2,n}, n \geqslant 0\}$ are two independent random walks on Γ_1 (resp. Γ_2) associated respectively to μ_1 and μ_2 on Γ_1 (resp. Γ_2). This implies that almost surely, for n big enough, the subgroup $\langle S_{1,n}, S_{2,n}\rangle$ is Zariski dense and free.

See Section 7 for the comparison of these results with Rivin's in [29].

Remark 1.8. — The fact that $\{w \in \Omega; \langle S_n(w), {S_n}'(w)\rangle \text{ is Zariski dense}\}$ is measurable will follow from Lemma 7.7.

1.1. Outline of the paper

In order to prove Theorem 1.2 (or 1.5, 1.6), one can clearly suppose that $\mathcal{V}$ is a proper hypersurface (*i.e.*, the common zeroes of one polynomial equation). We will do so in all the paper.

In Section 2, we provide two examples to explain the general idea of the proofs.

Section 3 is purely algebraic. To every proper algebraic hypersurface $\mathcal{V}$ of $\mathbf{G}$ we associate a rational real representation ρ of $\mathbf{G}$ such that $g \in \mathcal{V}$ is equivalent to: the matrix coefficients of $\rho(g)$ satisfy a linear condition "(L)". Thus we have "linearized" our variety. This can be seen as a generalization of the well-known Chevalley theorem (Theorem 3.3) concerning the particular case of subgroups.

In Section 4 we recall standard facts about semisimple algebraic groups and their rational representations.

In Section 5 we precise some results in the theory of random matrix products. They will be used in Section 6 in order to show that $\rho(S_n)$ may verify (L) only with a probability decreasing exponentially in n.

We consider a random walk on a Zariski dense subgroup Γ of the real points of an algebraic semisimple group. First we define the Lyapunov vector, which is the normalized Cartan projection of the random walk. We recall in Theorem 5.8 that it belongs to the interior of the Weyl chamber. In Lemma 5.10, we show that for every finite union of hyperplanes in the Weyl chamber, one can always find a probability measure whose support generates Γ such that the Lyapunov vector does not belong to this union (this is the condition stated in Theorem 1.2).

Next, we will be interested in the behavior of the components of the random walk in the Cartan decomposition. Almost all our results will be quoted from our previous work [1].

In Section 6, we prove our mains results: Theorems 1.2, 1.5 and 1.6. The key is Theorem 6.1 which computes the probability that a random walk on a linear algebraic group verifies a linear condition on the matrix coefficients. No irreducibility assumptions are made, a genericity condition on the geometry of the Lyapunov vector is however needed.

Finally in Section 7, we apply Theorem 6.1 to prove Theorem 1.7. We compare our results with Rivin's in [29].

Acknowledgments. I sincerely thank Emmanuel Breuillard for fruitful discussions, remarks and advices. It is my pleasure also to thank Emile Le Page and Yves Guivarc'h for many discussions and Igor Rivin for his interest and his comments. I thank also the referee for the very useful comments and corrections. Finally, I thank Orsay university (Paris 11) for the perfect and exceptional working atmosphere and "Université Saint-Joseph" (Lebanon) for their warm welcome during Fall 2012.

2. Examples

In this section, we give examples to illustrate the ideas and methods we will use in the next section to prove our main results.

2.1. Example 1

This example illustrates Theorem 1.5.

Let Γ be Zariski dense subgroup of $SL_3(\mathbb{R})$ ($SL_3(\mathbb{Z})$ for example). Consider a probability measure μ on $SL_3(\mathbb{R})$ with an exponential moment (see Section 5.1) whose support generates Γ. For example, if Γ is finitely generated, choose a probability measure whose support is a finite symmetric generating set. Let $S_n = X_n \cdots X_1$ be the associated random walk. We write S_n in the canonical basis of $M_{3,3}(\mathbb{R})$:

$$S_n = \begin{pmatrix} a_n & b_n & c_n \\ d_n & e_n & f_n \\ g_n & h_n & i_n \end{pmatrix}.$$

We propose to see if the following probability decreases exponentially fast to zero:

$$p_n = \mathbb{P}(a_n^2 - a_n e_n + 2a_n d_n - a_n b_n - b_n d_n = 0).$$

In other words if $\mathcal{V}$ is the proper algebraic hypersurface of $SL_3(\mathbb{R})$ defined by $\mathcal{V} = \{ \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \in \Gamma; a^2 - ae + 2ad - ab - bd = 0\}$, then we are interested in estimating $\mathbb{P}(S_n \in \mathcal{V})$.

Step 1: Linearization of the algebraic hypersurface $\mathcal{V}$. Let E be the vector space of homogenous polynomials on three variables X, Y, Z of degree 2. The group $SL_3(\mathbb{R})$ acts on E by the formula:

$$g \cdot P \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = P\Big(g^t \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}\Big)$$

where g^t is the transposed matrix of g when g is expressed in the canonical basis. Let us write down this representation. We will consider the basis

$\{X^2, Y^2, Z^2, XY, XZ, XY\}$ of E.

$$\begin{array}{ccc} SL_3(\mathbb{R}) & \xrightarrow{\rho} & GL(E) \simeq GL_6(\mathbb{R}) \\ \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} & \mapsto & \begin{pmatrix} a^2 & b^2 & c^2 & ab & ac & bc \\ d^2 & e^2 & f^2 & de & df & ef \\ g^2 & h^2 & i^2 & gh & gi & hi \\ 2ad & 2be & 2cf & ae+bd & af+cd & bf+ec \\ 2ag & 2bh & 2ci & ah+gb & ai+cg & bi+ch \\ 2dg & 2eh & 2fi & dh+eg & di+gf & ei+hf \end{pmatrix}. \end{array}$$

In what follows we identify E with $\mathbb{R}^6$ by sending $\{X^2, Y^2, XY, XZ, YZ\}$ to the canonical basis $\{e_i; i = 1, \cdots, 6\}$. Then it is clear that

$$\mathcal{V} = \{g \in SL_3(\mathbb{R}); \rho(g)(e_1 - e_4) \in H\}$$

where H is the hyperplane in E defined by $H = \{x = (x_i)_{i=1}^6 \in \mathbb{R}^6; x_1 + x_4 = 0\}$.

We say that we have linearized the hypersurface $\mathcal{V}$. This method generalizes easily and yields Lemma 3.2 which holds for arbitrary hypersurfaces.

Note that, for $x = e_1 - e_4$,

$$p_n = \mathbb{P}\left(\rho(S_n)x \in H\right).$$

Random matrix products in $GL_6(\mathbb{R})$. We have now a probability measure $\rho(\mu)$, image of μ under ρ, on $GL_6(\mathbb{R})$ with an exponential moment. The smallest closed group $G_{\rho(\mu)}$ containing the support of $\rho(\mu)$ is a Zariski dense subgroup of $\rho(SL_3(\mathbb{R}))$. One can verify that ρ is in fact $SL_3(\mathbb{R})$-irreducible. Since $SL_3(\mathbb{R})$ is Zariski connected, we deduce that $G_{\rho(\mu)}$ is a strongly irreducible (Definition 5.2) subgroup of $GL_6(\mathbb{R})$. Moreover, the group $\rho\left(SL_3(\mathbb{R})\right)$ contains clearly a proximal element, then by Goldsheid-Margulis Theorem [18] (see Theorem 5.3 for the statement), the same applies for $G_{\rho(\mu)}$.

Thus, we can use the theory of random matrix products which gives (see Theorem 5.15) what we wanted to prove, *i.e.*, :

$$\limsup_{n\to+\infty} \frac{1}{n} \log \mathbb{P}\left(\rho(S_n)x \in H\right) < 0.$$

A word about the proof: if $[x]$ denote the projection of $x \in \mathbb{R}^6 \setminus \{0\}$ in the projective space $P(\mathbb{R}^6)$, then $\rho(S_n)[x]$ converges in law towards a random variable Z with law the unique μ-invariant probability measure ν on the projective space $P(\mathbb{R}^6)$. Moreover, almost surely, Z cannot belong to the hyperplane H because ν is proper. More precisely, we can control the distance between Z and a fixed hyperplane H.

Remark 2.1. — This method does not give an estimate of the growth of $Q(S_n)$ where Q is the polynomial that defines $\mathcal{V}$. We will see in the next section (Theorem 6.1) how such quantities can be estimated.

2.2. Example 2

This example illustrates situations in which we are unable to obtain the exponential decrease of the probability of lying in a subvariety for all probability measures (see the statement of Theorem 1.2).

As in Example 1, consider a probability measure on $SL_3(\mathbb{R})$ with an exponential moment whose support generates a Zariski dense subgroup of $SL_3(\mathbb{R})$. Say that we would like to estimate the following probability:

$$q_n = \mathbb{P}(a_n e_n - b_n d_n + 2e_n = 0).$$

Let $\mathcal{S}$ be the following hypersurface of $SL_3(\mathbb{R})$: $\mathcal{S} = \{ae - bd + 2e = 0\}$ so that $q_n = \mathbb{P}(S_n \in \mathcal{S})$. Consider the natural action of $SL_3(\mathbb{R})$ on $F = \bigwedge^2 \mathbb{R}^3 \oplus \mathbb{R}^3$. Denote by η this representation and write $\eta = \eta_1 \oplus \eta_2$. We fix the basis $(e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3, e_1, e_2, e_3)$ of F. Formally, we have:

$$\begin{array}{ccc} SL_3(\mathbb{R}) & \xrightarrow{\eta} & GL(F) \simeq GL_6(\mathbb{R}) \\ \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} & \mapsto & \begin{pmatrix} ae-bd & af-cd & bf-ec & 0 & 0 & 0 \\ ah-gb & ai-gc & bi-hc & 0 & 0 & 0 \\ dh-eg & di-gf & ei-hf & 0 & 0 & 0 \\ 0 & 0 & 0 & a & b & c \\ 0 & 0 & 0 & d & e & f \\ 0 & 0 & 0 & g & h & i \end{pmatrix}. \end{array}$$

Thus

$$\mathcal{S} = \{g \in SL_3(\mathbb{R}); \eta(g)x \in H\}$$

where $x = e_1 \wedge e_2 + e_2$ and $H = \{x \in \mathbb{R}^6; x_1 + 2x_5 = 0\}$. Hence, we have linearized our variety $\mathcal{S}$ as in Example 1. The difference between these two examples is that the representation η is no longer irreducible (η_1 and η_2 are its irreducible sub-representations). Hence we cannot use Theorem 5.13.

