Abstract: We show that on an arbitrary finitely generated non virtually solvable linear group, any two independent random walks will eventually generate a free subgroup. In fact, this will hold for an exponential number of independent random walks.

Contents

1 Introduction ................................................. 1
  1.1 Outline of the paper .................................. 3

2 Preliminary reductions ..................................... 4
  2.1 Notation and terminology ............................ 5
  2.2 Outline of the proof of Theorem 1.1 ............... 6

3 Generating free subgroups in linear groups .......... 8
  3.1 The ping-pong method ............................... 8
  3.2 The Cartan decomposition ........................... 9

4 Random matrix products in local fields .............. 9
  4.1 Introduction ......................................... 10
  4.2 Convergence in direction ............................ 10
  4.3 Preliminaries on algebraic groups .................. 19
  4.4 Estimates in the Cartan decomposition - the connected case ............ 21
  4.5 Estimates in the Cartan decomposition - the non-connected case .......... 29

5 Proof of Theorem 2.11 ..................................... 33

1 Introduction

The Tits alternative [Tit72] says that every finitely generated linear group which is not virtually solvable contains a free group on two generators. A question that arises immediately is to see if this property is “generic” in the sense that two “random” elements (in a suitable sense) on such groups generate or not a free subgroup. In recent works of Rivin - [Riv08] - and Kowalski - [Kow08]- where groups coming from an arithmetic setting are considered, similar situations occur: a random element is shown to verify a property \( P \) with high probability, for example, a random matrix in one of the classical groups \( GL(n,\Z) \), \( SL(n,\Z) \) or \( Sp(n,\Z) \) has irreducible characteristic polynomial. In our case we take two elements at random and the property \( P \) will be “generate a free subgroup”. The method of the authors cited above relies deeply on arithmetic sieving techniques. In this paper, we consider an arbitrary finitely generated linear group, that is a subgroup of \( GL_n(K) \) for some field \( K \), and we use an entirely different set of techniques, namely random matrix products theory.

Let us explain what we mean by choosing two elements “at random”: a random element will be the realization of the random walk associated to some probability measure on the group. Formally

---

*Laboratoire de Mathématiques, Bâtiment 425, Université Paris Sud 11, 91405 Orsay- FRANCE, E-mail: richard.aoun@math.u-psud.fr
The main purpose of this paper is to show the following statement, which answers a question of Guivarch [Gui90] - 2.10-:

**Theorem 1.1.** Let $K$ be a field, $V$ a finite dimensional vector space over $K$, $\Gamma$ a finitely generated non virtually solvable subgroup of $GL(V)$ equipped with two probability measures $\mu$ and $\mu'$ having an exponential moment and such that $\Gamma_\mu = \Gamma_{\mu'} = \Gamma$. Let $(M_n)_{n \in \mathbb{N}^*}$, $(M'_n)_{n \in \mathbb{N}^*}$, be the independent random walks associated respectively to $\mu$ and $\mu'$. Then almost surely, for $n$ large enough, the subgroup $\langle M_n, M'_n \rangle$ generated by $M_n$ and $M'_n$ is free (non abelian). More precisely,

$$\limsup_{n \to \infty} \frac{1}{n} \log P(\langle M_n, M'_n \rangle \text{ is not free}) < 0$$

(1)

These conditions are fulfilled when the support of $\mu$ (resp. $\mu'$) is a finite symmetric generating set, say $S$ (resp. $S'$) of $\Gamma$. In this case, $M_n$ (resp. $M'_n$) is a random walk on the Cayley graph associated to $S$ (resp. $S'$). In other terms, if we consider the word metric, the theorem says that the probability that two “random” elements in the ball of radius $n$ do not generate a free subgroup is decreasing exponentially fast to zero; “random” here is to be understood with respect to $n^{th}$ convolution power of $\mu$ (resp. $\mu'$). In this statement we could have taken $S_n$ instead of $M_n$.

Let $\mu$ be a probability measure on $\Gamma$. For every integer $l$, we denote by $(M_{n,l})_{n \in \mathbb{N}^*}$, a family of $l$ independent random walks associated to $\mu$. From the proof of Theorem 1.1, we will deduce the following stronger statement:

**Corollary 1.2.** There exists $C > 0$ such that a.s., for all large $n$, $M_{n,1}, \ldots, M_{n,\lfloor \exp(Cn) \rfloor}$ generate a free group on $l_n = \lfloor \exp(Cn) \rfloor$ generators.

**remark 1.3.** As explained above, our main result shares a common flavor with the works by Rivin and Kowalski - [Riv08] and [Kow08] -, in the sense that random elements in a finitely generated group are shown to verify a generic property with high probability. Use of the theory of random matrix products allows us to treat arbitrary finitely generated linear groups while the arithmetic sieving techniques in [Riv08] and [Kow08] use reduction modulo prime numbers and deal with subgroups of arithmetic groups $\Gamma(G(\mathbb{Z}))$, where $G$ is an algebraic group. However what we loose is the effectiveness: in [Riv09], Rivin proved that the bounds he obtains in [Riv08] are effective while ours are not. Indeed, our method uses the Guivarch-Raugi theorem on the separation of the first two Lyapunov exponents $\lambda_1$ and $\lambda_2$ and the known bounds on $\lambda_1 - \lambda_2$ rely on the ergodic theorem and are thus non effective.

**remark 1.4.** In Guivarch’s proof of the Tits alternative in [Gui90] he showed that $S_{n_k}$ and $S'_{n'_k}$ can be turned into ping-pong players (see Section 3 for a definition of these terms) in a suitable linear representation for some subsequence $n_k$, $n'_k$ which were obtained as certain return times thanks to Poincaré recurrence. There is a substantial difficulty in passing from some subsequence to the version we give in our main theorem. This situation is not dissimilar to the difficulty encountered in [BG03] where ping-pong players were gotten from a precise control of the KAK decomposition, in contrast with Tits’ original argument which exhibited ping-pong players as high powers of proximal elements.

In the proof, we will use the theory of random matrix products over an arbitrary local field (i.e. $\mathbb{R}$, $\mathbb{C}$, a $p$-adic field, or a field of Laurent series over a finite field). Very little literature exists on this topic apart from the case of real or complex matrices ([Gui89]). So, in this paper, we will develop most of the theory from scratch in the context of local fields. Some of our statements will be just an adaptation of results known over the reals to arbitrary local fields while some are new even over $\mathbb{R}$. This is the case for Theorem 4.33 which shows the exponential convergence speaking, if $\mu$ is a probability measure on a group $\Gamma$, we denote by $\Gamma_\mu$ the smallest semigroup containing the support of $\mu$; we consider a sequence $\{X_n; n \geq 0\}$ of independent random variables on $\Gamma$ with the same law $\mu$, defined on a probability space $(\Omega, \mathcal{F}, \mathbb{P})$. The $n^{th}$ step of the random walk $M_n$ is defined by $M_n = X_1 \ldots X_n$. We will also consider the reversed random walk: $S_n = X_n^{-1} \ldots X_1$. The main purpose of this paper is to show the following statement, which answers a question of Guivarch [Gui90] - 2.10-:
of the K-components of the KAK decomposition, and for Theorems 4.35 and 4.38, which prove the asymptotic independence of the directional components of the KAK decomposition. Similar statements for the Iwasawa decomposition can be found in [Gu89]. We refer the reader to Section 4 for the statements of these results. Let us only state here one of them regarding the asymptotic independence in the KAK decomposition.

**Theorem 1.5** (Asymptotic independence in KAK with exponential rate). Let \( k \) be a local field, \( G \) a \( k \)-algebraic group assumed to be semi-simple and \( k \)-split, \((\rho, V)\) an irreducible \( k \)-rational representation of \( G \). Consider a probability measure \( \mu \) on \( G = G(k) \) with an exponential moment (see Definition 4.24) such that \( \Gamma_\mu \) is Zariski dense in \( G \) and \( \rho(\Gamma_\mu) \) is contracting. Let \( \{X_n; n \geq 1\} \) be independent random variables with the same law \( \mu \), \( S_n = X_n \ldots X_1 \) the associated random walk. Denote by \( S_n = K_nA_nU_n \) a KAK decomposition of \( S_n \) in \( G \) (see Section 4.3). Denote by \( e_1 \in V \) (resp. \( e_1^* \in V^* \)) a highest weight vector for the action of \( A \) on \( V \) via \( \rho \) (resp. \( \rho^* \) the contragredient representation). Then the random variables \( K_n[e_1] \) and \( U_n^{-1}[e_1^*] \) are asymptotically independent in the following sense. There exist independent random variables \( Z \) and \( T \) on \( P(V) \) (resp. \( P(V^*) \)) with law the unique \( \mu \)-invariant (resp. \( \mu^{-1} \)-invariant) probability measure on \( P(V) \) (resp. \( P(V^*) \)) such that the following holds. For every \( \epsilon > 0 \), there is some \( \rho = \rho(\epsilon) \in [0,1] \) such that for every \( \epsilon \)-Holder function \( \phi \) on \( P(V) \times P(V^*) \) and all large enough \( n \), we have:

\[
|\mathbb{E}(\phi(K_n[e_1], U_n^{-1}[e_1])) - \mathbb{E}(\phi(Z, T))| \leq \rho^n ||\phi||_\epsilon
\]

Here we have used the following notation: \( V^* \) is the dual space of \( V \), \( P(V) \) (resp. \( P(V^*) \)) is the projective space of \( V \) (resp. \( V^* \)) and \( G \) acts on \( V^* \) by the formula: \( g.f(x) = f(g^{-1}x) \) for every \( g \in G \), \( f \in V^* \), \( x \in V \). We have denoted by \( \mu^{-1} \) the law of \( X_1^{-1} \) and by \( ||\phi||_\epsilon \) the Holder constant of \( \phi \):

\[
||\phi||_\epsilon = \sup_{[x],[y],[x'][y']} |\phi([x],[x']) - \phi([y],[y'])|/\delta^\epsilon([x],[y]) + \delta^\epsilon([x'],[y'])
\]

where \( \delta \) is the standard angle metric (i.e. Fubini-Study metric) on \( P(V) \) and \( P(V^*) \). A similar statement for the KAK decomposition of \( \rho(S_n) \) in \( SL(V) \) (see section 3.2) holds: in this case, \( G \) need not be assumed Zariski connected any longer (see Theorem 4.38). Although we have not checked, it is likely that the above result holds without assuming that the Zariski closure of \( \Gamma_\mu \) is semi-simple and \( k \)-split, but assuming instead proximality and strong irreducibility.

### 1.1 Outline of the paper

In Section 2, we split the proof of our main theorem, i.e. Theorem 1.1, into two parts: an arithmetic part (Theorem 2.13) and a probabilistic part (Theorem 2.11). In our work, the probabilistic part replaces the dynamical part of the original proof of the Tits alternative. The arithmetic one is a variant of a classical lemma of Tits [Tit72, Lemma 4.1] proved by Margulis and Soifer [MS81]. The probabilistic one will be shown in Section 5 using the results of Section 4.

In Section 3, we recall a classical method, known as ping-pong, to show that a pair of linear automorphisms generate a free group.

Section 4 is the core of the paper and constitutes a self-contained treatment of the basics of random matrix theory over local fields. It can be read independently of the rest of the paper. To our knowledge, apart from [Gu89], this is the first time that this subject is treated over non-archimedean fields. Over \( \mathbb{R} \) or \( \mathbb{C} \), this theory is well developed, starting with Furstenberg and Kesten in the 60's and later the French school in the 70's and 80's: Bougerol, Le Page, Raugi and in particular Guivarc'h, whose work especially in [Gu90] and [GR85] inspired us a lot.

One of our main goals in this section is to give limit theorems for the random walk \( M_n \) in three aspects: its norm, its action on projective space and its components in the Cartan decomposition. Our main results in this section are the following:
• Theorem 4.16 shows the exponential convergence in direction of the random walk $M_n$. Namely, under the usual assumptions, for every point $[x]$ on the projective space, $M_n[x]$ converges exponentially fast to a random variable $Z$ on the projective space.

• Theorem 4.18 and more precisely its proof shows the exponential decay of the probability that $M_n[x]$ lies in a given hyperplane, uniformly over the hyperplane. We deduce that the unique $\mu$-invariant measure has some regularity.

• Theorem 4.33 shows that the $K$-components of the random walk $M_n$ in the Cartan decomposition converge exponentially fast.

• Theorem 4.35 proves that the $K$-components of the random walk $M_n$ in the Cartan decomposition become independent asymptotically.

Theorem 4.18 is a weaker version of a well-known statement over $\mathbb{R}$ or $\mathbb{C}$. Its proof can be found in Bougerol’s book and is due to Guivarc’h [Gui90, Theorem 7’]. We will verify that it holds over an arbitrary local field. Theorems 4.16, 4.33 and 4.35 on the other hand are new even over $\mathbb{R}$ (on $\mathbb{R}$ or $\mathbb{C}$ only the exponential rate is new). They also hold over an arbitrary local field, and so does everything we do in Section 4.2. The analog of Theorem 4.35 for the orthogonal and unipotent parts of the Iwasawa decomposition was proven over $\mathbb{R}$ by Guivarch in [Gui90, Lemma 8].

Our proof of Theorems 4.18 is not an mere translation of the standard proof of this statement over the reals. Rather we take a different and more direct route via our key cocycle lemma, Lemma 4.12, a result giving control on the growth of cocycles in an abstract context. This lemma is itself an extension of a result of Le Page (see the proof of [LP82, Theorem 1]) which was key in his proof of the spectral gap on Holder functions on projective space ([LP82, Proposition 4]).

Another key ingredient and intermediate step is our Proposition 4.14, which says that, under the usual assumptions, for every non zero vector $x$, with high probability the ratio $||M_n x||/||M_n||$ is not too small. This fact can be interpreted as a weak form of Le Page’s large deviation theorem in $GL_n(\mathbb{R})$.

Our proof of Theorem 4.33 is based on this approach as well and makes key use of the cocycle lemma, Lemma 4.12 and of Proposition 4.14. Theorem 4.16 is also an important ingredient in the proof of 4.33. Finally the proof of Theorem 4.35 combines all of the above.

We note that two Cartan decompositions will be considered in Section 4, the one coming from the ambient $SL_d(k)$ and the one attached to the (semi-simple) algebraic group in which the group generated by the random walk is Zariski dense. Our limit theorems will be proved in the two cases. In fact the results for the Cartan decomposition in $SL_d(k)$, which are our main interest, will be deduced from the analogous results in the algebraic group. These statements will be deduced from a delicate study of the Iwasawa decomposition in the algebraic group (Theorem 4.28). If this Zariski closure is not Zariski connected, further technicalities arise. They will be dealt with in Section 4.5 using standard Markov chains and stopping times techniques.

Finally, we note that our proofs rely deeply on the pointwise ergodic theorem via our cocycle lemma, Lemma 4.12.

Section 5 is devoted to the proof of Theorem 2.11, i.e. the probabilistic part of our main result, using the results of Section 4.

Acknowledgments I sincerely thank my supervisor Emmanuel Breuillard for pointing me out this question, for his great availability, his guidance through my Ph.D. thesis and many remarks on an anterior version of this paper. I’m also grateful to Yves Guivarc’h whose work inspires me a lot.

2 Preliminary reductions

In this section we reduce the proof of Theorem 1.1 to its probabilistic part, i.e. Theorem 2.11 below.
2.1 Notation and terminology

All random variables will be defined on a probability space \((\Omega, \mathcal{F}, \mathbb{P})\). \(\mathbb{E}\) refers to the expectation with respect to \(\mathbb{P}\). The symbol “a.s.” refers to almost surely. Let us recall the definition of a random walk on a group:

**Definition 2.1** (Random walks on groups). Let \(\Gamma\) be a discrete group, \(\mu\) a probability measure on \(\Gamma\), \((X_i)_{i \in \mathbb{N}^*}\) a family of independent random variables on \(\Gamma\) with the same law \(\mu\). For each \(n\), we define the \(n\)th step of the following random walks by:

\[
M_n = X_1 \cdots X_n ; \quad S_n = X_n \cdots X_1
\]

The product being the group law of \(\Gamma\). We denote by \(\Gamma_\mu\) the smallest semigroup containing the support of \(\mu\).

**Remark 2.2.** For our main Theorem 1.1, there will be no difference taking the natural \((M_n)\) or the reversed random walk \((S_n)\) as explained in the Remark 2.6 below. Note however that the asymptotic behavior of the two walks is not the same in general.

When \(\Gamma\) is a finitely generated group, \(\Gamma\) is a metric space for the word length distance: for each symmetric generating set \(S\) containing 1, define:

\[
l_S(g) = \text{Min}\{r; g = s_1 \cdots s_r; \quad s_i \in S \forall i = 1, \ldots, r}\.
\]

The following defines then a distance on \(\Gamma\):

\[
d_S(g, g') = l_S(g^{-1}g) \quad g, g' \in \Gamma.
\]

**Definition 2.3** (Exponential moment on finitely generated groups). Let \(\mu\) be a probability measure on a finitely generated group \(\Gamma\). Let \(S\) be as above. We say that \(\mu\) has an exponential moment if there exists \(\tau > 0\) such that:

\[
\int \exp(\tau l_S(g)) \, d\mu(g) < \infty
\]

It is immediate that having exponential moment is independent of the choice of the generating set defining \(l_S\).

Let us recall our main result in this paper:

**Theorem** Let \(K\) be a field, \(V\) a finite dimensional vector space over \(K\), \(\Gamma\) a finitely generated non virtually solvable subgroup of \(\text{GL}(V)\) equipped with two probability measures \(\mu\) and \(\mu'\) having an exponential moment and such that \(\Gamma_\mu = \Gamma_\mu' = \Gamma\). Let \((M_n)_{n \in \mathbb{N}^*}\), \((M'_n)_{n \in \mathbb{N}^*}\) be two independent random walk associated respectively to \(\mu\) and \(\mu'\). Then almost surely, for \(n\) large enough, the group \(\langle M_n, M'_n \rangle\) generated by \(M_n\) and \(M'_n\) is free (non abelian). More precisely,

\[
\limsup_{n \to \infty} \frac{1}{n} \log \mathbb{P}(\langle M_n, M'_n \rangle \text{ is not free}) < 0 \quad (2)
\]

**Remark 2.4.** The assumptions on \(\mu\) (resp. \(\mu'\)) of the theorem are clearly fulfilled if the support of \(\mu\) (resp. \(\mu'\)) is a finite, symmetric generating set of \(\Gamma\).

**Remark 2.5.** The bound (2) implies that there exists \(\rho \in ]0, 1[\) such that for \(n\) large enough,

\[
\mathbb{P}(\langle M_n, M'_n \rangle \text{ is not free}) \leq \rho^n \quad (3)
\]

By the Borel-Cantelli lemma, it suffices to prove the first assertion of the theorem. Hence in the rest of the paper, we will focus on showing (3).

**Remark 2.6.** There is no difference taking \((M_n)_{n \in \mathbb{N}^*}\) or the reversed random walk in Theorem 1.1. In fact, the increments are independent and have the same law which implies that \((X_1, \ldots, X_n)\) has the same law as \((X_n, \ldots, X_1)\) for every integer \(n\), hence (2) is unchanged if we replaced \(M_n\) by \(S_n\).
2.2 Outline of the proof of Theorem 1.1

A local field (i.e. a commutative locally compact field) is isomorphic either to \( \mathbb{R} \) or \( \mathbb{C} \) (archimedian case) or a finite extension of the \( p \)-adic field \( \mathbb{Q}_p \) for some prime \( p \) in characteristic zero or to the field of formal Laurent series \( L((T)) \) over a finite field \( L \). When \( k \) is archimedian, we denote by \(|.|\) the Euclidean absolute value. When \( k \) is not archimedian, we denote by \( \Omega_k \) its discrete valuation ring, \( \pi \) a generator of its unique maximal ideal, \( q \) the degree of its residual field, \( v(.) \) a discrete valuation and consider the following ultrametric norm: \( |.| = q^{-v(.)}. \)

When we consider a finitely generated linear group \( \Gamma \), i.e. \( \Gamma \subset GL_d(K) \) for some \( d \geq 2 \) and a finitely generated field \( K \), we can benefit from other nice metrics than the word metric: for each local field \( k \) containing \( K \), \( \Gamma \) can be considered as a metric space with the topology of \( End_d(k) \) induced on \( \Gamma \). This justifies the two parts of our proof: the arithmetic part (Theorem 2.13) which consists in finding a suitable local field containing \( K \) and the probabilistic one (Theorem 2.11) consisting in using limit theorems for random walks on linear groups over local field. Theorem 2.13 will be borrowed from [MS81] and Theorem 2.11 is the main part of this paper. Before stating them and showing how they provide a proof of Theorem 1.1, we give some basic definitions:

**Definition 2.7. (Strong irreducibility and contraction properties)**

- **Strong irreducibility**: let \( k \) be a field, \( V \) a vector space over \( k \) and \( \Gamma \) a subgroup of \( GL(V) \). The action of \( \Gamma \) on \( V \) is said to be strongly irreducible if \( \Gamma \) does not fix a finite union of proper subspaces of \( V \). This is equivalent to saying that \( \Gamma \) contains no subgroup of finite index that acts reducibly on \( V \). In particular, if the Zariski closure \( \overline{\Gamma} \) is connected then irreducibility and strong irreducibility are equivalent (because the identity component of \( \overline{\Gamma} \) is contained in any algebraic subgroup of finite index - [Hum75]-). We note that this notion is “algebraic” in the sense that \( \Gamma \) is strongly irreducible if and only if \( \overline{\Gamma} \) is.

- **Contraction for local fields**: let \( (k,|.|) \) be a local field, \( V \) a vector space over \( k \) and \( \Gamma \subset GL(V) \). We choose any norm \( |.| \) on \( End(V) \). We say that a sequence \( \gamma_n \) \( n \in \mathbb{N} \) \( \subset \Gamma \) is contracting, if \( r_n \gamma_n \) converges, via a subsequence, to a rank one endomorphism for every (or equivalently one) suitable normalization \( (r_n) \) in \( k \) such that \( |r_n \gamma_n| = 1 \). It is equivalent to say that the projective transformation \( \gamma_n \) \( PGL(V) \) contracts \( P(V) \) into a point, outside a hyperplane. Note that in the archimedean case, this is just saying that \( \frac{\gamma_n}{||\gamma_n||} \) converges to a rank one endomorphism.

A representation \( \rho \) of \( \Gamma \) is said to be contracting if the group \( \rho(\Gamma) \) contains a contracting sequence.

The following classical lemma gives a more practical method to verify contraction. It will be useful to us in Section 4.5.

**Lemma 2.8 (Contraction and proximality).** An element \( \gamma \in GL(V) \) is said to be proximal if and only if it has a unique eigenvalue of maximal modulus. If \( \Gamma \) contains a proximal element then it is contracting. If \( \Gamma \) acts irreducibly on \( V \) and is contracting then it contains a proximal element.

**Proof.** If \( \gamma \in \Gamma \) is proximal, then its maximal eigenvalue \( \lambda \) belongs to the field \( k \) and the corresponding eigendirection is defined on \( k \). The latter has a \( \gamma \)-invariant supplementary hyperplane defined on \( k \). Consequently, in a suitable basis, \( \gamma \) is of the form: \( \begin{pmatrix} \lambda & 0 \\ 0 & M \end{pmatrix} \). By the spectral radius formula, we deduce that sequence \( \{\gamma^n; n \in \mathbb{N}\} \) is contracting. Conversely, consider sequences \( \{\gamma_n; n \in \mathbb{N}\} \) in \( \Gamma \), \( \{r_n; n \in \mathbb{N}\} \) in \( k \) such that \( r_n \gamma_n \) converges to a rank one endomorphism \( h \). \( h \) is proximal if and only if \( Im(h) \not\subset Ker(h) \). Suppose first that \( h \) is proximal and notice that \( \{g \in End(V); g \text{ is proximal}\} \) is open (for the topology on \( End(V) \) induced by that of the local field \( k \)); hence for sufficient large \( n \), \( r_n \gamma_n \) is proximal, a fortiori \( \gamma_n \) and we are done. If \( h \) fails to be proximal, or equivalently \( Im(h) \subset Ker(h) \), we claim that one can still find \( g \in \Gamma \) such that \( gh \) is proximal; this would end the proof since by the same reasoning \( \gamma_n h \) would be proximal for large \( n \). Let us prove the claim: denote by \( kx_0 \) the image of \( h \) and notice that \( V = Vect\{gx_0; g \in \Gamma\} \) because the action of \( \Gamma \) on \( V \) is irreducible. Consequently, there exists \( g \in \Gamma \) such that \( gx_0 \not\subset Ker(h) \). But \( gx_0 = Im(gh) \) and \( Ker(h) = Ker(gh) \); whence \( gh \) is proximal.
Definition 2.9 (Exponential local moment on linear groups). Let $k$ be a local field, $d$ an integer $\geq 2$, $\Gamma$ be a subgroup of $SL_d(k)$, $\| \cdot \|$ a norm on $End_k(k)$, $\mu$ a probability measure on $\Gamma$. We say that $\mu$ has an exponential local moment if for some $\tau > 0$,

$$\int \| g \|^\tau d\mu(g) < \infty$$

Remark 2.10 (Interpretation). The definition above can be reformulated as follows: there exists $\tau > 0$ such that $\int \exp(\tau \log \| g \|) d\mu(g) < \infty$ or equivalently $\int \exp(d_X(g, I_d)) d\mu(g) < \infty$ where $X = SL_d(k)/K$ is the symmetric space associated to $SL_d(k)$ (see Section 4.2 for definition of $K$), $d_X(g_1, g_2) = \log \| g_2^{-1} g_1 \|$ is a distance on $X$, $I_d$ is the identity matrix of order $d$.

Now we are able to state the two results. In the following theorem, for a measure $\mu$ on $SL_d(k)$, $\Gamma_{\mu}$ denotes the smallest closed semigroup containing the support of $\mu$.

Theorem 2.11 (Probabilistic part). Let $k$ be a local field, $d \geq 2$, $\mu$, $\mu'$ two probability measures on $SL_d(k)$ having an exponential local moment and such that $\Gamma_{\mu} = \Gamma_{\mu'}$ is a strongly irreducible and contracting subgroup. We assume its Zariski closure to be $k$-split and its connected component semi-simple. We denote by $(M_n)_{n \in \mathbb{N}}$, $(M'_n)_{n \in \mathbb{N}}$ the random walks associated to $\mu$ (resp. $\mu'$). Then a.s. for all $n$ large enough, the group $(M_n, M'_n)$ generated by $M_n$ and $M'_n$ is free. More precisely,

$$\limsup_{n \to \infty} \frac{1}{n} \log \mathbb{P}(\langle M_n, M_n' \rangle \text{ is not free}) < 0 \quad (4)$$

Remark 2.12. The assumptions $\Gamma_{\mu}$ semi-simple and k-split can be dropped: $\Gamma_{\mu}$ being strongly irreducible, the Zariski connected component of $\Gamma_{\mu}$ is immediately reductive and everything we will do in Section 4.4 for semi-simple groups is applicable to reductive groups. The assumption k-split will be used to simplify the Cartan and Iwasawa decompositions in Sections 4.4 and 4.3, however similar decompositions hold in the general case. To keep the exposition as simple as possible we kept these conditions.