However, we will see in the proof of Theorem 6.1 that we are able to solve the problem if the top Lyapunov exponents of $\eta_1(\mu)$ and $\eta_2(\mu)$ are distinct.

Let us calculate them. If λ_1, λ_2 are top two Lyapunov exponents of μ[(2)], then the top Lyapunov exponent of $\eta_1(\mu)$ is $\lambda_1 + \lambda_2$ and the one corresponding to $\eta_2(\mu)$ is clearly λ_1. So the problem occurs when $\lambda_2 = 0$. This

[(2)] $\lambda_1 = \lim_{n\to+\infty} \frac{1}{n}\mathbb{E}(\log ||S_n||)$ and $\lambda_1 + \lambda_2 = \lim_{n\to+\infty} \frac{1}{n}\mathbb{E}(\log || \bigwedge^2 S_n||)$

can happen for example when μ is a symmetric probability measure (*i.e.*, the law of X_1 is the same as X_1^{-1}).

However, we can still find a probability measure whose support generates Γ such that $\lambda_2 \neq 0$, see Lemma 5.10.

3. Linearization of algebraic varieties

Let $\mathbf{G}$ be a semisimple algebraic group defined over $\mathbb{R}$, G its group of real points.

The goal of this section is to linearize every algebraic hypersurface of $\mathbf{G}$ defined over $\mathbb{R}$. More precisely, to every proper algebraic hypersurface $\mathcal{V}$ defined over $\mathbb{R}$, we associate a finite dimensional rational real representation (ρ, V) of $\mathbf{G}$, a linear form L of $\mathrm{End}(V)$ such that $\mathcal{V} = \{g \in \mathbf{G}; L(\rho(g)) = 0\}$. In fact, we will find a representation (ρ, V) of $\mathbf{G}$, a line D in V, a hyperplane H in V defined over $\mathbb{R}$ such that $\mathcal{V} = \{g \in \mathbf{G}; g \cdot D \subset H\}$ (see Lemma 3.2). This has to be seen as a generalization of the well-known Chevalley theorem for subgroups (see Theorem 3.3).

Definition 3.1 (Matrix coefficients). — *If (V, ρ) is a finite dimensional representation of G, $\langle \cdot, \cdot \rangle$ a scalar product on V, we call $\langle \rho(g)v, w \rangle$ for $v, w \in V$ a matrix coefficient and we denote by $C(\rho)$ the span of the matrix coefficients of the representation ρ, thus a function $f \in C(\rho)$ can be written $L \circ \rho$ where L is a linear form on the vector space* $\mathrm{End}(V)$.

Let $\rho_1, \cdots, \rho_r$ be independent $\mathbb{R}$-rational irreducible representations of $\mathbf{G}$. Any $f_1 \in C(\rho_1), \cdots, f_r \in C(\rho_r)$ are linearly independent provided that the representation ρ_i are pairwise non-isomorphic (see the proof of the Lemma 3.2 below). The set of elements of G where such a linear dependance is realized defines clearly an algebraic hypersurface of $\mathbf{G}$. The following lemma says also that each algebraic hypersurface can be realized in this way.

Lemma 3.2. — *For every algebraic hypersurface $\mathcal{V}$ of $\mathbf{G}$ defined over $\mathbb{R}$, there exist a representation (ρ, V) of $\mathbf{G}$, a line D in V, a hyperplane H of V defined over $\mathbb{R}$ such that $\mathcal{V} = \{g \in \mathbf{G}; g \cdot D \subset H\}$. In particular, there exist a representation (ρ, V) of $\mathbf{G}$* ***whose irreducible sub-representations****, say $\rho_1, \cdots, \rho_r$,* ***occur only once****, $f_1 \in C(\rho_1), \cdots, f_r \in C(\rho_r)$ such that:*

$$\mathcal{V}(\mathbb{R}) = \{g \in G; \sum_{i=1}^{r} f_i(g) = 0\}. \tag{3.1}$$

This is equivalent to saying that there exists $A \in \mathrm{End}(V_1) \oplus \cdots \oplus \mathrm{End}(V_r)$ *such that:*

$$\mathcal{V}(\mathbb{R}) = \{g \in G;\ \mathrm{Tr}\,(\rho(g)A) = 0\}.$$

Here $\mathrm{Tr}(M)$ *denotes the trace of the endomorphism* M*.*

Proof. — Without loss of generality, we can assume that $\mathcal{V}$ is proper. Let $\mathbb{R}[\mathbf{G}]$ be the algebra of functions on $\mathbf{G}$, $\mathbf{G}$ acting on $\mathbb{R}[\mathbf{G}]$ by right translations: $g \cdot f(x) = f(xg)\ \forall g, x \in \mathbf{G}$, P the generator of the ideal vanishing on $\mathcal{V}$ (which is of rank one since $\mathcal{V}$ is a hypersurface). Then $g \in \mathcal{V} \iff g\cdot P(1) = 0$. Consider the sub-representation $V = Vect(g\cdot P, g \in G)$. By [22, Chapter 8, Proposition 8.6], V is a finite dimensional $\mathbb{R}$-rational representation of $\mathbf{G}$. When $\mathcal{V}$ is proper, the subspace $H = \{f \in V; f(1) = 0\}$ is a hyperplane defined over $\mathbb{R}$ so that $g \in \mathcal{V} \iff g \cdot P \in H$ and the first part of lemma is proved. $\mathbf{G}$ being semisimple, we decompose (ρ, V) into irreducible sub-representations : $V = \oplus_{i=1}^{r} V_i$. Decomposing P in the $V_i's$ gives easily (3.1) with the only difference that the $V_i's$ are not necessarily pairwise non isomorphic.

Suppose for instance that $V_1 \simeq V_2$. In this case, there exists an invertible matrix M such that $\rho_2(g) = M\rho_1(g)M^{-1}$ for every $g \in \mathbf{G}$. Let $f_i = L_i \circ \rho_i$ where L_i is a suitable linear form on $\mathrm{End}(V_i)$ for $i = 1, 2$. Then $f_2 = \widetilde{L_2} \circ \rho_1$ where $\widetilde{L_2}$ is the linear form defined on $\mathrm{End}(V_1)$ by $\widetilde{L_2}(h) = L_2(MhM^{-1})$, $h \in \mathrm{End}(V_1)$. Consequently, f_2 can be seen in $C(\rho_1)$ so that $f_1 + f_2 \in C(\rho_1)$ and V_2 can be dropped. By updating r if necessary, we obtain (3.1). □

3.1. The particular case of subgroups

Let $\mathbf{G}$ be an algebraic group. The linearization of proper subgroups of $\mathbf{G}$ is Chevalley's theorem:

THEOREM 3.3 (Chevalley, [22]). — *Let* $\mathbf{H}$ *be a proper subgroup of* $\mathbf{G}$*, then there exist a rational representation* (ρ, V) *of* $\mathbf{G}$*, a line* D *in* V *such that* $\mathbf{H} = \{g \in \mathbf{G}; g \cdot D = D\}$*.*

In the particular case where the subgroup $\mathbf{H}$ is reductive, that is contains no proper connected unipotent subgroups, we have the following stronger statement:

PROPOSITION 3.4 ([7]). — *A subgroup* $\mathbf{H}$ *of* $\mathbf{G}$ *is reductive if and only if there exists a rational representation* (ρ, V) *of* $\mathbf{G}$*, a non zero vector* $x \in V$ *such that* $\mathbf{H}$ *is the stabilizer of* x *and such that* $\mathbf{G}x$ *is Zariski closed in* V*.*

4. Preliminaries on algebraic groups

4.1. The Cartan decomposition

Let $\mathbf{G}$ be a semisimple algebraic group defined over $\mathbb{R}$, G its group of real points, $\mathbf{A}$ be a maximal $\mathbb{R}$-split torus of $\mathbf{G}$, $X(\mathbf{A})$ be the group of $\mathbb{R}$-rational characters of $\mathbf{A}$, Δ the restricted root system of $\mathbf{A}$ in the Lie algebra of $\mathbf{G}$, Δ^+ the system of positive roots (for a fixed order) and Π the system of simple roots (roots than cannot be obtained as product of two positive roots).

We consider the natural order on $X(\mathbf{A})$: $\chi_1 > \chi_2$ if and only if there exist non negative integers $\{n_\alpha; \alpha \in \Pi\}$ with at least one non zero n_α such that $\frac{\chi_1}{\chi_2} = \prod_{\alpha\in\Pi} \alpha^{n_\alpha}$.

Finally define $A^\circ = \{a \in A; \chi(a) \in]0;+\infty[\ \forall \chi \in X(\mathbf{A})\}$ and set

$$A^+ = \{a \in A^\circ\ ;\ \alpha(a) \geqslant 1\ ;\ \forall \alpha \in \Pi\}.$$

Then there exists a compact subgroup K of G such that

$$G = KA^+K \qquad \text{Cartan or } KAK \text{ decomposition}$$

(see [21, Chapter 9, Theorem 1.1]).

We denote by $\mathfrak{a}$ the Lie algebra of $\mathbf{A}$. The exponential map is a bijection between A° and $\mathfrak{a}$. A Weyl chamber is $\mathfrak{a}^+ = \log A^+$. We denote by m the corresponding Cartan projection $m : G \longrightarrow \mathfrak{a}^+$.

4.2. Rational representations of algebraic groups

A reference for this section is [22] and [30]. If (ρ, V) is an $\mathbb{R}$-rational representation of $\mathbf{G}$ then $\chi \in X(\mathbf{A})$ is called a weight of ρ if it is a common eigenvalue of $\mathbf{A}$ under ρ. We denote by V_χ the weight space associated to χ which is $V_\chi = \{x \in V; \rho(a)x = \chi(a)x\ \forall\ a \in \mathbf{A}\}$. The following holds: $V = \oplus_{\chi\in X(\mathbf{A})} V_\chi$. Irreducible representations ρ are characterized by a particular weight χ_ρ called highest weight which has the following property: every weight χ of ρ different from χ_ρ is of the form $\chi = \frac{\chi_\rho}{\prod_{\alpha\in\Pi} \alpha^{n_\alpha}}$, where $n_\alpha \in \mathbb{N}$ for every simple root α. The V_χ's are not necessarily of dimension 1. When $\mathbf{G}$ is $\mathbb{R}$-split, V_{χ_ρ} is one dimensional. Recall that an element $\gamma \in GL_d(\mathbb{R})$ is called proximal if it has a unique eigenvalue of maximal modulus. A representation ρ of a group Γ is said to be proximal if the group $\rho(\Gamma)$ has a proximal element. Thus, we obtain

Lemma 4.1. — *Every $\mathbb{R}$-rational irreducible representation of an $\mathbb{R}$-split semisimple algebraic group is proximal*

Let $\Theta_\rho = \{\alpha \in \Pi;\ \chi_\rho/\alpha$ is a weight of $\rho\}$.