If $V$ is a vector space over a field $k$ and $\Gamma$ a group, we say that a representation $\rho : \Gamma \to GL(V)$ is absolutely (strongly) irreducible if it remains (strongly) irreducible on $V \otimes_k k'$ for every algebraic extension $k'$ of $k$.

Theorem 2.13 (Arithmetic part). [MS81, Theorem 2] Let $K$ be a finitely generated field, $G$ an algebraic group over $K$ such that the Zariski connected component $G^0$ is not solvable, $\Gamma$ be a $K$-Zariski dense subgroup. Then there exists a local field $k$ containing $K$, a vector space $V$ over $k$ and a $k$-algebraically absolutely strongly irreducible representation $\rho : G \to SL(V)$ such that $\rho(\Gamma)$ is contracting and the Zariski component of $\rho(G)$ is a semi-simple group.

Remark 2.14. A classical lemma of Tits [Tits72] says (or at least implies) the same as Theorem 2.13 except that $\rho$ is a representation of a finite index subgroup of $G$. This is insufficient for us because the random walk lives in all of $\Gamma$. However, when $G$ is Zariski connected the above theorem and the aforementioned lemma of Tits are exactly the same. We note that the proof of Theorem 2.13 by Margulis and Soifer depends heavily on the classification of semi-simple algebraic groups through their Dynkin diagram. A more conceptual proof can be found in [BG07] except that the representation $\rho$ takes value in $PGL(V)$, and this is not enough for our purposes.

End of the proof of Theorem 1.1 modulo Theorem 2.11. Let $\Gamma = \Gamma_{\mu} = \Gamma_{\mu'}$. Since $\Gamma$ is finitely generated, we can replace $K$ with the field generated over its prime field by the matrix coefficients of the (finitely many) generators of $\Gamma$. Let $G$ be the Zariski closure of $\Gamma$. Then, we can apply Theorem 2.13. It gives a local field $k$, a $k$-rational absolutely strongly irreducible representation $(\rho, V)$ of $G$ such that the Zariski-connected component of $H = \rho(G)$ is semi-simple and $\rho(\Gamma)$ is contracting. Passing to a finite extension of $k$ if necessary, $H$ can be assumed $k$-split; $\rho$ remains absolutely strongly irreducible. We are now in the situation of Theorem 2.11: we have a probability measure $\rho(\mu)$ (image of $\mu$ under $\rho$) on some $SL_d(k)$ such that $\Gamma_{\rho(\mu)} = \rho(\Gamma)$ is strongly
irreducible and contracting. Moreover, the connected component of its Zariski closure \( H \) is semi-simple and \( k \)-split. To apply Theorem 2.11 we only have to check that \( \rho(\mu) \) has an exponential local moment knowing that \( \mu \) has an exponential moment. Indeed, if \( g = s_{1\mu}(g) \ldots s_{r\mu}(g) \in \text{Supp}(\mu) \) is a minimal expression of \( g \) in terms of the generators of a symmetric finite generating set \( S \) of \( \Gamma \), then \( \ell_S(g) = |n_1(g)| + \ldots + |n_r(g)| \) whence \( ||\rho(g)|| \leq \left[ \text{Max}\{\log||\rho(s)|| : s \in S\} \right]^{\ell_S(g)} \).

Consequently, if \( \mathbb{E}(\exp(\tau \ell_S(X_1))) \) is finite, then for some \( \tau' > 0 \), \( \mathbb{E}(||\rho(X_1)||^{\tau'}) \) is also finite. We can now apply Theorem 2.11: a.s., for \( n \) large enough, \( \langle \rho(M_n), \rho(M'_n) \rangle \) is free, a fortiori \( \langle M_n, M'_n \rangle \) is also free. This ends the proof.

\[ \square \]

3 Generating free subgroups in linear groups

In Theorem 2.11 we must show that \( M_n \) and \( M'_n \) generate a free group. Below we use the classical ping-pong method to obtain two generators of a free subgroup. For a detailed description of these ping-pong techniques one can refer to [BG03] for a self-contained exposition or to the original article of Tits [Tit72].

3.1 The ping-pong method

Let \( k \) be a local field, \( V \) a vector space over \( k \), \( P(V) \) its projective space, \( \delta \) the Fubini-Study distance on \( P(V) \) defined by:

\[ \delta([x], [y]) = \frac{||x \wedge y||}{||x|| ||y||} ; \quad [x], [y] \in P(V) \]

where \([x]\) is the projection of \( x \in V \setminus \{0\} \) on \( P(V) \).

- Let \( \epsilon \in ]0,1[ \). A projective transformation \([g] \in PSL(V)\) is called \( \epsilon \)-contracting if there exists a point \( v_g \in P(V) \), called an attracting point of \([g] \), and a projective hyperplane \( H_g \), called a repelling hyperplane of \([g] \), such that \([g]\) maps the complement of the \( \epsilon \)-neighborhood of \( H_g \subset P(V) \) into the \( \epsilon \)-ball around \( v_g \). We say that \([g]\) is \( \epsilon \)-very contracting if both \([g]\) and \([g^{-1}]\) are \( \epsilon \)-contracting.

- \([g]\) is called \( (r, \epsilon) \)-proaximal \((r > 2 \epsilon > 0)\) if it is \( \epsilon \)-contracting with respect to some attracting point \( v_g \in P(V) \) and some repelling hyperplane \( H_g \), such that \( \delta(v_g ; H_g) > r \). The transformation \([g] \) is called \( (r, \epsilon) \)-very proximal if both \([g]\) and \([g^{-1}]\) are \( (r, \epsilon) \)-proximal.

- A pair of projective transformations \( a, b \in PSL(V) \) is called a ping-pong pair if both \( a \) and \( b \) are \((r, \epsilon)\)-very proximal, with respect to some \( r > 2 \epsilon > 0 \), and if the attracting points of \( a \) and \( a^{-1} \) (resp. of \( b \) and \( b^{-1} \)) are at least \( r \)-apart from the repelling hyperplanes of \( b \) and \( b^{-1} \) (resp. of \( a \) and \( a^{-1} \)). More generally, a \( m \)-tuple of projective transformations \( a_1, \ldots, a_m \) is called a ping-pong \( m \)-tuple if all \( a_i \)'s are \((r, \epsilon)\)-very proximal (for some \( r > 2 \epsilon > 0 \)) and the attracting points of \( a_i \) and \( a_i^{-1} \) are at least \( r \)-apart from the repelling hyperplanes of \( a_j \) and \( a_j^{-1} \), for any \( i \neq j \).

The following useful lemma is an easy exercise:

**Lemma 3.1** (Ping-pong lemma). If \( a, b \in PSL(V) \) form a ping-pong pair then the subgroup \( \langle a, b \rangle \) generated by \( a \) and \( b \) is free. More generally if \( a_1, \ldots, a_m \) is a ping-pong \( m \)-tuple then \( \langle a_1, \ldots, a_m \rangle \) is free.
3.2 The Cartan decomposition

Let $d \geq 2$, $V = k^d$ and $(e_1, \ldots, e_d)$ its canonical basis. The attracting points and repelling hyperplanes are not unique. In this article, they will be defined via the Cartan decomposition in $SL(V)$. Let’s recall it.

When $k = \mathbb{R}$ or $\mathbb{C}$, consider the usual Euclidean (resp. Hermitian) norm on $k^d$ and the canonical basis $(e_1, \ldots, e_d)$. Let $K = SO_d(k)$ (resp. $SU_n(\mathbb{C})$) be the orthogonal (resp. unitary) group, $A = \{\text{diag}(a_1, \ldots, a_d); a_i > 0 \; \forall i = 1, \ldots, d; \prod_{i=1}^d a_i = 1\}, A^+ = \{\text{diag}(a_1, \ldots, a_d) \in A; a_1 \geq \ldots \geq a_d > 0\}$. In this setting, the Cartan decomposition holds: $SL_d(k) = KA^+K$. This is the classical polar decomposition.

When $k$ is non archimedean, denote $K = SL_d(\Omega_k)$ and $A = \{\text{diag}(\pi^{n_1}, \ldots, \pi^{n_d}); n_i \in \mathbb{Z} \; \forall i = 1, \ldots, d; \sum_{i=1}^d n_i = 0\}; A^+ = \{\text{diag}(\pi^{n_1}, \ldots, \pi^{n_d}) \in A; n_1 \leq \ldots \leq n_d\}$. If we consider the Max norm on $V$: $||x|| = \text{Max}\{|x_i|; i = 1, \ldots, d\}, \; x \in V$, then one can show that $K$ is the group of isometries of $V$. With these notations, the Cartan decomposition is: $SL_d(k) = KA^+K$. This decomposition can be seen as an application of the well-known Invariant Factor Theorem for Matrices (see for example [CR06]). One can also see it as a particular case of the Cartan decomposition for algebraic groups (see Section 4.3).

In both cases, given $g$ in $SL_d(k)$ its components in the KAK decomposition are not uniquely defined (only the component in $A$ is). Nevertheless, we can always fix once and for all a privileged way to construct KAK in $SL_d(k)$. Therefore, for $g \in SL_d(k)$, we denote by $g = k(g)u(g)u(g)$ “its” KAK decomposition with $a(g) = \text{diag}(a_1(g), \ldots, a_d(g))$.

Till the end of the paper, we write $v_g = k(g)[e_1]$ and $H_g = [\text{Span}(u(g)^{-1}e_2, \ldots, u(g)^{-1}e_d)]$. The following lemma taken from [BG03] shows that a large ratio between $a_1(g)$ and $a_2(g)$ implies contraction. Then $v_g$ can be taken as an attracting point and $H_g$ as a repelling hyperplane.

Lemma 3.2. [BG03] Let $\epsilon > 0$. If $\frac{|a_2(g)|}{|a_1(g)|} \leq \epsilon^2$, then $[g]$ is $\epsilon$-contracting. Moreover, one can take $v_g$ to be the attracting point and $H_g$ to be the repelling hyperplane.

Proof. $v_g = [k(g)e_1]$ and $H_g = [\text{Span}(u(g)^{-1}e_2, \ldots, u(g)^{-1}e_d)]$. Let $x \in V$ such that $d(x,H_g) > \epsilon$. We want to prove that $d(g[x],v_g) < \epsilon$. Notice that $H_g = \text{Ker}(u(g)^{-1}e_1)$. Hence $\frac{|u(g)^{-1}e_1(x)|}{||x||} > \epsilon$. But,

$$d(g[x],v_g) = \frac{|gx \wedge k(g)e_1|}{||gx||} = \frac{||a(g)u(g)x \wedge e_1||}{||a(g)u(g)x||}$$

Since $|a_1(g)| \geq \ldots \geq |a_d(g)|$, $||a(g)u(g)x \wedge e_1|| \leq |a_2(g)|||x||$. Moreover, $||a(g)u(g)x|| \geq |a_1(g)| \cdot |u(g)^{-1}e_1(x)|$. Hence,

$$d(g[x],v_g) < \frac{1}{|a_1(g)|} \frac{||a_2(g)||}{\delta(x,H_g)} \leq \epsilon$$

\[\square\]

4 Random matrix products in local fields

- In this section, $d$ is an integer $\geq 2$ and $k$ a local field. We set $V = k^d$.

- When $\mu$ is a probability on a group $G$, we consider both random walks $M_n = X_1 \ldots X_n$ and $S_n = X_1 \ldots X_n$ as defined in Section 2. $\Gamma_\mu$ is the smallest closed semigroup containing the support of $\mu$. 
4.1 Introduction

Our aim in this section is to establish the basics of the theory of random matrix products over local fields. The section is structured as follows.

In Section 4.2, we generalize the first principles and tools of random matrix theory to all local fields. In particular we establish the exponential convergence in direction (Theorem 4.16) and the exponential decay of the probability of hitting a hyperplane (Theorem 4.18). A key ingredient in the proofs is our cocycle lemma, Lemma 4.12, which is a rather general statement giving control on the size of a cocycle in an abstract context. Another important tool will be Proposition 4.14, which compares the size of the norm of the random walk with the size of the random walk applied to any fixed vector. It can be viewed as a weak form of Le Page’s large deviations theorem ([LP82, Theorem 7]) in the context of local fields. Making use of these two ingredients, we then compare the A-component of the random walk in the Iwasawa decomposition with the A-component in the Cartan decomposition (Proposition 4.27).

In Section 4.3, we review some basic facts about algebraic groups, absolutely irreducible linear representations of semi-simple algebraic groups over local fields and their classification through the highest weight theory.

In Section 4.4 and Section 4.5, we establish limit theorems for the components of the Cartan decomposition of the random walk. The main results are Theorem 4.31 (exponential contraction of the A-component), Theorem 4.33 (exponential convergence of the K-components) and Theorem 4.35 (asymptotic independence of the K-components). Our method consists in investigating the Iwasawa decomposition first by proving the exponential contraction of the A-component of the Iwasawa decomposition (Theorem 4.28). In fact, in order to study the Cartan decomposition in the ambient SLd(k), we will first look at the behavior of the Cartan decomposition of the random walk inside the semi-simple algebraic group which is the Zariski closure of the group generated by the random walk, and then compare the two decompositions (Corollary 4.32). The case when the Zariski closure is connected is easier and is handled in Section 4.4, while the general case is handled in Section 4.5.

4.2 Convergence in direction

4.2.1 Generalization of well-known results in an non archimedean setting

This section does not require any prior knowledge on algebraic groups.

Let B = (e1, ..., ed) be the canonical basis of V = k^d. By canonical norm, we mean either the standard Euclidean (or Hermitian) norm when k is archimedean or the Max norm, ||x|| = Max{|xi|; i = 1, ..., d} for every x ∈ V, when k is non archimedean.

Recall that by Section 3, there exist a compact subgroup K acting by isometries on V, a subgroup A^+ consisting of diagonal matrices such that: SLd(k) = KA^+K (Cartan decomposition). For g ∈ SLd(k), we denote by g = k(a)(g)u(g) a privileged decomposition of g in this product.

We denote by V^* the dual of V and (e_1^*, ..., e_d^*) the canonical basis of V^* dual to (e_1, ..., e_d). We consider the canonical norm induced on V^*. Recall that SLd(k) acts on V^* by g.f(x) = f(g^{-1}x) for every g ∈ SLd(k), f ∈ V^*, x ∈ V. The projective space of V is denoted by P(V) and the projection of a non zero vector x ∈ V by [x]. The norm on V (resp. V^*) induces a distance on P(V) sometimes called the Fubini-Study distance:

δ([x], [y]) = ||x ∧ y|| / ||x|| ||y|| ; [x], [y] ∈ P(V)

A similar formula holds for V^*. If H is a hyperplane of V, f ∈ V^* such that H = Ker(f), then

δ([x], H) = ||f(x)|| / ||f|| ||x|| ; x ∈ V \ {0}

Consider a probability measure μ on SLd(k). No assumptions will be made on the Zariski
closure of \( \Gamma_\mu \). Recall that \( M_n = X_1 \ldots X_n \) and \( S_n = X_n \ldots X_1 \). The KAK decomposition of \( S_n \) will be simply denoted by: \( S_n = K_n A_n U_n \).

**Definition 4.1.** If \( G \) is a group acting on a topological space \( X \), \( \mu \) (resp. \( \nu \)) a probability measure on \( G \) (resp. \( X \)), \( \nu \) is said to be \( \mu \)-invariant if \( \mu * \nu = \nu \), which means that for every Borel function \( f \) on \( X \),
\[
\int f(gx) \, d\mu(g) \, dv(x) = \int f(x) \, dv(x).
\]

**Definition 4.2** (Lyapunov exponents). Suppose that \( \int \log ||g|| \, d\mu(g) < \infty \) (i.e. existence of a moment of order one). The Lyapunov exponents relative to \( \mu \) are defined recursively by:
\[
\lambda_1 + \ldots + \lambda_i = \lim \frac{1}{n} \mathbb{E}(\log \big| \bigwedge^i S_n \big|) = \lim \frac{1}{n} \log \big| \bigwedge^i S_n \big|
\]

The limit on the left hand side is an easy application of the subadditive lemma. The one on the right hand side is an almost sure limit and its existence is guaranteed by the subadditive ergodic theorem of Kingman [Kin73].

**Definition 4.3** (Index of a semigroup). For any semigroup \( \Gamma \) of \( GL(V) \), we define its index as the least integer \( p \) such that there exist sequences \( \{ M_n; n \geq 0 \} \) in \( \Gamma \), \( \{ r_n; n \geq 0 \} \) in \( k \) such that \( ||r_n M_n|| = 1 \), for which \( r_n M_n \) converges to a rank \( p \) matrix. We say that \( \Gamma \) is contracting when the index is one. (Note that in the archimedean case, one can just look at the quantity \( ||M_n|| \).)

We begin by a fundamental lemma in this theory due to Furstenberg.

**Lemma 4.4.** [Fur63] Let \( G \) be a topological semigroup acting on a \( \mathbb{Z} \)-countable locally compact space \( X \). Consider a sequence \( \{ X_n, n \geq 1 \} \) of independent random elements of \( G \) with a common distribution \( \mu \) defined on \( (\Omega, \lambda, \mathbb{P}) \). We denote \( \lambda = \sum_{n=0}^{\infty} 2^{-n-1} \mu^n \). If \( \nu \) is a \( \mu \)-invariant probability measure on \( X \) such that for \( \mathbb{P} \otimes X \)-almost every \( (\omega, g) \), the sequences of probability measures \( X_1(\omega) \ldots X_n(\omega) \, g \nu \) converge weakly to \( \nu_\omega \) as \( n \) goes to infinity.

Using Lemma 4.4, Guivarc’h and Raugi proved in their fundamental work in [GR85] the following crucial two theorems in the archimedean setting. For a nice exposition of these results (over \( \mathbb{R} \) or \( \mathbb{C} \), one can see chapter III of the book of Philippe Bougerol and Jean Lacroix [BL85]). We claim that these theorems hold in an arbitrary local field. For the reader’s convenience, we will check this for the first theorem and assume it for the second one since the proof is just cutting and pasting their original proof (for example one can see pages 64-65 of [BL85]).

**Theorem 4.5.** Suppose that \( \Gamma_\mu \) is strongly irreducible. Then, for \( p = \text{index}(\Gamma_\mu) \), there exists a random subspace \( V(\omega) \) of \( V \) of dimension \( p \) such that: a.s. for every \( (r_n)_{n \in \mathbb{N}} \in \mathbb{K}^\mathbb{N} \) s.t. \( ||r_n M_n|| = 1 \), every limit point of \( r_n M_n \) is a rank \( p \) matrix with image \( V(\omega) \). Moreover for every \( f \in V^* \),
\[
\mathbb{P} \left( \left| f \right|_{V(\omega)} = 0 \right) = 0
\]
When \( \Gamma_\mu \) is contracting, \( p = 1 \) and there exists a unique \( \mu \)-invariant probability measure on the projective space \( P(k^d) \) and a.s., \( M_n(\omega) \nu \) converges weakly to \( \delta_Z(\omega) \) where \( Z \) is a random variable on \( P(k^d) \) with law \( \nu \).

**Theorem 4.6.** Suppose that \( \int \log ||g|| \, d\mu(g) < \infty \). Under the same assumptions as in the previous theorem, \( \lambda_1 > \lambda_2 \).

**Proof of Theorem 4.5:** A general lemma of Furstenberg (see for example [BL85], Proposition 2.3 page 49) says that every \( \mu \)-invariant probability measure on \( P(V) \) is proper, i.e. does not charge any projective hyperplane. Now, fix a \( \mu \)-invariant probability measure on \( P(V) \) and an event \( \omega \in \Omega \). Choose \( \{ r_n; n \geq 1 \} \) in \( k \) such that \( ||r_n M_n(\omega)|| = 1 \) and a limit point \( A(\omega) \) along a subsequence \( \{ n_k \}_{k \in \mathbb{N}} \) of \( \{ r_n M_n; n \geq 1 \} \). Hence for every \( x \in V \) such that \( x \not\in \text{Ker}(A(\omega)) \), \( M_n(\omega)[x] \) converges to \( A(\omega)[x] \). Since \( \nu \) is proper, we deduce that \( M_n(\omega)[g] \nu \) converges weakly
towards $A(\omega)g\nu$ for every $g \in SL_d(k)$. On the other hand, by Lemma 4.4, there exists a random probability measure $\nu_\omega$ on $P(V)$ (whose expectation is $\nu$) such that $M_n(\omega)g\nu$ converges weakly towards $\nu_\omega$ for $\lambda$-almost every $g \in SL_d(k)$, where $\lambda$ is a probability measure supported on $\Gamma_\mu \cup \{I_d\}$. By uniqueness of convergence in weak topology, $A(\omega)g\nu = \nu_\omega$ for $\lambda$-almost every $g \in SL_d(k)$. But \{\(g \in SL_d(k); A(\omega)g\nu = \nu_\omega\}\} is closed and the support of $\lambda$ is $\Gamma_\mu \cup \{I_d\}$, hence

$$A(\omega)g\nu = \nu_\omega \quad \forall g \in \Gamma_\mu \cup \{I_d\}$$ (5)

Let $V(\omega)$ be the linear span of \{\(x \in V; [x] \in \text{Supp}(\nu_\omega)\}\}. (5) applied to $g = I_d$ shows that the image of $A(\omega)$ is exactly $V(\omega)$. Therefore, the image of $A(\omega)$ is indeed independent from the subsequence taken. It is left to show that its dimension is exactly the index $p$ of $\Gamma_\mu$. By definition of the index, the rank of $A(\omega)$ is at least $p$. The index of $\Gamma_\mu$ being $p$, there exists \(\{h_n; n \geq 1\}\) in $\Gamma_\mu$, \(\{s_n; n \geq 1\}\) in $k$ such that $s_nh_n$ converges towards $A$ (Convergence in KAK). It is clear that we can replace $U_n^{-1}.e_1^*,...,U_n^{-1}.e_p^*$ with $U_n^te_1,...,U_n^te_p$ where $U_n^t$ is the transpose of the matrix $U_n$. However, we prefer to work with the action on the dual vector space because it will give us more freedom later on.

\begin{proof}

We claim that one can find $g \in \Gamma_\mu$ such that:

$$A(\omega)gh\nu = \nu_\omega$$

This would end the proof because the dimension of $V(\omega)$ would be less or equal to the range of $h$, which is $p$. It suffices to show that there exists $g \in \Gamma_\mu$ such that $\nu\{x \in V; A(\omega)ghx = 0\} = 0$, because in this case for $\nu$-almost every $[x] \in P(V)$, $A(\omega)gh_n[x]$ would converge to $A(\omega)gh[x]$ so that $\nu_\omega = A(\omega)gh_n\nu$ would converge to $A(\omega)\nu$. If on the contrary, for every $g \in \Gamma_\mu$, $\nu\{x \in V; A(\omega)ghx = 0\} > 0$, then by the aforementioned property of $\nu$,

$$A(\omega)ghx = 0 \quad \forall x \in V$$

Hence $\{gx; g \in \Gamma_\mu; x \in \text{Im}(h)\}$ would be contained in the kernel of $A(\omega)$. Since it is $\Gamma_\mu$-invariant, this contradicts the irreducibility assumption on $\Gamma_\mu$. We have then proved that $V(\omega)$ is a $p$-dimensional subspace of $V$ and is the image of every limit point of $rr_nM_n$, where $||r_nM_n|| = 1$. By Lemma 4.4, $\nu = \int \nu_\omega \ d\mathbb{P}(\omega)$. Therefore,

$$\mathbb{P}(f|_{V(\omega)} \equiv 0) = \mathbb{P}(f(y) = 0 \ \forall y \in \text{Supp}(\nu_\omega)) \leq \mathbb{E} \left( \int 1_{f(y) = 0} \ d\nu_\omega(y) \right) = \nu(\text{Ker}(f))$$

Since $\nu$ is proper, this is equal to zero.

Finally, if $\Gamma_\mu$ is contracting, then $p = 1$ by definition and $|V(\omega)|$ is reduced to a point $Z(\omega) \in P(V)$. Since, by Lemma 4.4, $\nu = \int \delta_{Z(\omega)} \ d\mathbb{P}(\omega)$, we deduce that the distribution of $Z$ is $\nu$ and hence $\nu$ is unique.

\end{proof}

**Corollary 4.7 (Convergence in KAK).** Suppose that $\Gamma_\mu$ acts strongly irreducibly on $V$. Then the subspace $(k(M_n)e_1,...,k(M_n)e_p)$ converges a.s. to a random subspace $V(\omega)$ of dimension $p = \text{index}(\Gamma_\mu)$. Similarly, the same holds for the subspace $(U_n^{-1}.e_1^*,...,U_n^{-1}.e_p^*)$. Moreover, a.s. $\lim_{n \to \infty} \frac{q_{a+1}(M_n)}{q_{a+1}(M_n)} = 0$ and $\text{inf}_{n} \frac{q_{a}(M_n)}{q_{a}(M_n)} > 0$. The latter two assertions hold for $S_n$.

**Remark 4.8.** It is clear that we can replace $U_n^{-1}.e_1^*,...,U_n^{-1}.e_p^*$ with $U_n^te_1,...,U_n^te_p$ where $U_n^t$ is the transpose of the matrix $U_n$. However, we prefer to work with the action on the dual vector space because it will give us more freedom later on.
Proof. Let \( a_1(M_n), \ldots, a_d(M_n) \) be the diagonal components of \( a(M_n) \). Since \( K \) acts by isometries on \( V \), \( |a_1(M_n)| = ||M_n|| \). Hence, for the \( p \)-index \( \Gamma_\mu \), Theorem 4.5 gives a \( p \)-dimensional (random) subspace \( V(\omega) \) which is the range of every limit point of \( \frac{M_n}{a_1(M_n)} \). Fix a realization \( \omega \), we have:

\[
\frac{M_n(\omega)}{a_1(M_n(\omega))} = k(M_n(\omega)) \operatorname{diag} \left(1, \ldots, \frac{a_d(M_n(\omega))}{a_1(M_n(\omega))}\right) u(M_n(\omega))
\]

Each component in this equation lies in a compact set. If \( A(\omega), K_\omega(\omega), U(\omega), \alpha_2(\omega), \ldots, \alpha_d(\omega) \) are limit points of \( \frac{M_n}{a_1(M_n)} \times k(M_n(\omega)), u(M_n(\omega)), \frac{a_2(\omega)}{a_1(\omega)}, \ldots, \frac{a_d(\omega)}{a_1(\omega)} \), then

\[
A(\omega) = K_\omega(\omega)\operatorname{diag}(1, \ldots, \alpha_d(\omega)) U(\omega)
\]

Since \( A(\omega) \) is almost surely of range \( p \), almost surely, \( \alpha_p(\omega) = \ldots = \alpha_d(\omega) = 0 \) and \( \alpha_2(\omega), \ldots, \alpha_p(\omega) \) are non zero elements of \([0, 1]\) when \( k \) is archimedean and of \( \Omega_k \) when \( k \) is non archimedean; proving the last assertion of the corollary.