Proposition 4.2 ([30]). — *For every $\alpha \in \Pi$, let w_α be the fundamental weight associated to α. Then, there exists an $\mathbb{R}$-rational representation (ρ_α, V_α) of $\mathbf{G}$ whose highest weight is a power of w_α and whose highest weight space $V_{\chi_{\rho_\alpha}}$ is one-dimensional. Moreover, $\Theta_{\rho_\alpha} = \{\alpha\}$*

Mostow theorem [27, §2.6]**.** Let $G = KAK$ be the Cartan decomposition of G, (ρ, V) an irreducible rational real representation of $\mathbf{G}$. There exists a scalar product on V for which the elements of $\rho(K)$ are orthogonal and those of $\rho(A)$ are symmetric. In particular, the weight spaces are orthogonal with respect to it. The norm on V induced by this scalar product is qualified by "good".

4.3. Standard Parabolic subgroups and their representations

A reference for this section is [8, §4].

For every subset $\theta \subset \Pi$, denote $\mathbf{A}_\theta = \{a \in \mathbf{A}; \alpha(a) = 1 \forall \alpha \in \theta\}$ and let $\mathbf{L}_\theta$ be its centralizer in $\mathbf{G}$. Denote by $\mathfrak{g}$ the Lie algebra of $\mathbf{G}$ and for every $\alpha \in \Delta$ denote by $\mathbf{U}_\alpha$ the unique closed unipotent subgroup of $\mathbf{G}$ with Lie algebra: $\mathfrak{u}_\alpha = \mathfrak{g}_\alpha \oplus \mathfrak{g}_{2\alpha}$ where $\mathfrak{g}_{i\alpha} = \{X \in \mathfrak{g}; Ad(a)(X) = \alpha(a)^i X\ \forall a \in \mathbf{A}\}$.

Let $[\theta] \subset \Delta$ be the set of roots which can be written as integral combination of roots of θ. Denote by $\mathbf{U}_\theta$ the unipotent closed subgroup of $\mathbf{G}$ whose Lie algebra is

$$\mathfrak{u}_\theta = \bigoplus_{\alpha \in \Delta^+ \setminus ([\theta] \cap \Delta^+)} \mathfrak{u}_\alpha.$$

We set

$$\mathbf{P}_\theta = \mathbf{L}_\theta \mathbf{U}_\theta.$$

This is the standard parabolic subgroup associated to θ. Its Lie algebra is

$$\mathfrak{p}_\theta = \mathfrak{z} \oplus \bigoplus_{\alpha \in \Delta^+ \cup [\theta]} \mathfrak{u}_\alpha$$

where $\mathfrak{z}$ is the Lie algebra of $\mathbf{Z}$, the centralizer of $\mathbf{A}$ in $\mathbf{G}$. Notice that $\mathbf{P}_\Pi = \mathbf{G}$.

The following lemma will be useful to us for the proof of Theorem 1.6.

Lemma 4.3. — *Let (ρ, V) be a proximal rational irreducible representation of $\mathbf{G}$ and consider $\theta \subset \Pi$. Then the line generated by a highest weight vector of (ρ, V) is fixed by the parabolic subgroup $\mathbf{P}_\theta$ if $\beta \notin \Theta_\rho$ for every $\beta \in \theta$. In particular, the line generated by a highest weight vector x_α of the representation (ρ_α, V_α) defined in Proposition 4.2 is fixed by the standard parabolic $\mathbf{P}_\theta$ whenever $\alpha \notin \theta$.*

Proof. — Let χ_ρ be the highest weight of ρ. We look at the action of the Lie algebra $\mathfrak{g}$ on V. It is clear that $\mathfrak{g}_{-\beta} \cdot v \in V_{\chi_\rho - \beta}$ for every $v \in V_{\chi_\rho}$ and $\beta \in \Pi$. If $\beta \notin \Theta_\rho$, then $\chi_\rho - \beta$ is not a weight of ρ so that $V_{\chi_\rho - \beta} = 0$. Hence if θ is a subset of Π such that $\beta \notin \Theta_\rho$ for every $\beta \in \theta$, then the parabolic subgroup $\mathbf{P}_\theta$ stabilizes the highest weight space V_{χ_ρ}, which is the line generated by any highest weight vector (because ρ is assumed proximal). This proves the first part of the lemma. The last part follows immediately because the representation ρ_α defined in Proposition 4.2 satisfies $\Theta_{\rho_\alpha} = \{\alpha\}$ and its highest weight space is a line. $\square$

5. Random matrix products - convergence in the Cartan decomposition

We will use in this section standard results in the theory of random matrix products. A nice reference is the book of Bougerol and Lacroix [10].

5.1. Preliminaries

In the following, $G = \mathbf{G}(\mathbb{R})$ is the group of real points of a semisimple connected algebraic group, Γ a Zariski dense subgroup of G, μ a probability measure whose support generates Γ, (ρ, V) an irreducible $\mathbb{R}$-rational representation of $\mathbf{G}$ and χ_ρ its highest weight. Let $\{X_n; n \in \mathbb{N}^*\}$ be independent random variables on Γ with the same law μ and $S_n = X_n \cdots X_1$ the associated random walk . Fix a measurable section of the product map $K \times A \times K \to G$ and denote for every $n \in \mathbb{N}^*$, $S_n = K_n A_n U_n$ the corresponding decomposition of S_n. If θ is a probability measure on $GL_d(\mathbb{R})$, we denote by G_θ the smallest closed subgroup containing the support of θ.

We consider the basis of weights of V and the "good norm" given by Mostow theorem (Paragraph 4.2). It induces a K-invariant norm on $\bigwedge^2 V$ and hence a K-invariant distance $\delta(\cdot,\cdot)$ on the projective space $P(V)$, called Fubini-Study distance, defined by: $\delta([x],[y]) = \frac{||x \wedge y||}{||x|| ||y||}$; $[x],[y] \in P(V)$.

We fix an orthonormal basis on each weight space V_χ, and for an element $g \in \mathrm{End}(V)$, g^t will be the transpose matrix of g in this basis.

G is isomorphic to a Zariski closed subgroup of $SL_d(\mathbb{R})$ for some $d \in \mathbb{N}^*$ (see [22]). Let i be such an isomorphism. We say way that μ has a moment of order one (resp. an exponential moment) if for some (or equivalently any) norm on $\mathrm{End}(\mathbb{R}^d)$, $\int \log ||i(g)|| d\mu(g) < \infty$ (resp. for some $\tau > 0$, $\int ||i(g)||^\tau d\mu(g) < \infty$). Lemma 5.1 below shows that is indeed a well defined notion, *i.e.*, the existence of a moment of order one or an exponential moment is independent of the embedding.

Lemma 5.1. — *Let $G \subset SL(V)$ be the $\mathbb{R}$-points of a semisimple algebraic group $\mathbf{G}$ and $\mathbf{G} \xrightarrow{\rho} \mathbf{SL}_d$ a finite dimensional $\mathbb{R}$-algebraic representation of $\mathbf{G}$. If μ has a moment of order one (resp. an exponential moment) then the image of μ under ρ has also a moment of order one (resp. exponential moment).*

Proof. — Let us identify every $g \in G$ with a vector of $\mathbb{R}^{m^2}$, where $m = \dim(V)$. Since ρ is a rational representation, for every $i, j \in \{1, \cdots, d\}$, there exists a polynomial $P_{i,j}$ on m^2 variables such that for every $g \in G$, $\rho(g)_{i,j} = P_{i,j}(g)$. Consider the canonical norm on $\mathbb{R}^d$. In particular, $||g|| \geqslant 1$ for every $g \in G$. Then there exists a constant $C_{i,j} > 0$ depending only on the polynomial $P_{i,j}$ such that $||\rho(g)_{i,j}|| \leqslant ||g||^{C_{i,j}}$. Hence there exists $C > 0$, such that $||\rho(g)|| \leqslant ||g||^C$ for every $g \in G$. This ends the proof. □

Let us recall some definitions and well-known results.

Definition 5.2. — *A subgroup Γ of $GL_d(\mathbb{R})$ is called strongly irreducible if and only if the identity component of its Zariski closure does not fix a proper subspace. It is called proximal if it contains a proximal element (see Section 4).*

The key result which prevents our results from being generalized to an arbitrary local field is that Goldsheid-Margulis theorem below is valid only over $\mathbb{R}$.

Theorem 5.3 ([18]). — *Let $d \geqslant 2$. A strongly irreducible subgroup of $GL_d(\mathbb{R})$ is proximal if and only if its Zariski closure is.*

5.2. Geometry of the Lyapunov vector

First, let us recall the definition of the Lyapunov exponent.

Demonstration/Proposition 5.4 (Lyapunov exponent). — *If μ is a probability measure on $GL_d(\mathbb{R})$ having a moment of order one (see Section 5.1), $||\cdot||$ a matricial norm on* $\mathrm{End}(V)$, *$S_n = X_n \cdots X_1$ the corresponding random walk, then the Lyapunov exponent L_μ is $L_\mu = \lim \frac{1}{n}\mathbb{E}(\log ||S_n||)$ which exists by simple application of the subadditive lemma.*

Moreover, the following a.s. limit holds $L_\mu = \lim \frac{1}{n} \log ||S_n||$. It can be proved via the Kingman subadditive ergodic theorem [24].

A useful result will be the following

Proposition 5.5 ([10] Corollary 4, page 53). — *Let θ be a probability measure on $GL_d(\mathbb{R})$ with a moment of order one and such that $G_\theta := \overline{\langle \mathrm{Supp}(\theta)\rangle}$ is strongly irreducible. Then for every sequence $\{x_n; n \geqslant 0\}$ of vectors in $\mathbb{R}^d$ converging to some non zero vector $x \in \mathbb{R}^d$, $\frac{1}{n} \log ||S_n x_n|| \xrightarrow[n\to\infty]{a.s.} L_\theta$.*

Remark 5.6. — In [10], the condition is made on the smallest closed sub-semi-group Γ_θ containing the support of θ. There is no difference taking Γ_θ or G_θ because they have the same Zariski closure. Hence if one is strongly irreducible than the other satisfies the same property. This remark applies also for later applications when proximality is envolved (see for example the statement of Theorem 6.5). This is due to Goloshes-Margulis theorem (Theorem 5.3) which is special to the field of real numbers.