Since the image of \( A(\omega) \) is \( V(\omega) \),

\[
V(\omega) \subset \operatorname{Span}(K_\omega(\omega)e_1, \ldots, K_\omega(\omega)e_p)
\]

By equality of dimension, we deduce that the two subspaces above are almost surely equal. As this holds for any convergent subsequence, we have the convergence a.s. of the subspace \( (k(M_n)e_1, \ldots, k(M_n)e_p) \) towards \( V(\omega) \).

Now notice that \( \Gamma_\mu \) acts strongly irreducibly on \( V \) if and only if \( \Gamma_\mu^{-1} \) acts strongly irreducibly on \( V^* \). Moreover, \( \Gamma_\mu \) has the same index as \( \Gamma_\mu^{-1} \) viewed as a subgroup of \( SL(V^*) \) (it is just formed by the transposed matrices of \( \Gamma_\mu \)). Hence the same proof as above holds by looking at \( S_n^{-1} = X_1^{-1} \ldots X_n^{-1} \) acting on \( V^* \) instead of \( M_n = X_1 \cdots X_n \) acting on \( V \). \( \square \)

Proposition 4.9. If \( \Gamma_\mu \) acts strongly irreducibly on \( V \), then for any sequence \( \{x_n; n \geq 0\} \) in \( V \) converging to a non zero vector:

\[
a.s. \quad \inf_{n \in \mathbb{N}^*} \frac{||S_n x_n||}{||S_n||} > 0 \quad (6)
\]

Proof. Let \( S_n = K_n A_n U_n \) be a KAK decomposition and \( \{x_n\}_{n \in \mathbb{N}} \) a sequence in \( V \) converging to some \( x \neq 0 \).

When \( k \) is archimedean: To keep the exposition as simple as possible, we will work here with the transpose matrices instead of working on the dual vector space: for \( g \in SL_d(k) \), \( g^* \) will denote its transpose (resp. conjugate transpose) matrix when \( k = \mathbb{R} \) (resp. \( k = \mathbb{C} \)).

\[
\frac{||S_n x_n||^2}{||S_n||^2} = \frac{||A_n U_n x_n||^2}{||A_n||^2} = \sum_{i=1}^d \frac{a_i(n)^2}{a_1(n)^2} |U_n x_n, e_i > |^2 \geq \left( \frac{a_p(n)}{a_1(n)} \right)^2 \sum_{i=1}^p |< x_n, U_n^* e_i > |^2
\]

By Corollary 4.7, a.s. \( \inf_{n \in \mathbb{N}^*} \frac{a_p(n)}{a_1(n)} > 0 \).

We claim that a.s.

\[
\inf_{n \in \mathbb{N}^*} \sum_{i=1}^p |< x_n, U_n^* e_i > |^2 > 0 \quad (7)
\]

Indeed, by Corollary 4.7, the subspace \( (U_n^* e_1, \ldots, U_n^* e_d) \) converges a.s. to a subspace \( V(\omega) \). Let \( \Pi_{\nu}(\omega) \) be the orthogonal projection on \( V(\omega) \). Hence \( \sum_{i=1}^p |< U_n^* e_i, x_n > |^2 \xrightarrow{n \to \infty} ||\Pi_{\nu}(\omega)(x)||^2 \). By Theorem 4.5: \( \mathbb{P}(\Pi_{\nu}(\omega)(x) = 0) = 0 \). The claim is proved.

When \( k \) is non archimedean,

\[
\frac{||S_n x_n||}{||S_n||} = \frac{1}{|a_1(n)|} \max\{|a_i(n)||U_n^{-1} e_i^*(x_n)|; i = 1, \ldots, d\} \geq \frac{|a_p(n)|}{|a_1(n)|} \max\{|U_n^{-1} e_i^*(x_n)|; i = 1, \ldots, p\}
\]
Again, by Corollary 4.7, $\inf_{n \in \mathbb{N}} \frac{|x(n)|}{|x(0)|} > 0$ and it suffices to show that, a.s.,

$$\inf_{n \in \mathbb{N}} \text{Max}\{\|U_n^{-1}e_i^*(x_n)\|; \ i = 1, \ldots, p\} > 0$$

(8)

Indeed, let $V(\omega)$ be the limiting subspace of $\{U_n^{-1}e_1^*, \ldots, U_n^{-1}e_p^*\}$ and $U_\infty$ a limit point of $U_n$.

$\text{Max}\{\|U_n^{-1}e_i^*(x_n)\|; \ i = 1, \ldots, p\}$ converges a.s., via a subsequence, to $\text{Max}\{\|U_\infty^{-1}e_i^*(x)\|; \ i = 1, \ldots, p\}$. The following claim shows that this is in fact independent from the subsequence and equals $\text{Sup}\{\|f_\omega\|; \ f \in V(\omega)\}$, which is a.s. positive because by Theorem 4.5, $P\{f(x) = 0 \ \forall f \in V(\omega)\} = 0$.

**Claim:** Let $V$ be a vector space of dimension $d \geq 2$ with basis $(e_1, \ldots, e_d)$, $E$ a subspace of the dual $V^*$ of dimension $p < d$, $B = (f_1, \ldots, f_p)$ a basis of the dual $E$. We suppose that $B$ is in the orbit of $(e_1^*, \ldots, e_d^*)$ under the natural action of $K = SL_d(\mathbb{R})$ on $(V^*)^p$. In other words, assume that there exists $g \in K$ such that $f_i = ge_i^*$ for every $i = 1, \ldots, p$. Then for every non zero vector $x \in V$

$$\max\{|f_i(x)|; i = 1, \ldots, p\} = \text{Sup}\{\frac{|f(x)|}{\|f\|}; \ f \in E^*\}$$

**Proof of the claim:** let $f \in E^*$; $f = \sum_{i=1}^p \lambda_i f_i$, $\lambda_i \in k$. Since $\|\cdot\|$ is ultrametric, $|f(x)| \leq \text{Max}\{|\lambda_i|, i = 1, \ldots, p\}\text{Max}\{|f_i(x)|; i = 1, \ldots, p\}$. But, $f_i = ge_i^*$ with $g \in K$ which implies that $g^{-1}f = \sum_{i=1}^p \lambda_i^* e_i^*$ so that $|f(x)| = |g^{-1}f| = \text{Max}\{|\lambda_i|; i = 1, \ldots, p\}$. Hence $|f(x)| \leq \|f\| \text{Max}\{|f_i(x)|; i = 1, \ldots, p\}$.

**Corollary 4.10.** Suppose that $\int \log(|g|)d\mu(g) < \infty$. For any sequence $\{x_n; n \geq 0\}$ converging to a non zero vector $x$ of $V$:

$$\frac{1}{n} \log \|S_n x_n\| \overset{a.s.}{\longrightarrow} \lambda_1 \quad \text{Sup}_{x \in V \setminus \{0\}} \frac{1}{n} \mathbb{E} (\log \|S_n x\|) \relbar\joinrel\longrightarrow_{n \rightarrow \infty} \lambda_1$$

**Proof.** The convergence on the left hand side is an immediate application of last proposition and the definition of the Lyapunov exponent. For the right hand side, by compactness of $P(V)$, it suffices to show that for any sequence $\{x_n; n \geq 0\}$ in the unit sphere converging to a non zero vector $x$ of $V$: $\frac{1}{n} \mathbb{E} (\log \|S_n x_n\|) \longrightarrow \lambda_1$. By independence and equidistribution of the increments and by the inequality $|g| \geq 1$ true for every $g \in SL_d(k)$ we get: $\frac{1}{n} \log \|S_n x_n\| \leq \frac{1}{n} \sum_{i=1}^n \log \|X_i\|$. By the moment assumption on $\mu$, we can apply the strong law of large numbers which shows that the right hand side of the latter quantity converges in $L^1$ and is consequently uniformly integrable. A fortiori, $\{\frac{1}{n} \log \|S_n x_n\|; n \geq 0\}$ is uniformly integrable. Since it converges in probability (by the law of large numbers), we deduce that it converges in $L^1$.

### 4.2.2 A cocycle lemma - Application 1: “weak” large deviations

**Definition 4.11.** Let $G$ be a semigroup acting on a space $X$. A map $G \times X \overset{s}{\rightarrow} X$ is said to be an additive cocycle if $s(g_1g_2, x) = s(g_1, g_2 x) + s(g_2, x)$ for any $g_1, g_2 \in G$, $x \in B$.

**Lemma 4.12 (Cocycle lemma).** Let $G$ be a semigroup acting on a space $X$, $s$ a cocycle on $G \times X$, $\mu$ a probability measure on $G$ satisfying for $r(g) = \sup_{x \in X} |s(g, x)|$: there exists $\tau > 0$ such that

$$\mathbb{E} (\exp(\tau r(X_1))) < \infty$$

(9)

- If

$$\lim_{n \rightarrow \infty} \frac{1}{n} \text{Sup}_{x \in X} \mathbb{E}(s(S_n, x)) < 0,$$

then there exist $\lambda > 0$, $\epsilon_0 > 0$, $n_0 \in \mathbb{N}^*$ such that for every $0 < \epsilon < \epsilon_0$ and $n > n_0$:

$$\text{Sup}_{x \in X} \mathbb{E} [\exp(\epsilon s(S_n, x))] \leq (1 - \epsilon \lambda)^n$$

- If

$$\lim_{n \rightarrow \infty} \frac{1}{n} \text{Sup}_{x \in X} \mathbb{E}(s(S_n, x)) = 0,$$
then for all $\gamma > 0$, there exist $\epsilon(\gamma) > 0$, $n(\gamma) \in \mathbb{N}^*$ such that for every $0 < \epsilon < \epsilon(\gamma)$ and $n > n(\gamma)$,

$$\sup_{x \in X} \mathbb{E}[\exp(\epsilon(s(S_n, x)))] \leq (1 + \epsilon)^n.$$ 

**Remark 4.13.** The limit $\lim_{n \to \infty} \frac{1}{n} \sup_{x \in X} \mathbb{E}(s(S_n, x))$ always exists by sub-additivity.

**Proof.** Let $\epsilon > 0$ and $Q_n = \sup_{x \in X} \mathbb{E}[\exp(\epsilon(s(S_n, x)))]$. $Q_n$ being sub-multiplicative, for every $p$, we get for $\rho$

$$\lim_{n \to \infty} \frac{1}{n} \log Q_n \leq \frac{1}{p} \log Q_p$$

Using the inequality

$$\exp(x) \leq 1 + x + \frac{x^2}{2} \exp(|x|) ; x \in \mathbb{R}$$

we get for $\tau' = \frac{\epsilon}{p}$, $0 \leq \epsilon \leq \tau'$,

$$\lim_{n \to \infty} \frac{1}{n} \log Q_n \leq \frac{1}{p} \log \left(1 + \epsilon \sup_{x \in X} \mathbb{E}(s(S_p, x)) + \frac{\epsilon^2}{2 \tau'} \mathbb{E}(\exp(\tau r(S_p)))\right)$$

Let $C = \mathbb{E}(\exp(\tau(r(X_1)))) < \infty$. The cocycle property implies that $r(g_1 g_2) \leq r(g_1) + r(g_2)$ for every $g_1, g_2 \in G$, whence $\mathbb{E}(\exp(\tau(r(S_p)))) \leq C^p$. Hence, for every integer $p$,

$$\lim_{n \to \infty} \frac{1}{n} \log Q_n \leq \frac{1}{p} \log \left(1 + a_p + \frac{\epsilon^2}{2 \tau'} C_p\right) \quad (10)$$

The following inequality being true for every $x \in [-1; \infty]$:

$$(1 + x)\frac{1}{p} \leq 1 + \frac{x}{p}$$

(10) becomes: for every integer $p$,

$$\lim_{n \to \infty} \frac{1}{n} \log Q_n \leq \log \left(1 + a_p + \frac{\epsilon^2 C_p}{2 \tau'}\right) \quad (11)$$

- Suppose first that $\frac{a_p}{p}$ converges to $\lambda' < 0$ as $p$ goes to infinity. The quantity $a_p$ being sub-additive, $\frac{a_p}{p}$ converges to $\inf_p \frac{a_p}{p}$, hence $\inf_p \frac{a_p}{p} = \gamma' < 0$. Then, for some $p_0$, $a_{p_0} < 0$. Put $\lambda = \frac{a_{p_0}}{2p_0} > 0$. Apply (11) with $p = p_0$ and choose $\epsilon > 0$ small enough such that:

$$\frac{a_{p_0}}{p_0} + \frac{\epsilon^2 C_{p_0}}{2 \tau'} \leq -\lambda \iff 0 < \epsilon \leq \frac{-\tau' a_{p_0}}{C_{p_0}}.$$ 

- Suppose that $\frac{a_p}{p}$ converges to zero as $p$ goes to infinity.