Demonstration/Proposition 5.7 (Lyapunov vector). — *Suppose that μ has a moment of order one. Then the Lyapunov vector is the constant vector in the Weyl chamber $\mathfrak{a}^+$ of G (see Section 4.1) defined as the following a.s. limit:*

$$\frac{1}{n} m(S_n) \xrightarrow[n\to\infty]{a.s} \mathrm{Liap}(\mu)$$

where m is the Cartan projection (Section 4.1).

Proof. — Let $\alpha \in \Pi$. Since the fundamental weights $(w_\beta)_{\beta\in\Pi}$ is a basis of $\mathfrak{a}^*$, there exists real numbers $(n_\beta)_{\beta\in\Pi}$ such that $\alpha = \prod_{\beta\in\Pi} w_\beta^{n_\beta}$. For every $\beta \in \Pi$, consider the rational real irreducible representation (ρ_β, V_β) given by Proposition 4.2 and a good norm on V_β (Paragraph 4.2). By the definition of ρ_β, there exists an integer l_β such that for every $n \in \mathbb{N}^*$, $||\rho_\beta(S_n)|| = w_\beta^{l_\beta}(A_n)$ (where A_n is the A-part of S_n in the KAK decomposition). Hence,

$$\frac{1}{n} \log\ \alpha(A_n) = \sum_{\beta\in\Pi} \frac{n_\beta}{l_\beta} \frac{1}{n} \log\ ||\rho_\beta(S_n)||. \tag{5.1}$$

By Definition/Proposition 5.4, $\lim \frac{1}{n} \log\ \alpha(A_n) \overset{a.s.}{=} \sum_{\beta\in\Pi} \frac{n_\beta}{l_\beta}\ L_{\rho_\beta(\mu)}$. Thus $\mathrm{Liap}(\mu)$ is well defined. ☐

THEOREM 5.8 ([20]). — *Suppose that μ has a moment of order one. Then the Lyapunov vector* $\mathrm{Liap}(\mu)$ *belongs to the interior of the Weyl chamber* $\mathfrak{a}^+$, *i.e.,* $\alpha\,(\mathrm{Liap}(\mu)) > 0\ \forall \alpha \in \Pi$.

Remark 5.9. — When the local field in not $\mathbb{R}$, the Lyapunov vector does not necessarily belong to the interior of $\mathfrak{a}^+$. The reason is that Goldsheid-Margulis theorem (Theorem 5.3) is valid only over the real field.

The following lemma describes the geometry of the Lyapunov vector inside the Weyl chamber.

LEMMA 5.10. — *Let Γ be a Zariski dense subgroup of G. Then for every finite union F of hyperplanes in $\mathfrak{a}$ (see Section 4.1 for the definition of $\mathfrak{a}$), there exist a probability measure μ on Γ with an exponential moment whose support generates Γ and whose Lyapunov vector* $\mathrm{Liap}(\mu)$ *is not included in F. In consequence, if $(V_1, \rho_1), \cdots, (V_r, \rho_r)$ are pairwise non isomorphic irreducible representations of* $\mathbf{G}$ *(with $r \geqslant 2$), then one can exhibit a probability measure μ whose support generates Γ, a permutation σ of $\{1, \cdots, r\}$ such that $L_{\rho_{\sigma(1)}(\mu)} > \cdots > L_{\rho_{\sigma(r)}(\mu)}$ (See Definition 5.4).*

Proof. — Let l_Γ be the cone in $\mathfrak{a}^+$ asymptote to $m(\Gamma)$ (we recall that m is the Cartan projection defined in Section 4.1). Y. Banjoist proved in [4] that l_Γ is convex and has a non empty interior. Hence, there exists an sub-cone C of l_Γ with non empty interior and whose intersection with every hyperplane of F is empty.

By [5, Proposition 5.1], there exists a sub-semi-group Γ' of Γ such that Γ' is Zariski dense and $l_{\Gamma'} = C$. Without loss of generality, we can assume Γ' finitely generated. Let μ be a finitely generated probability measure on Γ' whose support generates all of Γ'. Since, by the definition of the Lyapunov vector, $\mathrm{Liap}(\mu)$ belongs to the cone C, we deduce that $\mathrm{Liap}(\mu) \notin F$.

Let us perturb μ on Γ, that this define a sequence of probability measure μ_n with an exponential moment whose support generates Γ such that μ_n converge weakly to μ , for example $\mu_n = (1 - 1/n)\mu + \eta/n$ where η is a probability measure with an exponential moment whose support generates Γ. The strong irreducibility of Γ' and the definition of the top Lyapunov exponent by means of the unique stationary probability measure on the projective space (see for example) imply that the Lyapunov vector depends continuously on the probability measure: see for instance [10, Corollary 7.3, page 72-73]). Hence, $\mathrm{Liap}(\mu_n)$ converge to $\mathrm{Liap}(\mu)$. Hence, for n big enough, μ_n is a probability measure on Γ with $\mathrm{Liap}(\mu_n) \notin F$.

Now we prove the last part of the lemma. Let $\rho_1, \cdots, \rho_r$ be r rational real irreducible representations of $\mathbf{G}$ and denote by χ_{ρ_i} the highest weight of ρ_i.

Recall that the set Π of simple roots is a basis of the space $\mathbb{R}\otimes_{\mathbb{Z}}X(A)$, where $X(A)$ is the set of rational characters of A. Hence for every $i = 1, \cdots r$, there exist real numbers $\{n_{i,\alpha}; \alpha \in \Pi\}$ such that:

$$\log \chi_{\rho_i} = \sum_{\alpha\in\Pi} n_{i,\alpha} \log \alpha.$$

It can occur that one of the representations is trivial, say ρ_r. In this case, for every probability measure μ on Γ, the Lyapunov exponent is zero, *i.e.*, $L_{\rho_r(\mu)} = 0$. But in this case, Furstenberg theorem [17] ensures that for every $i = 1, \cdots, r-1$, $L_{\rho_i(\mu)} > 0$. Hence, without loss of generality, we can assume that all the representations are non trivial. . For every $i < j$, denote by $H_{i,j}$ the following hyperplane of $\mathfrak{a}$:

$$H_{i,j} = \{\chi_{\rho_i} = \chi_{\rho_j}\}.$$

Set $F = \cup_{i<j} H_{i,j}$. Applying the first part of the lemma shows that there exists a probability measure on Γ with an exponential moment such that $\mathrm{Liap}(\mu) \notin F$. This ends the proof because for every $i = 1, \cdots, r$,

$$L_{\rho_i(\mu)} = \lim \frac{1}{n} \log \chi_{\rho_i}(A_n).$$

$\square$

5.3. Estimates in the A-part

The following theorem gives an estimates in the A-part of the Cartan decomposition of the random walk. It can be proved by the same techniques as in [1] where the theory of random matrix products is treated over an arbitrary local field. However, since we are working here in $\mathbb{R}$, we will use another route and apply the large deviations theorem of Le Page [26] in $GL_d(\mathbb{R})$ we recall below. First, let us state our result:

THEOREM 5.11 (Ratio in the A-component). — *Suppose that μ has an exponential moment then for every $\epsilon > 0$ and every non zero weight χ of ρ distinct from χ_ρ,*

$$\limsup_{n\to\infty} \left[\mathbb{E}[(\frac{\chi(A_n)}{\chi_\rho(A_n)})^\epsilon]\right]^{\frac{1}{n}} < 1. \tag{5.2}$$

Moreover, if ρ_1, ρ_2 are two irreducible rational real representations of $\mathbf{G}$ such that $L_{\rho_1(\mu)} > L_{\rho_2(\mu)}$ (Definition 5.4), then for every small enough $\epsilon > 0$:

$$\limsup_{n\to\infty} \left[\mathbb{E}[(\frac{\chi_{\rho_2}(A_n)}{\chi_{\rho_1}(A_n)})^\epsilon]\right]^{\frac{1}{n}} < 1. \tag{5.3}$$

Before giving the proof, we recall Le Page large deviations theorem in $GL_d(\mathbb{R})$:

THEOREM 5.12 ([26] Large deviations in $GL_d(\mathbb{R})$). — *Let μ be a probability on $GL_d(\mathbb{R})$ having an exponential moment and such that G_μ is strongly irreducible. Let $S_n = X_n \cdots X_1$ be the corresponding random walk. Then for every $\epsilon > 0$,*

$$\limsup_{n\to\infty} \left[\mathbb{P}\left(\left|\frac{1}{n}\log ||S_n|| - L_\mu\right| > \epsilon\right)\right]^{\frac{1}{n}} < 1.$$

A similar estimate holds for $\frac{1}{n}\log ||S_n x||$ for every non zero vector $x \in \mathbb{R}^d$.

Proof of Theorem 5.11. — For every $\beta \in \Pi$, a similar large deviation inequality as in Theorem 5.12 holds for the quantity $\frac{1}{n}\log ||\rho_\beta(S_n)||$ because ρ_β is strongly irreducible and $\rho_\beta(\mu)$ has an exponential moment by Lemma 5.1. Hence by equation (5.1) a large deviation inequality holds for $\frac{1}{n}\log \alpha(A_n)$ for every $\alpha \in \Theta$. Since $\chi_\rho/\chi = \prod_{\alpha\in\Pi} \alpha^{n_\alpha}$ for non-negative integers $\{n_\alpha; \alpha \in \Pi\}$, we get for $\lambda = -\sum_{\alpha\in\Pi} n_\alpha \lim_{n\to\infty} \frac{1}{n}\log\ \alpha(A_n)$ and for every $\epsilon > 0$,

$$\limsup_{n\to\infty} \left[\mathbb{P}\left(\left|\frac{1}{n}\log\ \frac{\chi(A_n)}{\chi_\rho(A_n)} - \lambda\right| > \epsilon\right)\right]^{\frac{1}{n}} < 1. \tag{5.4}$$

By Theorem 5.8, $\lambda < 0$. Hence, by relation (5.4), there exists $C_1, C_2 > 0$ such that for all large n: $\mathbb{P}\left(\frac{\chi(A_n)}{\chi_\rho(A_n)} \geqslant \exp(-nC_1)\right) \leqslant \exp(-nC_2)$. Since $\chi(a) \leqslant \chi_\rho(a)$ for every $a \in A^+$, we get for every $\epsilon > 0$, $\mathbb{E}\Big[\left(\frac{\chi(A_n)}{\chi_\rho(A_n)}\right)^\epsilon\Big] \leqslant \exp(-nC_1) + \exp(-nC_2)$. This shows (5.2).

By the same large deviations techniques, we can show a similar estimate as (5.4) for the quotient $\frac{\chi_{\rho_2}(A_n)}{\chi_{\rho_1}(A_n)}$ with $\lambda = L_{\rho_2(\mu)} - L_{\rho_1(\mu)} < 0$. Hence, for some $C_3, C_4 > 0$,

$$\mathbb{P}\left(\frac{\chi_{\rho_2}(A_n)}{\chi_{\rho_1}(A_n)} \geqslant \exp(-nC_3)\right) \leqslant \exp(-nC_4). \tag{5.5}$$

If we assume the stronger condition that χ_{ρ_1} is strictly bigger than χ_{ρ_2}[(3)], then the conclusion of the proof can be done along the same lines as the proof of inequality (5.2). In order to cover the general case, it suffices to show that, for every small enough $\epsilon > 0$ we have:

$$\limsup_{n\to\infty} \left[\mathbb{E}\Big[\left(\frac{\chi_{\rho_2}(A_n)}{\chi_{\rho_1}(A_n)}\right)^\epsilon \mathbb{1}_{\frac{\chi_{\rho_2}(A_n)}{\chi_{\rho_1}(A_n)} \geqslant \exp(-nC_3)}\Big]\right]^{\frac{1}{n}} < 1. \tag{5.6}$$

(3) For an example when this condition can occur, see the proof of Theorem 1.5 in Section 6. For a situation when it doesn't (and therefore the probabilistic condition $L_{\rho_1(\mu)} > L_{\rho_2(\mu)}$ is needed), see Example 2 in Section 6.

Indeed, since μ has an exponential moment (see Section 5.1), then Lemma 5.1 shows that for every finite dimensional $\mathbb{R}$-algebraic representation ρ of $\mathbf{G}$, there exist $C_5 > 0$, $\epsilon_0 \in]0,1[$ such that: $\mathbb{E}\left(||\rho(X_1^{\pm 1})||^{\epsilon}\right) \leqslant \exp(C_5)$. By Jensen inequality, this implies that for every $\epsilon \in]0, \epsilon_0[$, $\mathbb{E}\left(||\rho(X_1)^{\pm 1}||^{\epsilon}\right) \leqslant \exp(\frac{C_5}{\epsilon_0}\,\epsilon)$. Applying this remark to the representations ρ_1, ρ_2, we get a new constant $C_6 > 0$ such that for every $\epsilon \in]0, \epsilon_0[$:

$$\mathbb{E}\Big[\left(\frac{\chi_{\rho_2}(A_n)}{\chi_{\rho_1}(A_n)}\right)^{\epsilon}\Big] \leqslant \exp(C_6 \epsilon\, n).$$

Combining the latter estimate, inequality (5.5) and the Cauchy-Schwartz inequality we get for every $\epsilon \in]0, \frac{\epsilon_0}{2}[$:

$$\mathbb{E}\Big[\left(\frac{\chi_{\rho_2}(A_n)}{\chi_{\rho_1}(A_n)}\right)^{\epsilon} \mathbb{1}_{\frac{\chi_{\rho_2}(A_n)}{\chi_{\rho_1}(A_n)} \geqslant \exp(-nC_3)}\Big] \leqslant \exp\left((\epsilon C_6 - \frac{C_4}{2})n\right).$$

The latter quantity decreases exponentially fast to zero if ϵ is chosen small enough. This proves (5.6). $\square$

5.4. Estimates in the K-parts and in the direction of the random walk

Recall that we fix a measurable section of the Cartan decomposition $G \to KAK$ and the corresponding decomposition of the random walk S_n is denoted by $S_n = K_n A_n U_n$. In this part, we recall some results we proved in our previous work [1]. The following result shows that the K-parts of the Cartan decomposition of S_n converges exponentially fast.

Theorem 5.13 ([1], Theorem 4.33. Exponential convergence of the K-components). — *Suppose that μ has an exponential moment and ρ is proximal. Let v_ρ be a highest weight vector. Then there exists a random variable Z on the projective space $P(V)$ such that for every $\epsilon > 0$:*

$$\limsup_{n\to\infty} \left[\mathbb{E}\left(\delta(U_n^{-1}\cdot[v_\rho], Z)^{\epsilon}\right)\right]^{\frac{1}{n}} < 1.$$

Here, for $M \in GL(V)$, we have denoted by M^t the transpose matrix of M with respect to the basis of weights. We recall that δ is the Fubini-Study distance (see the beginning of Section 5.1). In particular, $U_n^{-1}\cdot[v_\rho]$ converges a.s. towards Z. Moreover, the law of Z is the unique $\rho(\mu)^t$-invariant probability measure on $P(V)$ (see for example [10, Proposition 3.2 page 50]*). A similar estimate holds if we replace U_n with $k(X_1\cdots X_n)$ where $k(g)$ is the K-component of $g \in G$ for the fixed KAK decomposition in G.*

A crucial result we will need in the next section is the asymptotic independence in the K-parts.

Theorem 5.14 ([1], Theorem 4.35. Asymptotic independence of the K-components). — *With the same assumptions as in Theorem 5.13, there exist* ***independent random variables*** *Z and T with respective laws the unique $\rho(\mu)^t$ (resp. $\rho(\mu)$)- invariant probability measure on $P(V)$ such that for every small enough $\epsilon > 0$, every ϵ-holder (real) function ϕ on $P(V) \times P(V)$ and all large n we have:*

$$\left|\mathbb{E}\left(\phi([U_n^{-1} \cdot v_\rho], [K_n \cdot v_\rho])\right) - \mathbb{E}\left(\phi(Z,T)\right)\right| \leqslant ||\phi||_\epsilon \rho(\epsilon)^n$$

where $||\phi||_\epsilon = \operatorname*{Sup}_{[x],[y],[x'],[y']} \frac{\left|\phi([x],[x'])-\phi([y],[y'])\right|}{\delta([x],[y])^\epsilon+\delta([x'],[y'])^\epsilon}$.

Finally, we quote the following result of [1] which holds in the more general context of random walks on linear groups over local fields[4]. It shows that the direction $S_n[x]$, where $x \in \mathbb{R}^d \setminus \{0\}$, can be inside a fixed hyperplane, with only a probability decreasing exponentially fast to zero.

Theorem 5.15 ([1], Theorem 4.18). — *Let k be a local field and μ be a probability measure on $GL_d(k)$ with an exponential moment, such that the smallest closed group G_μ containing the support of μ is strongly irreducible and proximal, then*

$$\limsup_{n \to +\infty} \frac{1}{n} \log \mathbb{P}\left(S_n[x] \in H\right) < 0 \tag{5.7}$$

uniformly on $x \in k^d \setminus \{0\}$ and the hyperplanes H of k^d.

6. Proof of the main theorems

The proof of the main theorems we presented in the introduction is based on the following

Theorem 6.1. — *Let $\mathbf{G}$ be a semisimple algebraic group defined over $\mathbb{R}$, G its group of real points, let (ρ, V) be a non trivial rational real representation of $\mathbf{G}$ such that its irreducible sub-representations $(\rho_1, V_1), \cdots, (\rho_r, V_r)$ are pairwise non isomorphic and let finally $A \in \operatorname{End}(V_1) \oplus \cdots \oplus \operatorname{End}(V_r)$ such that its projection on $\operatorname{End}(V_1)$ is non zero. Consider a probability measure μ on G with an exponential moment and such that $G_\mu := \overline{\langle \operatorname{Supp}(\mu) \rangle}$ is Zariski dense in G. Denote by $\{S_n; n \geqslant 0\}$ the corresponding random walk. Assume that :*

[4] A local field is isomorphic either to $\mathbb{R}$, $\mathbb{C}$, a p-adic field, or a field of Laurent series over a finite field.

(1) *ρ_1 is proximal.*
(2) *$L_{\rho_1(\mu)} > L_{\rho_i(\mu)}$, $i = 2, \cdots, r$ (see Definition 5.4).*

Then for every $\epsilon > 0$ there exists $\rho(\epsilon) \in]0,1[$ such that for all large n:

$$\mathbb{P}\Big(\big| \frac{1}{n} \log |\operatorname{Tr}(\rho(S_n)A)| - L_{\rho_1(\mu)} \big| > \epsilon \Big) \leqslant \rho(\epsilon)^n.$$

In particular, $\operatorname{Tr}(\rho(S_n)A)$ vanishes only with a probability decreasing exponentially fast to zero, and $\frac{1}{n}\log\Big|\operatorname{Tr}(\rho(S_n)A)\Big|$ converges a.s. towards $L_{\rho_1(\mu)}$.

Assumption 1 in Theorem 6.1 is fulfilled whenever $\mathbf{G}$ is $\mathbb{R}$-split (see Lemma 4.1). We provide two sufficient conditions for assumption 2 to hold: a probabilistic one and a determinist (algebraic) one.

Remark 6.2 (A probabilistic sufficient conditions for assumption 2*).* — Lemma 5.10 proves that assumption 2 is fulfilled whenever the Lyapunov vector $\operatorname{Liap}(\mu)$ does not belong to a finite union of hyperplanes in the Weyl chamber $\mathfrak{a}^+$.

Remark 6.3 (An algebraic sufficient conditions for assumption 2*).* — Let χ_i be the highest weight of V_i, $i = 1, \cdots, r$. A necessary condition for 2 to hold is that $\chi_1/\chi_i = \prod_{\alpha\in\Pi} \alpha^{n_\alpha}$ for some non negative integers $\{n_\alpha; \alpha \in \Pi\}$ with at least one non zero n_α. This is easily checked using the fact that the Lyapunov vector is in the interior of the weal chamber (Theorem 5.8).