Fix $\gamma > 0$. Since $\lim \frac{a_p}{p} = 0$, for $p \geq p(\gamma)$ large enough, $\frac{a_p}{p} \leq \frac{\gamma}{p}$. Fix such $p$. For $\epsilon \leq \epsilon(\gamma)$ small enough, $\epsilon^2 C_{p_0} \tau' \leq \epsilon^2$. It suffices now to apply (11). \square

**Application1:** “Weak large deviations” In the real and complex cases, Le Page [LP82] proved a large deviation inequality for the quantities $\frac{1}{n} \log ||S_n||$ and $\frac{1}{n} \log ||S_n x||$, for any non-zero vector $x$ of $V$. By Proposition 4.10 these quantities converge towards the first Lyapunov exponent $\lambda_1$. More precisely, for every $\epsilon > 0$, there exist $\rho = \rho(\epsilon) \in [0, 1]$ and $n_0 = n_0(\epsilon)$ such that for $n \geq n_0$,

$$\mathbb{P}\left(\left|\frac{1}{n} \log ||S_n|| - \lambda_1\right| \geq \epsilon\right) \leq \rho^n ; \quad \mathbb{P}\left(\left|\frac{1}{n} \log ||S_n x|| - \lambda_1\right| \geq \epsilon\right) \leq \rho^n \quad (12)$$

In particular, for some new $\rho = \rho(\epsilon) \in [0, 1]$,

$$\mathbb{P}\left(\frac{||S_n||}{||S_n x||} \geq \exp(n \epsilon)\right) \leq \rho^n \quad (13)$$

This bound will be important for us later. Verifying Le Page proof when $k$ is ultrametric is straightforward although somewhat lengthy. Alternatively we will directly show (13) using our cocycle Lemma 4.12. Moreover our bound will be uniform in $x$ ranging over the unit sphere in $V$. 15
Proposition 4.14 (Weak large deviations). Suppose that \( \mu \) has an exponential local moment and that \( \Gamma_\mu \) is strongly irreducible. Then for every \( \gamma > 0 \), there exist \( \epsilon(\gamma) > 0 \) and \( n(\gamma) \in \mathbb{N}^* \) such that for \( 0 < \epsilon < \epsilon(\gamma) \) and \( n > n(\gamma) \):

\[
\text{Sup}_{x \in V; \|x\|=1} \mathbb{E} \left[ \left( \frac{||S_n||}{||S_n x||} \right)^\gamma \right] \leq (1 + \epsilon \gamma)^n
\]

In particular, for every \( \epsilon > 0 \),

\[
\limsup_{n \to \infty} \left[ \text{Sup}_{x \in V; \|x\|=1} \mathbb{P} \left( \frac{||S_n||}{||S_n x||} \geq \exp(n\epsilon) \right) \right]^{\frac{1}{\epsilon}} < 0
\]

Proof. Let \( \gamma > 0 \). First we prove that for \( \epsilon < \epsilon(\gamma) \) and \( n > n(\gamma) \),

\[
\text{Sup}_{x \in [x], [y]} \mathbb{E} \left[ \left( \frac{||S_n x||}{||S_n y||} \right)^\gamma \right] \leq (1 + \epsilon \gamma)^n
\]

Indeed, \( s(g, ([x], [y])) = \log \frac{||S_n||}{||S_n x||} \) defines an additive cocycle on \( \Gamma_\mu \times (P(V) \times P(V)) \), for the natural action of \( \Gamma_\mu \) on \( P(V) \times P(V) \). It suffices now to verify the hypotheses of Lemma 4.12. Since for every \( g \in SL_d(k), ||g||^{-1} \leq ||g||^{-d-1} \), \( \mathbb{E}(\exp(\tau r(1_n))) \leq \mathbb{E}(||X_1||^r ||X_1^{-1}||^{r}) \leq \mathbb{E}(||X_1||^{-d}). \)

This is finite for \( \tau \) small enough because \( \mu \) has an exponential local moment. The condition (9) of Lemma 4.12 is then fulfilled. It suffices now to show that

\[
\lim_{n \to \infty} \text{Sup}_{x \in [x], [y]} \mathbb{E} \left( s(S_n, ([x], [y])) \right) = 0
\]

(\( \leq 0 \) suffices in fact). Since \( P(V) \times P(V) \) is compact, it suffices to show that for any convergent sequences \( (x_n) \) and \( (y_n) \) in the sphere of radius one:

\[
\lim_{n \to \infty} \frac{1}{n} \mathbb{E} (\log ||S_n x_n||) - \mathbb{E} (\log ||S_n y_n||) = 0
\]

This is true since by (the proof of ) Corollary 4.10:

\[
\lim_{n \to \infty} \frac{1}{n} \mathbb{E} (\log ||S_n x_n||) = \lim_{n \to \infty} \frac{1}{n} \mathbb{E} (\log ||S_n y_n||) = \lambda_1
\]

Notice that \( ||g|| \geq \max \{ ||g.e_i||; i = 1, ..., d \} \) for every \( g \in GL(V) \). Hence, \( \text{Sup}_{x \in [x]} \mathbb{E} \left[ \left( \frac{||S_n||}{||S_n x||} \right)^\gamma \right] \leq \sum_{g \in GL(V)} \text{Sup}_{x \in [x]} \mathbb{E} \left[ \left( \frac{||g.x||}{||g.x||} \right)^\gamma \right] \). Applying (16) shows (14).

Finally, we prove (15): let \( \epsilon > 0 \), \( \gamma > 0 \) to be chosen in terms of \( \epsilon \). By (14) and the Markov inequality there exist \( \epsilon'(\gamma) > 0, n(\gamma) > 0 \) such that for \( 0 < \epsilon' < \epsilon'(\gamma) \) and \( n > n(\gamma) \):

\[
\mathbb{P} \left( \frac{||S_n||}{||S_n x||} \geq \exp(n\epsilon) \right) \leq \exp(-n\epsilon') \mathbb{E} \left[ \left( \frac{||S_n||}{||S_n x||} \right)^{\epsilon'} \right] \leq \exp(-n\epsilon') (1 + \epsilon')^n
\]

Since \( \exp(-n\epsilon') = \exp(\epsilon')^{-n} \leq \frac{1}{(1 + \epsilon')^n} \), it suffices to choose \( \gamma = \frac{\epsilon'}{2} \). \( \square \)

4.2.3 Application 2: exponential convergence in direction

Proposition 4.15. Suppose that \( \mu \) has an exponential local moment and that \( \Gamma_\mu \) is strongly irreducible and contracting. Then there exist \( \lambda > 0 \), \( \epsilon_0 > 0 \), \( n_0 \in \mathbb{N}^* \) such that for \( 0 < \epsilon < \epsilon_0 \) and \( n > n_0 \):

\[
\mathbb{E} \left( \frac{\delta'(S_n[x], S_n[y])}{\delta'(x, y)} \right) \leq (1 - \lambda \epsilon)^n
\]

Proof. Let \( X = P(V) \times P(V) \) diagonal and \( s \) the application on \( \Gamma_\mu \times X \) defined by:

\[
s(g, ([x], [y])) = \log \frac{\delta(g[x], g[y])}{\delta([x], [y])} ; g \in \Gamma_\mu; ([x], [y]) \in X
\]
It is easy to verify that $s$ is an additive cocycle on $\Gamma_\mu \times X$ for the natural action of $\Gamma_\mu$ on $X$. It suffices now to check the hypotheses of Lemma 4.12.

By definition of the distance $\delta$, we have for every $g \in SL_d(k)$, $(\langle x \rangle, [y]) \in X$, $\log \frac{dP([z], [y])}{dP([x], [y])} \leq 2d \log \|g\|$. Since $\mu$ has an exponential local moment, (9) of Lemma 4.12 is valid. It is left to check that we are in the first case of the lemma, i.e. $\lim \frac{1}{n} \text{Sup}(\langle x \rangle, [y]) \in X E(s(S_n, (x, y))) < 0$.

\[ \frac{1}{n} \text{Sup}(\langle x \rangle, [y]) \in X E(s(S_n, (x, y))) \leq \frac{1}{n} \text{Sup}(\langle x \rangle, [y]) \in X E \left( \log \left\| \frac{\Lambda^2 S_n x \wedge y}{||x \wedge y||} \right\| \right) + \frac{2}{n} \text{Sup}(\langle x \rangle) \in P(V) E \left( \log \left\| \frac{||x||}{||S_n x||} \right\| \right) \]

By definition of the Lyapunov exponent,

\[ \frac{1}{n} E(\log \left\| \frac{1}{n} S_n \right\|) \rightarrow_{n \rightarrow \infty} \lambda_1 + \lambda_2 \]

By the proof of Corollary 4.10,

\[ \frac{1}{n} \text{Sup}(\langle x \rangle) \in P(V) E \left( \log \left\| \frac{||x||}{||S_n x||} \right\| \right) \rightarrow_{n \rightarrow \infty} -\lambda_1 \]

Hence,

\[ \lim \frac{1}{n} \text{Sup}(\langle x \rangle, [y]) \in X E(s(S_n, (x, y))) \rightarrow_{n \rightarrow \infty} \lambda_2 - \lambda_1 \]

Under the contraction and strong irreducibility assumptions on $\Gamma_\mu$, this is negative by Theorem 4.6. \hfill \square

We deduce the following

**Theorem 4.16** (Exponential convergence in direction). With the same notations and assumptions as in the previous proposition, there exists a random variable $Z_1$ (resp. $Z_2$) on $P(V)$ - with law $\nu$ (resp. $\nu^*$), the unique $\mu$-invariant probability measure on $P(V)$ (resp. $\mu^{-1}$-invariant on $P(V^*)$) such that for some $\lambda > 0$ and every $\epsilon > 0$:

\[ \text{Sup}(\langle x \rangle) \in P(V) E(\delta'(M_n[x], Z_1)) \leq (1 - \lambda \epsilon)^n \]  \hspace{1cm} (19)

\[ \text{Sup}(\langle x \rangle) \in P(V^*) E(\delta'(S_n^{-1}[f], Z_2)) \leq (1 - \lambda \epsilon)^n \]  \hspace{1cm} (20)

In particular, for every $[x] \in P(V)$ (resp. $[f] \in P(V^*)$), $M_n[x]$ (resp. $S_n^{-1}[f]$) converges almost surely towards $Z_1$ (resp. $Z_2$).

**Proof.** It suffices to prove (19). Indeed, (20) is the consequence of the fact that the action of $\Gamma_\mu$ on $V$ is strongly irreducible and contracting if and only if the action of $\Gamma_{\mu^{-1}}$ on $V^*$ is. Moreover, if (19) and (20) hold then $M_n[x]$ (resp. $S_n^{-1}[f]$) converges a.s. towards $Z_1$ (resp. $Z_2$) by an easy application of the Markov inequality.

Let $Z$ be the random variable on $P(V)$ obtained in Theorem 4.5. Let $\lambda > 0$, $\epsilon > 0$ small enough and $n \geq n_0$ given by the previous proposition. Fix $k > n$, $[y], [x] \in P(V)$. The triangle inequality gives:

\[ E(\delta'(M_n[x], Z)) \leq E(\delta'(M_n[x], M_k[y])) + E(\delta'(M_k[y], Z)) \]  \hspace{1cm} (21)

Since $M_k[y] = M_n X_{n+1} \ldots X_k [y]$, we condition by the $\sigma$-algebra generated by $(X_{n+1}, \ldots, X_k)$ and obtain by independence of the increments:

\[ (I) = \int d\mu^{k-n}(\gamma) E(\delta'(M_n[x], M_n[\gamma y])) \leq \text{Sup}(\langle a \rangle, [b]) E(\delta'(M_n[a], M_n[b])) \leq (1 - \lambda \epsilon)^n \]  \hspace{1cm} (22)
Inserting (22) in (21) gives for every \([y] \in P(V), k > n \geq n_0:\)

\[ Sup_{\mathcal{V}}\mathbb{E}(\delta'[M_n[x], Z]) \leq (1 - \lambda \epsilon)^n + \mathbb{E}(\delta'(M_k[y], Z)) \]

Let \(\nu\) be the unique \(\mu\)-invariant probability measure on \(P(V)\) (see Theorem 4.5). Integrating with respect to \(d\nu([y])\) the two members of the previous inequality and applying Fubini theorem, we get for every \(k > n \geq n_0:\)

\[ Sup_{\mathcal{V}}\mathbb{E}(\delta'(M_n[x], Z)) \leq (1 - \lambda \epsilon)^n + \mathbb{E}\left( \int \delta([y], Z) d(M_k\nu)([y]) \right) \]  \hspace{1cm} (23)

Again by Theorem 4.5, a.s. \(M_k\nu\) converges weakly towards the dirac measure \(\delta_Z\) when \(k\) goes to infinity. For \(w\) fixed and every \(0 < \epsilon \leq 1, \delta(\cdot, Z(\omega))\) is a continuous function on \(P(V)\). Hence, \(\int \delta'(\cdot, Z) d(M_k\nu)([y])\) converges a.s. to \(\delta'(Z, Z) = 0\) when \(k\) goes to infinity. By the dominated convergence theorem, \(\mathbb{E}\left( \int \delta'([y], Z) d(M_k\nu)([y]) \right) \to 0\). We conclude by letting \(k\) go to infinity in (23). Since \(\epsilon \mapsto \delta'(\cdot, \cdot)\) is decreasing, the corollary is true for every \(\epsilon > 0\).

\[ 4.2.4 \text{ Weak version of the regularity of invariant measure} \]

An important result in the theory of random matrix products is the regularity of the invariant measure \(\nu\), under contraction and strong irreducibility assumptions:

**Theorem 4.17.** [Gui90] \(k = \mathbb{R}\). Consider the same assumptions as in Proposition 4.15, then there exists \(\alpha > 0\) such that:

\[ Sup\{ \int \delta^{-\alpha}([x], H) d\nu([x]) ; H \text{ hyperplanes of } V \} < \infty \]

In particular, if \(Z\) is a random variable on \(P(V)\) with law \(\nu\), then for every \(\epsilon > 0\):

\[ Sup\{ \mathbb{P}(\delta(Z, H) \leq \epsilon) ; H \text{ hyperplane of } V \} \leq C\epsilon^\alpha \]  \hspace{1cm} (24)

(24) gives in particular for \(k = \mathbb{R}\): for every \(0 < t < 1:\)

\[ \limsup_{n \to \infty} \left[ Sup\{ \mathbb{P}(\delta(Z, [H]) \leq t^n) ; H \text{ hyperplanes of } V \} \right]^\frac{1}{n} < 1 \]

The latter assertion will be important for us. Proving Theorem 4.17 in an arbitrary local field can be done along the same lines as Guivarch’s proof over the reals. We will refrain from including the details of this proof here, since we will not need the full force of 4.17. Instead we give a direct proof of the last assertion, using our “weak large deviation” - Proposition 4.14.