See the applications of this remark in the proof of Theorem 1.5

Proof. — To simplify notation, we can assume $r = 2$. Let $d = \dim(V)$, $p = \dim(V_1)$, $B_1 = (v_1, \cdots, v_p)$ (resp. $B_2 = (v_{p+1}, \cdots, v_d)$) a basis of V_1 (resp. V_2) consisting of weight vectors. We impose v_1 and v_{p+1} to be a highest weight vectors. This gives a basis $B = (B_1, B_2)$ of V. The scalar products on V_1 and V_2 given by Theorem 4.2 induce naturally a scalar product on V for which V_1 and V_2 are orthogonal. In the basis B, $\rho(A_n) = \operatorname{diag}(\rho_1(A_n), \rho_2(A_n)) = \operatorname{diag}(a_1(n), \cdots, a_d(n))$ with $a_1(n) = \chi_{\rho_1}(A_n)$ and $a_{p+1}(n) = \chi_{\rho_2}(A_n)$ (notations of Section 4). Let W_{ρ_i} be the set of non zero weights of (V_i, ρ_i), $i = 1, 2$. A simple computation gives:

$$\begin{aligned}
\operatorname{Tr}(\rho(S_n)A) &= \operatorname{Tr}(\rho(K_n)\rho(A_n)\rho(U_n)A) = \operatorname{Tr}(\rho(A_n)\rho(U_n)A\rho(K_n)) \\
&= \sum_{i=1}^{d} a_i(n)\langle \rho(K_n)v_i, A^t\rho(U_n)^t v_i\rangle
\end{aligned}$$

where $S_n = K_nA_nU_n$ is the Cartan decomposition of S_n (see Section 4.1). Since ρ_1 is proximal, $a_2(n) = \chi(A_n)$ for some weight $\chi \in W_{\rho_1}$ distinct from

χ_ρ. Then,

$$\mathrm{Tr}(\rho(S_n)A) = \chi_{\rho_1}(A_n)\Big[\langle K_n\cdot v_{\rho_1}, A^t U_n^{-1}\cdot v_{\rho_1}\rangle + \sum_{\chi\neq\chi_{\rho_1}\in W_{\rho_1}} O\left(\frac{\chi(A_n)}{\chi_{\rho_1}(A_n)}\right) + \sum_{\chi\in W_{\rho_2}} O\left(\frac{\chi(A_n)}{\chi_{\rho_1}(A_n)}\right)\Big].$$

Le Page large deviations theorem (Theorem 5.12) shows that for every $\epsilon > 0$ and some $\rho \in]0,1[$:

$$\mathbb{P}\left(\exp(nL_{\rho_1(\mu)} - n\epsilon) \leqslant \chi_{\rho_1}(A_n) \leqslant \exp(nL_{\rho_1(\mu)} + n\epsilon)\right) \geqslant 1-\rho^n.$$

Next we show that for every $\chi \neq \chi_{\rho_1} \in W_{\rho_1}$ and $\chi \in W_{\rho_2}$ and every small enough $\epsilon > 0$:

$$\limsup_{n\to\infty}\left[\mathbb{E}\left(\frac{\chi(A_n)}{\chi_\rho(A_n)}\right)^{\epsilon}\right]^{\frac{1}{n}} < 1.$$

Indeed, for $\chi \neq \chi_{\rho_1} \in W_{\rho_1}$, this follows from Theorem 5.11 and the fact that ρ_1 is proximal. For $\chi \in W_{\rho_2}$, this follows also from Theorem 5.11 and Assumption 2.

Hence, by the Marked property, there exist $\epsilon_1, \epsilon_2 \in]0,1[$ such that for all n large enough: $\mathbb{P}\left(\frac{\chi(A_n)}{\chi_\rho(A_n)} \geqslant \epsilon_1^n\right) \leqslant \epsilon_2^n$. The following proposition applied to the (non trivial) projection of A on V_1 and to the representation (ρ_1, V_1) ends the proof. $\square$

Proposition 6.4. — *Let $\mathbf{G}$ be a semisimple algebraic group defined over $\mathbb{R}$, G its group of real points, Γ a Zariski dense subgroup of G, (ρ, V) an irreducible rational real representation of $\mathbf{G}$, μ a probability measure with an exponential moment and whose support generates Γ. If ρ is proximal, then for any non zero endomorphism $A \in \mathrm{End}(V)$, every $t \in]0,1[$,*

$$\limsup_{n\to\infty}\left[\mathbb{P}\left(|\langle K_n\cdot v_\rho, AU_n^{-1}\cdot v_\rho\rangle| \leqslant t^n\right)\right]^{\frac{1}{n}} < 1$$

where v_ρ is a highest weight vector.

Before giving the proof, we recall the following remarkable theorem of Guitar'h:

Theorem 6.5 ([19]). — *Let μ be a probability measure on $GL_d(\mathbb{R})$ having an exponential moment and such that G_μ is strongly irreducible and proximal. Denote by ν the unique μ-invariant probability measure on* *the projective space $P(\mathbb{R}^d)$. Then there exists $\alpha > 0$ (small enough) such that:*

$$\mathrm{Sup}\left\{\int \frac{1}{\left|\left\langle \frac{x}{||x||}, \frac{y}{||y||}\right\rangle\right|^{\alpha}} d\nu([x]) \;\; ; \;\; y \in \mathbb{R}^d \setminus \{0\}\right\} < \infty.$$

In particular, if Z is a random variable with law ν, there exists a constant $C > 0$ such that:

$$\mathrm{Sup}\left\{\mathbb{P}\Big(\Big|\Big\langle Z, \frac{x}{||x||}\Big\rangle\Big| \leqslant \epsilon);\;\; x \in \mathbb{R}^d \setminus \{0\}\right\} \leqslant C\epsilon^{\alpha}.$$

Proof of Proposition 6.4.

- Let η the function defined on $P(V) \times P(V) \to \mathbb{R}$ by $\eta([x],[y]) = |\langle x, Ay\rangle|$ where x and y are two representative of $[x]$ and $[y]$ in the sphere of radius one. The function η is lipstick with lipstick constant $\leqslant \mathrm{Max}\{1, ||A||\}$.
- For every $a > 0$, let ψ_a be the function defined on $\mathbb{R}$ by $\psi_a(x) = 1$ if $x \in [-a; a]$; affine on $[-2a; -a[\cup]a, 2a]$ and zero otherwise. One can easily verify that ψ_a is lipstick with constant equal to $\frac{1}{a}$.

  Note also that

$$\mathbb{1}_{[-a,a]} \leqslant \psi_a \leqslant \mathbb{1}_{[-2a,2a]}. \tag{6.1}$$

Define for $a > 0$, $\phi_a = \psi_a \circ \eta$. By the previous remarks, ϕ_a is lipstick with lipstick constant: $||\phi_a|| \leqslant \frac{\mathrm{Max}\{1,||A||\}}{a}$.

By Theorem 5.14 there exist independent random variables Z and T in $P(V)$ such that for any $t \in]0, 1[$, we have:

$$\mathbb{P}(|\langle K_n \cdot v_\rho, AU_n^{-1} \cdot v_\rho\rangle| \leqslant t^n) \leqslant \mathbb{E}\left(\phi_{t^n}([K_n \cdot v_\rho], [U_n{}^{-1} \cdot v_\rho])\right) \tag{6.2}$$

$$\leqslant \mathbb{E}\left(\phi_{t^n}(Z, T)\right) + ||\phi_{t^n}||\rho^n \tag{6.3}$$

$$\leqslant \mathbb{P}(|\langle Z, AT\rangle| \leqslant 2t^n) + \mathrm{Max}\{1, ||A||\}\frac{\rho^n}{t^n}. \tag{6.4}$$

In the last line, we confused between Z and T in $P(V)$ and some representative in the unit sphere. The bounds (6.2) and (6.4) follow from (6.1).

To prove our proposition, we can clearly suppose $t \in]\rho, 1[$. It suffices then to show that $\mathbb{P}(|\langle Z, AT\rangle| \leqslant 2t^n)$ is sub-exponential. The law of T is the unique $\rho(\mu)^t$-invariant probability measure ν on $P(V)$ (Theorem 5.14). Moreover, a general lemma of Furstenberg (see for example [10, Proposition 2.3 page 49]) shows that ν is proper, *i.e.*, does not charge any projective hyperplane. Hence, a.s. $AT \neq 0$. Moreover, we claim that the following stronger statement holds : there exist $D, \alpha > 0$ such that for every $t' \in]0,1[$ and $n \in \mathbb{N}^*$:

$$\mathbb{P}(||AT|| \leqslant t'^n) \leqslant Dt'^{n\alpha} \tag{6.5}$$

Indeed, A being a non zero endomorphism, there exist a non zero vector of norm one, v_0 such that $A^t v_0 \neq 0$. Then by Theorem 6.5,

$$\mathbb{P}(||AT|| \leqslant t'^n) \leqslant \mathbb{P}(|\langle AT, v_0\rangle| \leqslant t'^n) \leqslant \mathbb{P}(|\langle T, A^t v_0\rangle| \leqslant t'^n) \leqslant \frac{C}{||A^t v_0||^\alpha} t'^{n\alpha}.$$

Set $D = C/||A^t v_0||^\alpha$. Hence for every $t' \in]t, 1[$,

$$\begin{aligned}\mathbb{P}(|\langle Z, AT\rangle| \leqslant 2t^n) &= \mathbb{P}(|\langle Z, \frac{AT}{||AT||}\rangle| \leqslant 2\frac{t^n}{||AT||})\\ &\leqslant \mathbb{P}\left(|\langle Z, \frac{AT}{||AT||}\rangle| \leqslant 2(t/t')^n\right) + Dt'^{n\alpha}\\ &\leqslant \mathrm{Sup}\{\mathbb{P}\left(\delta(Z,[H]) \leqslant 2(t/t')^n\right);\\ &\qquad\qquad H \text{ hyperplane of } V\} + Dt'^{n\alpha}.\end{aligned}$$

We recall that δ is the Fubini-Study distance on the projective space. The last line is by independence of Z and T. Theorem 6.5 shows that it decreases exponentially fast to zero. □

As an application, we give the

Proof of Theorem 1.2. — Lemma 3.2 allows us to be in the situation of Theorem 6.1, *i.e.*, , we have a non trivial representation (ρ, V) whose irreducible sub-representations $\rho_1, \cdots, \rho_r$ are pairwise non isomorphic, a endomorphism $A \in \mathrm{End}(V_1) \oplus \cdots \oplus \mathrm{End}(V_r)$ whose restriction to each $\mathrm{End}(V_i)$ non zero such that $\mathcal{V} = \{g \in G; \mathrm{Tr}\,(\rho(g)A) = 0\}$. For every $i = 1, \cdot, r$, let χ_{ρ_i} be the highest weight of ρ_i. As in the proof of Lemma 5.10, for every $i < j$, denote by $H_{i,j}$ the following hyperplane of the Weyl chamber: $H_{i,j} = \{\chi_{\rho_i} = \chi_{\rho_j}\}$ and $F = \cup_{i,j} H_{i,j}$. Assuming that $\mathrm{Liap}(\mu) \notin F$ implies that one of the Lyapunov exponents $L_{\rho_i(\mu)}$, $i = 1, \cdots, r$ is the biggest. Without loss of generality, we can assume that $L_{\rho_1(\mu)} > L_{\rho_i(\mu)}$ for every $i \in \{2, \cdots, r\}$. Since $\mathbf{G}$ is split over $\mathbb{R}$, Lemma 4.1 shows that the representation ρ_1 is proximal. It suffices now to apply Theorem 6.1. □

Proof of Theorem 1.5. — For every $k \in \mathbb{N}$, let $\mathrm{Sym}^k(\mathbb{R}^d)$ be the vector space of homogenous polynomials on d variables of degree k. The group $SL_d(\mathbb{R})$ acts on $\mathrm{Sym}^k(\mathbb{R}^d)$ by the formula:

$$g.P(X_1, \cdots, X_d) = P\left(g^{-1}(X_1, \cdots, X_d)\right)$$

for every $g \in SL_d(\mathbb{R})$, $P \in \mathrm{Sym}^k(\mathbb{R}^d)$. A known fact (see for example [16]) is that the action of $\mathrm{SL}_d(\mathbb{R})$ on $\mathrm{Sym}^k(\mathbb{R}^d)$ is irreducible for every $k \in \mathbb{N}$.