**Theorem 4.18.** Consider the same assumptions as in Proposition 4.15. Let \(Z\) be a random variable with law \(\nu\), the unique \(\mu\)-invariant probability measure. Then, for all \(t \in ]0, 1],\)

\[ \limsup_{n \to \infty} \left[ Sup\{ \mathbb{P}(\delta(Z, [H]) \leq t^n) ; H \text{ hyperplanes of } V \} \right]^\frac{1}{n} < 1 \]

Before proving the theorem, we begin with an easy but crucial lemma.

**Lemma 4.19.** There exists a constant \(C(k)\) such that for every \(f \in V^*,\) a.s. there exists \(i = i(n, \omega) \in \{1, ..., d\}\) such that: \(|f(M_n e_i)| \geq C(k) ||M_n^{-1} f||\)
Proof. When $k$ in archimedean, a.s. $||M_n^{-1}f||^2 = \sum_{i=1}^{d} |M_n^{-1}f(e_i)|^2$. Take $C(k) = \frac{1}{d}$. When $k$ in non archimedean, the norm on $V^*$ is ultrametric. Hence, a.s. $||M_n^{-1}f|| = \max\{|M_n^{-1}f(e_i)|; i = 1, ..., d\}$. The lemma is then valid for $C(k) = 1$. □

Proof of Theorem 4.18: Let $H$ be a hyperplane of $V$, $f \in V^*$ such that $H = Ker(f)$. One can suppose $||f|| = 1$. Let $A_i$ be the event “$||f(M_n e_i)|| \geq C(k)||M_n^{-1}f||$”. By the previous lemma, $P(\cup_{i=1}^{d} A_i) = 1$. Hence,

$$P(\delta(Z, [H]) \leq t^n) \leq \sum_{i=1}^{d} P(\delta(Z, [H]) \leq t^n; 1_{A_i})$$

By Theorem 4.16, there exists $\rho_1 \in [0, 1]$ such that for all large $n$:

$$\sup_{x \in P(V)} E(\delta(M_n x, Z)) \leq \rho_1^n$$

This implies by the Markov inequality that for every $\rho_2 \in [\rho_1, 1]$ and for all large $n$:

$$P(\delta(M_n x, Z) \geq \rho_2^n) \leq (\frac{\rho_1}{\rho_2})^n; \forall x \in V \setminus \{0\}$$

(26)

On each event $A_i$, we apply inequality (26) for $x = e_i$. Inserting this in (25) and using the triangle inequality, we get:

$$P(\delta(Z, [H]) \leq t^n) \leq \sum_{i=1}^{d} P(\delta(M_n e_i, [H]) \leq \rho_2^n + t^n; 1_{A_i}) + d(\frac{\rho_1}{\rho_2})^n$$

(27)

On the event $A_i$,

$$\delta(M_n e_i, [H]) = \frac{|f(M_n e_i)|}{||M_n e_i||} \geq C(k) \frac{||M_n^{-1}f||}{||M_n e_i||}$$

(28)

Inserting (28) in (27) gives:

$$P(\delta(Z, [H]) \leq t^n) \leq \sum_{i=1}^{d} P\left(\frac{||M_n^{-1}f||}{||M_n e_i||} \leq \frac{\rho_2^n + t^n}{C(k)}\right) + d(\frac{\rho_1}{\rho_2})^n$$

The following assertion clearly ends the proof: for any $a \in [0, 1]$,

$$\limsup_{n \to \infty} \left[P\left(\frac{||M_n^{-1}f||}{||M_n x||} \leq a^n\right)\right]^\frac{1}{n} < 1$$

(29)

uniformly in $f \in V^*$ of norm one and $x \in V$ of norm one. Indeed, the action of $\Gamma_{\mu^{-1}}$ on $V^*$ is strongly irreducible and contracting. Hence we can apply Proposition 4.14 by replacing $S_n = X_n \cdots X_1$ with $M_n^{-1} = X_n^{-1} \cdots X_1^{-1}$, $V$ with $V^*$. If $M^*$ denotes the contragredient representation of $G$ on $V^*$, then for any $a \in [0, 1]$,

$$\limsup_{n \to \infty} \left[P\left(\frac{||M_n^{-1}f||}{||M_n^{-1} x||} \leq a^n\right)\right]^\frac{1}{n} < 1$$

uniformly in $x$ and $f$. Since $M_n^{-1} = \text{transpose of } M_n$, $||M_n x|| = ||M_n|| = ||\rho^*(M_n^{-1})||$. Then (29) is valid uniformly in $x$ and $f$.

4.3 Preliminaries on algebraic groups

Till the end of the paper, $k$ is a local field, $G$ is a $k$-algebraic group, $G = G(k)$ are the $k$-points of $G$. We will assume $G$ to be $k$-split and its connected component semi-simple. However $G$ itself is not assumed Zariski-connected unless explicitly mentioned. In general if $H$ is a $k$-algebraic group, $H$ will denote its group of $k$-points. The word “connected” will refer to the Zariski topology.

In this section, $G$ is connected. For references, one can see [Tit71] for the description of irreducible representations, [BT72], [BT84] or [Mac71] for the Cartan and the Iwasawa decomposition.
Decompositions in algebraic groups Let $A$ be a maximal $k$-torus of $G$, $X(A)$ be the group of $k$-rational characters of $A$, $\Delta$ be the system of roots of $G$ restricted to $A$, which consists of the common eigenvalues of $A$ in the adjoint representation. We fix an order on $\Delta$ and denote by $\Delta^+$ the system of positive roots, $\Pi$ the system of simple roots (roots than cannot be obtained as product of two positive roots) and define $A^+ = \{ a \in A ; |\alpha(a)| \geq 1 ; \forall \alpha \in \Delta^+ \}$. There exists a maximal compact subgroup $K$ of $G$ such that

$$G = KA^+K \quad \text{Cartan or KAN decomposition}$$

We denote by $\mathfrak{g}$ be the Lie algebra of $G$ over $k$ and define, for every $\alpha \in \Delta$, $\mathfrak{g}_\alpha = \{ x \in \mathfrak{g} ; Ad(a).x = \alpha(a)x \ \forall a \in A \}$. Let $N$ be the unique connected subgroup of $G$ whose Lie algebra is $\oplus_{\alpha \in \Delta^+} A\mathfrak{g}_\alpha$; it is a maximal unipotent connected subgroup. Then the following decomposition, called Iwasawa or KAN decomposition, holds:

$$G = KAN \quad \text{Iwasawa or KAN decomposition}$$

Rational Representations of algebraic groups In the previous paragraph, we used only the adjoint representation of $G$. More generally, if $(\rho, V)$ is a $k$-rational irreducible representation of $G$, $\chi \in X(A)$ is called a weight of $\rho$ if it is a common eigenvalue of $A$ under $\rho$. We denote by $V_\chi$ the weight space associated to $\chi$ which is $V_\chi = \{ x \in V ; \rho(a)x = \chi(a)x \ \forall a \in A \}$. Then $V = \oplus_{\chi \in X(A)} V_\chi$. The representation $\rho$ is characterized by a particular weight $\chi_{\rho}$ called highest weight which has the following properties:

- every weight $\chi$ of $\rho$ different from $\chi_{\rho}$ is of the form: $\chi = \frac{x_\alpha}{\prod_{\alpha \in \Delta} \alpha n_{\alpha}}$, where $n_{\alpha} \in \mathbb{N}$ for every simple root $\alpha$.
- Every $x \in V_{\chi_{\rho}}$ is fixed by the subgroup $N$.

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

Proposition 4.20. [Tit71] For every $\alpha \in \Pi$, let $w_\alpha$ be the fundamental weight associated to $\alpha$. Then the $k$-rational irreducible representation $(\rho_\alpha, V_\alpha)$ of $G$ whose highest weight is $w_\alpha$ (called fundamental representation) has a highest weight space of dimension one and satisfies $\Theta_{\rho_\alpha} = \{ \alpha \}$. 

Every $k$-rational irreducible representation $\rho$ of $G$ can be obtained as a sub-representation of tensor products of fundamental representations and $\chi_{\rho}$ is of the form $\prod_{\alpha \in \Pi} w_{\beta}^{n_{\beta}}$, with $s_{\alpha} \in \mathbb{N}$. We record below a basic fact about root systems ([Bou68, §1.9 et 1.10]).

Proposition 4.21. Every root $\alpha \in \Delta$ is of the form: $\alpha = \prod_{\beta \in \Pi} w_{\beta}^{n_{\beta}}$, with $n_{\beta} \in \mathbb{Z}$, for every $\beta \in \Pi$.

Good norm Let $\rho$ be a $k$-rational irreducible representation of $G$. We wish to find a special basis and norm of $V$ such that $\rho(G) = \rho(K)\rho(A^+)\rho(K)$ (resp. $\rho(G) = \rho(K)\rho(A)\rho(N)$) is the restriction of a Cartan (resp. Iwasawa) decomposition of $SL(V)$, i.e. $K$ acts by isometries on $V$, $A$ acts by diagonal matrices with $\rho(A^+) \subset \{ \text{diag}(a_1, ..., a_d) ; |a_i| | \forall i \neq 1 \}$, $\rho(N)$ fixes the first vector of the basis.

To do that we begin with standard definitions borrowed from Quint [Qui02b]. Let $V$ be a $k$-vector space. When $k$ is $\mathbb{R}$ (resp. $\mathbb{C}$), we say that a norm on $V$ is good if and only if it is induced by a Euclidian scalar product (resp. Hermitian scalar product). Now if $V$ is endowed with a good norm, a direct sum $V = V_1 \oplus V_2$ is good if and only if it is orthogonal with respect to the scalar product. When $k$ is non archimedean, we say that a norm on $V$ is good if and only if it is ultrametric, i.e., $||v + w|| \leq Max(||v||, ||w||) \ \forall v, w \in V$. A direct sum $V = V_1 \oplus V_2$ is good if and only if for every $v = v_1 + v_2$, with $v_1 \in V, v_2 \in V$, $||v|| = Max(||v_1||, ||v_2||)$.

Now let $(\rho, V)$ be $k$-rational irreducible representation of $G$ and $V = \oplus_{\chi} V_\chi$ its decomposition into weight spaces. We write $G = KAK$ its Cartan decomposition.
Theorem 4.22. ([Mos73, §2.6] for $k$ archimedean, [Qui02a, Theorem 6.1] for $k$ non archimedean) When $k = \mathbb{R}$ (resp. $\mathbb{C}$), there exists a scalar product (resp. Hermitian scalar product) on $V$ such that $\rho(K)$ acts by isometries on $V$ and $\rho(A)$ is symmetric (resp. Hermitian). The direct sum $V = \oplus \chi_V$ is good and $a \in A$ induces on each $V_\chi$ a homothety of ratio $\chi(a)$.

When $K$ is non archimedean, there exists a $K$-invariant ultrametric norm on $V$ such that the $V_\chi$'s are in good direct sum. The action of $a \in A$ on $V_\chi$ is by homothety of ratio $\chi(a)$.

Such a norm is said to be $(\rho, A, K)$-good.

Corollary 4.23. Let $(\rho, V)$ be a $k$-rational representation of $G$, $\chi_\rho$ its highest weight. Then there exists a good norm $\|\cdot\|$ on $V$ such that

$$\|\rho(g)\| = |\chi_\rho(a(g))| ; g \in G$$

And for every $x_\rho \in V_\chi \setminus \{0\}$,

$$\frac{\|\rho(g)x_\rho\|}{\|x_\rho\|} = |\chi_\rho(\tilde{a}(g))| ; g \in G$$

where $a(g)$ (resp. $\tilde{a}(g)$) is the $A^+$ (resp. $A$) - component of $g$ in the Cartan (resp. Iwasawa) decomposition.

Fubini-Study norm: Consider a good norm on $V$ and a good direct sum: $V = V_1 \oplus V_2$. Then, there exists a good norm on $\bigwedge^2 V$ such that the direct sum $\bigwedge^2 V_1 \oplus (V_1 \bigwedge V_2) \oplus \bigwedge^2 V_2$ is good. This induces the Fubini-Study distance $\delta$ on the projective space $P(V)$:

$$\delta([x], [y]) = \frac{||x \wedge y||}{||x|| \cdot ||y||} ; [x], [y] \in P(V)$$

An example: $SL_d(k)$ ([PR94]) Here we consider $G = SL_d$. A maximal $k$-torus is $A = \{\text{diag}(a_1, \ldots, a_d); \prod_{i=1}^d a_i = 1\}$ and $A^+ = \{\text{diag}(a_1, \ldots, a_d) \in A; |a_1| \geq \ldots \geq |a_d|\}$.