Consider now a proper algebraic hypersurface $\widetilde{\mathcal{V}}$ of $\mathbb{R}^d$ defined over $\mathbb{R}$, a non zero vector x of $\mathbb{R}^d$ and denote $\mathcal{V} = \{g \in SL_d(\mathbb{R}); gx \in \widetilde{\mathcal{V}}\}$. Let now P be the polynomial that defines $\widetilde{\mathcal{V}}$, k its degree. The polynomial P can be seen as a vector in $V = \oplus_{i=0}^{k} \mathrm{Sym}^i(\mathbb{R}^d)$. Let ρ_i be the action of $SL_d(\mathbb{R})$ on $\mathrm{Sym}^i(\mathbb{R}^d)$. If P_i denotes projection of P on $\mathrm{Sym}^i(\mathbb{R}^d)$, then "$gx \in \mathcal{V} \Leftrightarrow P(gx) = 0 \quad \Leftrightarrow \quad \sum_{i=0}^{k} f_i(g^{-1}) = 0$" where $f_i(g) = \rho_i(g)(P_i)(x) \in C(\rho_i)$ (see Definition 3.1). Moreover, the highest weight of $\mathrm{Sym}^i(\mathbb{R}^d)$ is strictly bigger (for the natural order on $X(\mathbf{A})$ defined in Section 4.1) than the one of $\mathrm{Sym}^{i-1}(\mathbb{R}^d)$, the ratio being the highest weight of the natural representation of $SL_d(\mathbb{R})$ on $\mathbb{R}^d$. We can then apply Remark 6.3 and Theorem 6.1 to the probability measure μ^{-1}. $\square$

An application of the results of Section 5 independent from Theorem 6.1 is the

Proof of Theorem 1.6. — If the identity component $\mathbf{H}^0$ of $\mathbf{H}$ is reductive, then by Proposition 3.4, there exist a rational representation (ρ, V) of $\mathbf{G}$ and a non zero vector $x \in V$ such that the reductive group $\mathbf{H}^0$ is the stabilizer of x and the orbit of x is Zariski closed. Let $V = \oplus_{i=1}^{r} V_r$ be the decomposition of V into irreducible sub-representations and $x = x_1 + \cdots + x_r$ the corresponding decomposition of x. Since $\mathbf{H}^0$ is the stabilizer of the vector x, then $\mathbf{H}^0 = \bigcap_{i=1}^{r} \mathbf{G}_{x_i}$ where $\mathbf{G}_{x_i}$ is the stabilizer of x_i in $\mathbf{G}$. Since $\mathbf{H}^0$ is proper, there exists $i = 1, \cdots, r$ such that $\mathbf{G}_{x_i}$ is proper. Hence, by replacing the representation V with V_i and the subgroup $\mathbf{H^0}$ with the proper subgroup $\mathbf{G}_{x_i}$, we can assume that (ρ, V) is irreducible and non-trivial. If $h_1, \cdots, h_s$ denote the closets of the finite group H/H^0, then we can write

$$\mathbb{P}(S_n \in H) \leqslant \sum_{i=1}^{s} \mathbb{P}(S_n h_i^{-1} \cdot x = x) \leqslant \sum_{i=1}^{s} \mathbb{P}\left(||\rho(S_n) \frac{h_i^{-1} \cdot x}{||x||}|| = 1 \right).$$

Since G has no compact factors, $\rho(G)$ is non compact. In particular, $\rho(G_\mu)$ is not contained in a compact subgroup of $SL(V)$ because compact subgroups of $SL(V)$ are algebraic and $\rho(G_\mu)$ is Zariski dense in $\rho(G)$. Hence we can apply Furstenberg theorem ([17]) which shows that $L_{\rho(\mu)} > 0$ (see Definition 5.4). Applying Le Page large deviations theorem (Theorem 5.12) shows that for every $i = 1, \cdots, s$, $\mathbb{P}\left(||S_n \cdot (h_i^{-1} \cdot x)|| \leqslant \exp(nL_{\rho(\mu)}/2)\right)$ decreases exponentially fast to zero [5].

[5] If the representation ρ is proximal, we can use only the fact that $\mathbf{H}^0$ fixes the line generated by the vector x and apply Theorem 5.15 instead of Le Page Large deviations theorem.

If $\mathbf{H}^0$ is not reductive, then it contains a unipotent Zariski connected $\mathbb{R}$-subgroup $\mathbf{U}$ which is normal in $\mathbf{H}^0$. Hence $\mathbf{H}^0 \subset N(\mathbf{U})$, where $N(\mathbf{U})$ is the normalizer of $\mathbf{U}$ in $\mathbf{G}$. By [9, Corollary 3.9], there is an $\mathbb{R}$-parabolic subgroup $\mathbf{P}$ of $\mathbf{G}$ such that $N(\mathbf{U}) \subset \mathbf{P}$. By [8, Proposition 5.14], $\mathbf{P}$ is conjugated to one of the standard parabolic subgroups $\mathbf{P}_\theta$, $\theta \subsetneq \Pi$ described in Section 4.3. Hence, by Lemma 4.3, $\mathbf{P}_\theta$ fixes the line generated by the highest weight x_α of (ρ_α, V_α) for every $\alpha \notin \theta$. Fix such α. Hence,

$$\mathbf{H}^0 \subset \{g \in \mathbf{G}^0; g \cdot [x_\alpha] = [x_\alpha]\}.$$

As in the previous paragraph, denote by $h_1, \cdots, h_s$ the closets of the finite group H/H^0. Hence,

$$\mathbb{P}(S_n \in H) \leqslant \sum_{i=1}^{s} \mathbb{P}(\rho_\alpha(S_n)[h_i^{-1} x_\alpha] = [x_\alpha]). \tag{6.6}$$

The representation ρ_α is G-irreducible hence by connectedness, strongly irreducible. Moreover, it is proximal because $\Theta_{\rho_\alpha} = \{\alpha\}$, its highest weight space is a line and G has no compact factors. By Goloshes-Margulis theorem (Theorem 5.3), $\rho_\alpha(\Gamma)$ is proximal. Hence we can apply Theorem 5.15 which proves the exponential decay of the probability (6.6). □

7. Application to generic Zariski density and to free subgroups of linear groups

7.1. Statement of the results and commentaries

Let $\mathbf{G}$ be a semisimple algebraic group defined over $\mathbb{R}$ and G its group of real points.

Question 7.1. — Let Γ be a Zariski dense subgroup of G. Is it true that two “random” elements in Γ generate a Zariski dense subgroup of G.

A motivation for this question is the following

Question 7.2. — By the Tits alternative [31], any Zariski dense subgroup Γ of G contains a Zariski dense free subgroup on two generators. A natural question is to see if this property is generic. In [1, Theorem 1.1], we proved that two “random” elements in Γ generate a free subgroup. The question that arises immediately is to see if the latter subgroup is Zariski dense.

In recent works of Rivin [29], he showed the following:

THEOREM 7.3 ([29], Corollary 2.11). — *Let* $\mathbf{G} = \mathbf{SL_d}$ *and* $\Gamma = SL_d(\mathbb{Z})$ *for some* $d \geqslant 3$. *Consider the uniform probability measure on a finite symmetric generating set and denote by* $\{S_n, n \geqslant 0\}$ *the associated random walk. Then, for any* $g \in \Gamma$, *there exists a constant* $c(g) \in]0,1[$ *such that*

$$\mathbb{P}(\langle g, S_n\rangle \text{is Zariski dense}) \geqslant 1 - c(g)^n.$$

Moreover, $c(g)$ *is effective.*

Passing from the "1.5 random subgroup" in Theorem 7.3 to the subgroup generated by two random elements is delicate since the constant $c(g)$ depends among others things on the norm of g.

Using our Theorem 1.2, we will prove the following

THEOREM 7.4. — *Let* G *be the group of real points of a semisimple algebraic group defined and split over* $\mathbb{R}$. *Let* Γ_1, Γ_2 *be two Zariski dense subgroups of* G. *Then there exists probability measures* μ_1 *and* μ_2 *respectively on* Γ_1 *and* Γ_2 *with an exponential moment such that for some* $c \in]0,1[$ *and all large* n,

$$\mathbb{P}(\langle S_{1,n}, S_{2,n}\rangle \text{ is Zariski dense and free}) \geqslant 1 - c^n$$

where $\{S_{2,n}; n \geqslant 0\}$ *and* $\{S_{2,n}, n \geqslant 0\}$ *are two independent random walks on* Γ_1 *(resp.* Γ_2*) associated respectively to* μ_1 *and* μ_2. *This implies that almost surely, for* n *big enough, the subgroup* $\langle S_{1,n}, S_{2,n}\rangle$ *is Zariski dense and free.*

When $\mathbf{G} = \mathbf{SL_2}$, a stronger statement holds. It will follow immediately from our result in [1].

THEOREM 7.5. — *Let* Γ_1, Γ_2 *be two Zariski dense subgroups of* $SL_2(\mathbb{R})$. *Then for any probability measures* μ_1 *and* μ_2 *with an exponential moment whose support generates respectively* Γ_1 *and* Γ_2, *there exists* $c \in]0,1[$ *such that*

$$\mathbb{P}(\langle S_{1,n}, S_{2,n}\rangle \text{ is Zariski dense}) \geqslant 1 - c^n.$$

Remark 7.6. — Let us compare Theorem 7.4 with Rivin's Theorem 7.3. The advantage of our method is that it allows us to consider two elements at random and not a "1.5 random subgroup", which is crucial to solve Question 7.2. Furthermore, we do not necessarily consider arithmetic groups, neither finitely generated groups: any Zariski dense subgroup Γ works. In addition to that, the statement shows that Zariski density is generic for a pair of random elements taken in two groups Γ_1 and Γ_2 not necessarily equal.

However, the big inconvenient is that our constants are not effective unlike Rivin's. Our result can be applied to prove the "1.5 random subgroup" but is less interesting than Rivin results since we don't know if the uniform probability measure on a finite symmetric generating of $SL_d(\mathbb{Z})$ works.

For $d=2$, Theorem 7.5 is more satisfying; there is no restrictions neither on μ_1 nor μ_2.

7.2. Proofs

Proof of Theorem 7.5. — A subgroup of $SL_2(\mathbb{R})$ is Zariski dense if and only it is not solvable. In particular, a free subgroup of $SL_2(\mathbb{R})$ is always Zariski dense. But in Theorem [1, Theorem 2.11], we proved that with the same assumptions as in Theorem 7.5, $\mathbb{P}(\langle S_{1,n}, S_{2,n}\rangle$ is not free) decreases exponentially fast. □

Proof of Theorem 7.4. — The key point is the following

Lemma 7.7 ([13], Lemma 6.8). — *Let k be a field of characteristic zero, $\mathbf{G}$ be a semisimple group defined over k, $G=\mathbf{G}(k)$. Then there exists a proper algebraic variety $\mathcal{W}$ of $\mathbf{G}\times\mathbf{G}$ defined over k such that any pair of elements $x,y\in G$ generate a Zariski dense subgroup unless $(x,y)\in\mathcal{W}(k)$.*

By Lemma 3.2, there exist a non trivial rational real representation (ρ, V) of $\mathbf{G}\times\mathbf{G}$, an endomorphism $A\neq 0\in \mathrm{End}(V_1)\oplus\cdots\oplus\mathrm{End}(V_r)$ such that

$$\mathcal{W}\subset\{(g,h)\in\mathbf{G}\times\mathbf{G};\ \mathrm{Tr}\,(\rho(g,h)A)=0\} \tag{7.1}$$

Let $\rho_1,\cdots,\rho_r$ the irreducible sub-representations of ρ. Since $\Gamma_1\times\Gamma_2$ is Zariski dense in $\mathbf{G}\times\mathbf{G}$, the proof of Lemma 5.10 shows that there exist two probability measures μ_1 and μ_2 respectively on Γ_1 and Γ_2, a permutation σ of $\{1,\cdots,r\}$ such that $L_{\rho_{\sigma(i)}(\mu_1\otimes\mu_2)} > L_{\rho_{\sigma(i+1)}(\mu_1\otimes\mu_2)}$ for $i=1,\cdots,r$. Let T_n be the random walk $(S_{1,n},S_{2,n})$ on $\Gamma_1\times\Gamma_2$ (*i.e.*, the one corresponding to the probability measure $\mu_1\otimes\mu_2$.) By Lemma 7.7 and identity (7.1),

$$\mathbb{P}(\langle S_{n,1},S_{n,2}\rangle \text{ is not Zariski dense in } G)\leqslant \mathbb{P}\Big(\,\mathrm{Tr}\,(\rho(T_n)A)=0\Big). \tag{7.2}$$

Theorem 6.1 shows that the latter quantity decreases exponentially fast to zero. □

8. Open problems and questions

- It is interesting to see if the probabilistic methods we used can generalize Theorem 1.2. More precisely, if μ is a probability measure with an exponential moment and whose support generates a Zariski dense subgroup of the real points of a semisimple algebraic group $\mathbf{G}$, is it true that for every proper algebraic subvariety $\mathcal{V}$ of $\mathbf{G}$,

$$\limsup \left[\mathbb{P}(S_n \in \mathcal{V})\right]^{\frac{1}{n}} < 1$$

where S_n the random walk associated to μ.

- The same question for Theorem 7.4 (*i.e.*, replace there exists by for all, and do not assume the semisimple algebraic group $\mathbf{G}$ $\mathbb{R}$-split.)

BIBLIOGRAPHY

[1] R. Aoun, "Random subgroups of linear groups are free.", *Duke Math. J.* **160** (2011), no. 1, p. 117-173 (English).

[2] P. de lya Arp, R. I. Grigorchuk & T. Chekerini-Sil'berstaĭn, "Amenability and paradoxical decompositions for pseudogroups and discrete metric spaces", *Tr. Mat. Inst. Steklova* **224** (1999), no. Algebra. Topol. Differ. Uravn. i ikh Prilozh., p. 68-111.

[3] M. Bekka, "Amenable unitary representations of locally compact groups", *Invent. Math.* **100** (1990), no. 2, p. 383-401.

[4] Y. Benoist, "Propriétés asymptotiques des groupes linéaires", *Geom. Funct. Anal.* **7** (1997), no. 1, p. 1-47.

[5] ———, "Propriétés asymptotiques des groupes linéaires. II", in *Analysis on homogeneous spaces and representation theory of Lie groups, Okayama–Kyoto (1997)*, Adv. Stud. Pure Math., vol. 26, Math. Soc. Japan, Tokyo, 2000, p. 33-48.

[6] ———, "Convexes divisibles. I", in *Algebraic groups and arithmetic*, Tata Inst. Fund. Res., Mumbai, 2004, p. 339-374.

[7] A. Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991, xii+288 pages.

[8] A. Borel & J. Tits, "Groupes réductifs", *Inst. Hautes Études Sci. Publ. Math.* (1965), no. 27, p. 55-150.

[9] ———, "Éléments unipotents et sous-groupes paraboliques de groupes réductifs. I", *Invent. Math.* **12** (1971), p. 95-104.

[10] P. Bougerol & J. Lacroix, *Products of random matrices with applications to Schrödinger operators*, Progress in Probability and Statistics, vol. 8, Birkhäuser Boston Inc., Boston, MA, 1985, xii+283 pages.

[11] J. Bourgain & A. Gamburd, "Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$", *Ann. of Math. (2)* **167** (2008), no. 2, p. 625-642.

[12] ———, "Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$ II - with an appendix by J. Bourgain", *J. Eur. Math. Soc. (JEMS)* **5** (2009), p. 1057-1103.

[13] E. Breuillard, "A Strong Tits Alternative", 2008, preprint.

[14] E. Breuillard & A. Gamburd, "Strong uniform expansion in $\mathrm{SL}(2,p)$", 2010, to appear in GAFA.

[15] P. Eymard, *Moyennes invariantes et représentations unitaires*, Lecture Notes in Mathematics, Vol. 300, Springer-Verlag, Berlin, 1972, ii+113 pages.

[16] W. Fulton & J. Harris, *Representation theory*, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, New York, 1991, A first course, Readings in Mathematics.

[17] H. Furstenberg, "Noncommuting random products", *Trans. Amer. Math. Soc.* **108** (1963), p. 377-428.

[18] I. Y. Goldsheid & G. A. Margulis, "Lyapunov exponents of a product of random matrices", *Russian Math. Surveys* **44** (1989), no. 5, p. 11-71.

[19] Y. Guivarc'h, "Produits de matrices aléatoires et applications aux propriétés géométriques des sous-groupes du groupe linéaire", *Ergodic Theory Dynam. Systems* **10** (1990), no. 3, p. 483-512.

[20] Y. Guivarc'h & A. Raugi, "Frontière de Furstenberg, propriétés de contraction et théorèmes de convergence", *Z. Wahrsch. Verw. Gebiete* **69** (1985), no. 2, p. 187-242.

[21] S. Helgason, *Differential geometry, Lie groups, and symmetric spaces*, Graduate Studies in Mathematics, vol. 34, American Mathematical Society, Providence, RI, 2001, Corrected reprint of the 1978 original, xxvi+641 pages.

[22] J. Humphreys, *Linear algebraic groups*, Springer-Verlag, New York, 1975, Graduate Texts in Mathematics, No. 21, xiv+247 pages.

[23] H. Kesten, "Symmetric random walks on groups", *Trans. Amer. Math. Soc.* **92** (1959), p. 336-354.

[24] J. F. C. Kingman, "Subadditive ergodic theory", *Ann. Probability* **1** (1973), p. 883-909.

[25] E. Kowalski, *The large sieve and its applications*, Cambridge Tracts in Mathematics, vol. 175, Cambridge University Press, Cambridge, 2008, Arithmetic geometry, random walks and discrete groups, xxii+293 pages.

[26] E. Le Page, "Théorèmes limites pour les produits de matrices aléatoires", in *Probability measures on groups (Oberwolfach, 1981)*, Lecture Notes in Math., vol. 928, Springer, Berlin, 1982, p. 258-303.

[27] G. D. Mostow, *Strong rigidity of locally symmetric spaces*, Princeton University Press, Princeton, N.J., 1973, Annals of Mathematics Studies, No. 78, v+195 pages.

[28] I. Rivin, "Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms", *Duke Math. J.* **142** (2008), no. 2, p. 353-379.

[29] ———, "Zariski density and genericity", *Int. Math. Res. Not. IMRN* (2010), no. 19, p. 3649-3657.

[30] J. Tits, "Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque", *J. Reine Angew. Math.* **247** (1971), p. 196-220.

[31] ———, "Free subgroups in linear groups", *J. Algebra* **20** (1972), p. 250-270.

[32] P. Varjú, "Expansion in $\mathrm{SL}_d(\mathrm{O_K}/\mathrm{I})$, I square-free", arXiv:1001.3664.

[33] È. B. Vinberg & V. G. Kac, "Quasi-homogeneous cones", *Mat. Zametki* **1** (1967), p. 347-354.

Manuscrit reçu le 25 mars 2011,
révisé le 9 février 2012,
accepté le 20 septembre 2012.

Richard AOUN
Université Paris Sud 11
Laboratoire de Mathématiques
Bâtiment 425
91405 Orsay (France)

Département de Mathématiques
Faculté des Sciences de l'Université Saint-Joseph
Campus des Sciences et Technologies
B.P. 11-514 Riad El Solh
Beyrouth 1107 205 (Liban)
richard.aoun@math.u-psud.fr