To simplify notations, for $i = 1, \ldots, d$, we denote by $\lambda_i$ the following rational character of $A$: $(\lambda_1, \ldots, \lambda_d) \mapsto \lambda_i$. Simple roots are $\lambda_i/\lambda_{i+1}$, $i = 1, \ldots, d-1$. Positive roots are $\lambda_i/\lambda_j$, $1 \leq i < j \leq d$. The fundamental weight associated to $\alpha_i = \lambda_i/\lambda_{i+1}$ is $w_i = \lambda_i \ldots \lambda_1$ and the representation $\rho_{\lambda_i}$ of Proposition 4.20 is just $\bigwedge^i V$. The expression of simple roots in terms of fundamental weights is:

$$\alpha_i = w_{i-1}^{-1}.w_i^2.w_{i+1}^{-1} ; i = 1, \ldots, d$$

Let $K = SO_d(\mathbb{R})$ (resp. $K = SU_d(\mathbb{C})$) when $k = \mathbb{R}$ (resp. $k = \mathbb{C}$) and $K = SL_d(\Omega_k)$ when $k$ is non archimedean. We denote by $N$ the subgroup of upper triangular matrices with 1 on the diagonal. Then the Cartan decomposition is $G = KA^+K$ and the Iwasawa decomposition: $G = KAN$. As seen in Section 3.2, we can also take the following other choice for $A^+$: $A^+ = \{\text{diag}(a_1, \ldots, a_d); a_i \in [0; +\infty]; a_1 \geq \ldots \geq a_d > 0; \prod_{i=1}^d a_i = 1\}$ when $k = \mathbb{R}$ or $\mathbb{C}$ and $A^+ = \{\text{diag}(\pi^{n_1}, \ldots, \pi^{n_d}); n_1 \leq \ldots \leq n_d; \sum_{i=1}^d n_i = 0\}$ when $k$ is non archimedean. Let $B = (e_1, \ldots, e_d)$ be the canonical basis on $V$ and $\|\cdot\|$ the canonical norm on $V$ (see Section 4.2.1), then it is clear that $K$ acts by isometries on $V = k^d$. Consequently, $B$ is in a good direct sum and $\|\cdot\|$ is $(A, K)$-good.

4.4 Estimates in the Cartan decomposition - the connected case

In this section $G$ is assumed Zariski-connected. Recall that $G$ is also assumed semi-simple and $k$-split.

Let $\mu$ be a probability measure on $G = G(k)$ and $\rho$ a $k$-rational irreducible representation of $G$ into some $SL_d(k)$. We assume $\Gamma_{\mu}$ to be Zariski dense in $G$.

Our aim in this section is to give estimates of the Cartan decomposition in $\rho(G)$ of the random walks $\rho(M_n)$, $\rho(S_n)$ using their Iwasawa decomposition.
Let $\chi_\rho$ be the highest weight for $V$, and $r$ the number of non zero weights of $V$. We set $\chi_1 = \chi_\rho$, $\chi_2, \ldots, \chi_l \ (l \in \{2, \ldots, r\})$ the weights adjacent to $\chi_1$, i.e., such that $\chi_1 = \chi_l$ or there is $\alpha \in \Theta_n$ such that $\chi_l = \chi_1/\alpha$. We consider a $(\rho, A, K)$-good norm on $V$ (for the basis of weights) given by Theorem 4.22 of the preliminaries.

For $g \in G$, we denote by $g = k(g)a(g)u(g) \ (\text{resp. } g = k(g)a(g)n(g))$ a privileged Cartan (resp. Iwasawa) decomposition in $G = KA^+K = KAN$. When it comes to the random walk $S_n = X_n \ldots X_1$, we simply write $S_n = K_nA_nU_n$ (resp. $S_n = K_n\tilde{A}_nN_n$) for the KAK (resp. KAN) decomposition of $S_n$ in $G$ and set $\rho(A_n) = \text{diag}(a_1(n), \ldots, a_d(n))$ ; $\rho(\tilde{A}_n) = \text{diag}(a_1(n), \ldots, a_d(n))$.

It is known that $G$ is isomorphic to a closed subgroup of $GL_r(k)$ for some $r \geq 2$ - [Hum75]. Let $i$ be such an isomorphism. (When $G$ is simple and of adjoint type, one can take the adjoint representation).

**Definition 4.24** (Exponential moment for algebraic groups). If $\mu$ is a probability measure on $G$, we say that $\mu$ has an exponential local moment if $i(\mu)$ (image of $\mu$ under $i$) has an exponential local moment (see Definition 2.9).

The following lemma explains why this is a well defined notion, i.e. the existence of exponential moment is independent of the embedding $^{-i}$.

**Lemma 4.25.** Let $G \subset SL(V)$ be the $k$-points of a semi-simple algebraic group and $\rho$ a finite dimensional $k$-algebraic representation of $G$. If $\mu$ has an exponential local moment then the image of $\mu$ under $\rho$ also has an exponential local moment.

**Proof.** Each matrix coefficient $(\rho(g))_{i,j}$ of $\rho(g)$, for $g \in G$, is a fixed polynomial in terms of the matrix coefficients of $g$. Since for the canonical norm, $||g|| \geq 1$ for every $g \in G$, we see that there exists $C > 0$ such that $||\rho(g)|| \leq ||g||^C$ for every $g \in G$. This suffices to show the lemma. \(\square\)

### 4.4.1 Comparison between (the A-components of) the Cartan and Iwasawa decompositions.

Estimating the asymptotic behavior of the components of $S_n$ in the KAK decomposition will be crucial for us. We will derive these estimations from their analogs for the KAN decomposition. The following proposition explains why it is legal to do so:

**Proposition 4.26** (Comparison between KAK and KAN). *Almost surely there exists a compact subset $C$ of $G$ such that for every $\alpha \in \mathbb{N}^*$, $A_n\tilde{A}_n^{-1}$ belongs to $C$. In particular, there exists a compact subset $D$ of $GL(V)$ such that $\rho(A_n)\rho(\tilde{A}_n)^{-1}$ belongs to $D$.*

**Proof.** Since the kernel of the adjoint representation is finite, it suffices to show that there exists a compact subset $E$ of $GL(g)$ such that $Ad(A_n)Ad(\tilde{A}_n^{-1})$ belongs to $E$. This is equivalent to show that almost surely $\frac{\alpha(A_n)}{\alpha(\tilde{A}_n)}$ is in a random compact subset of $k$ for every $\alpha \in \Pi$. Indeed, we decompose $\alpha$ into fundamental weights: $\alpha = \prod_{\beta \in \Pi} w_\beta^{n_\beta}$; $n_\beta \in \mathbb{Z}$. Hence,

$$
\frac{\alpha(A_n)}{\alpha(\tilde{A}_n)} = \prod_{\beta \in \Pi} \left( \frac{w_\beta(A_n)}{w_\beta(\tilde{A}_n)} \right)^{n_\beta}, \quad (30)
$$

By Theorem 4.22, for each $\beta \in \Pi$, there exists a representation $(\rho_\beta, V_\beta)$ of $G$ whose highest weight is $w_\beta$ and highest weight space is a line, say $k x_\beta$. Fix a $(\rho_\beta, A, K)$-good norm on $V_\beta$. Corollary 4.23 applied to the representation $\rho_\beta$ gives then:

$$
||\rho_\beta(S_n)|| = |w_\beta(A_n)| ; \quad \frac{||\rho_\beta(S_n)x_\beta||}{||x_\beta||} = |w_\beta(\tilde{A}_n)|
$$

22
Then (30) becomes then
\[ \frac{\alpha(A_n)}{\alpha(\tilde{A}_n)} = \prod_{\beta \in \Pi} \left( \frac{||\rho_\beta(S_n)||}{||\rho_\beta(\tilde{S}_n)\chi|\beta||} \right)^{\eta_\beta} \] (31)

It suffices to control the terms where \( n_\beta \geq 0 \). Since \( G \) is Zariski-connected, \( \rho_\beta \) is in fact strongly irreducible. By Zariski density, \( \rho_\beta(\Gamma_n) \) also. Hence we can apply Proposition 4.9:
\[ \text{a.s.} \quad \sup_{n \in \mathbb{N}} \frac{||\rho_\beta(S_n)||}{||\rho_\beta(\tilde{S}_n)\chi|\beta||} < \infty \]

This is what we want to show. \hfill \Box

A version of the latter proposition “in expectation” will be needed.

**Proposition 4.27** (Comparison between KAK and KAN in expectation). Assume that \( \mu \) has an exponential local moment (Definition 4.24). For every \( \gamma > 0 \), there exist \( \epsilon(\gamma) > 0 \) and \( n(\gamma) \in \mathbb{N}^* \) such that for \( 0 < \epsilon < \epsilon(\gamma) \), \( n > n(\gamma) \) and every \( \alpha \in \Pi \):
\[ E\left( \left| \frac{\alpha(A_n)}{\alpha(\tilde{A}_n)} \right|^{\epsilon} \right) \leq (1 + \epsilon\gamma)^n \quad ; \quad E\left( \left| \frac{\alpha(\tilde{A}_n)}{\alpha(A_n)} \right|^{\epsilon} \right) \leq (1 + \epsilon\gamma)^n \] (32)

Moreover,
\[ E(||\rho(A_n)|\rho(\tilde{A}_n)\chi|^{-1})||^{\epsilon} \leq (1 + \epsilon\gamma)^n \] (33)

**Proof.** Let \( \epsilon > 0 \) and \( \alpha \in \Pi \). Let \( \beta_1, ..., \beta_s \) be an order of the simple roots appearing in identity (31). Holder inequality (for \( s \) maps) applied to the same identity gives:
\[ E\left( \left| \frac{\alpha(A_n)}{\alpha(\tilde{A}_n)} \right|^{\epsilon} \right) \leq \prod_{i=1}^{s} \left[ E\left( \left| \frac{||\rho_\beta(S_n)||}{||\rho_\beta(\tilde{S}_n)\chi|\beta||} \right|^{\epsilon} \right) \right]^\frac{1}{n} \]

Terms with \( n_{\beta_i} \leq 0 \) are less or equal to one. Hence, it suffices to control the terms where \( n_{\beta_i} > 0 \). Fix such \( i \in \{1, ..., s\} \) and let \( \gamma > 0 \). By Lemma 4.25, the image of \( \mu \) under \( \rho_\beta \) has an exponential local moment. Moreover, as explained in the previous proposition, \( G \) being Zariski-connected, \( \rho_\beta \) is strongly irreducible. Consequently, we can apply Proposition 4.14 which shows that
\[ E\left( \left| \frac{||\rho_\beta(S_n)||}{||\rho_\beta(\tilde{S}_n)\chi|\beta||} \right|^{\epsilon} \right) \leq (1 + \gamma\epsilon)^n. \]

Hence \( E\left( \left| \frac{\alpha(A_n)}{\alpha(\tilde{A}_n)} \right|^{\epsilon} \right) \leq (1 + \gamma\epsilon)^n \). In the same way, we show the inequality on the right hand side of (32).

In particular, for every non zero weight \( \chi \) of \( (\rho, V) \) different from \( \chi_{\rho'} \),
\[ E\left( \left| \frac{\chi(A_n)}{\chi(\tilde{A}_n)} \right|^{\epsilon} \right) \leq (1 + \gamma\epsilon)^n. \]

Indeed, this follows from the expression \( \chi = \chi_1 / \prod_{i \in \Pi} \alpha^{s_i} \) with \( s_i \in \mathbb{N} \) and the Holder inequality applied to (32). For \( \chi = \chi_{\rho} \), a similar inequality holds because \( \chi_\rho(\tilde{A}_n)/\chi_\rho(\tilde{A}_n) = ||S_n||/||\tilde{S}_n\chi|| \) for some \( (\rho, A, K) \)-good norm and every \( x \in V_{\chi_{\tilde{A}}}. \) This proves (33). \hfill \Box

The following theorem shows that the ratio between the first two components in the Iwasawa decomposition is exponentially small.

**Theorem 4.28** (Exponential contraction in KAN). Assume that \( \mu \) has an exponential local moment and that \( \rho(\Gamma_n) \) is contracting. Then there exists \( \lambda > 0 \), such that for every \( \epsilon > 0 \) small enough and all \( n \) large enough:
\[ E\left( \frac{a_i(n)}{a_1(n)} \right)^{\epsilon} \leq (1 - \lambda\epsilon)^n \quad ; \quad i = 2, ..., d \]

We recall that \( \tilde{A}_n \) is the \( A \)-component of \( S_n \) in the Iwasawa decomposition of \( S_n \) in \( G \) and that \( \tilde{a}_1(n), ..., \tilde{a}_d(n) \) are the diagonal components of \( \rho(\tilde{A}_n) \) in the basis of weights.
4.12 Remark. When \( k = \mathbb{R} \), no contraction assumption is needed. Indeed, by a theorem of Goldscheid-Marquis [GM89], a semigroup \( \Gamma \) of \( GL_d(\mathbb{R}) \) is strongly irreducible and contracting if and only if its Zariski closure is. Hence \( \rho(\Gamma_n) \) is contracting if and only if \( \rho(G) \) is. But \( G \) is \( \mathbb{R} \)-split, hence the highest weight space of \( \rho \) is a line, thus \( \rho \) is contracting.

Before proving the proposition, we state a standard lemma in this theory:

**Lemma 4.30.** [Dek82] Let \( G \) be a group, \( X \) be a \( G \)-space, \( (X_n)_{n \in \mathbb{N}^*} \) a sequence of independent elements of \( G \) with distribution \( \mu \) and \( s \) an additive cocycle on \( G \times X \). Suppose that \( \nu \) is a \( \mu \)-invariant probability measure on \( X \) such that:

1. \( \int \int s^\gamma(g,x) d\mu(g) d\nu(x) < \infty \) where \( y^\gamma = \sup(0,y) \) for every \( y \in \mathbb{R} \).
2. For \( \mathbb{P} \otimes \nu \)-almost every \((\omega, x)\), \( \lim_{n \to \infty} s(X_n(\omega) \ldots X_1(\omega), x) = +\infty \).

Then \( s \) is in \( L^1(\mathbb{P} \otimes \nu) \) and \( \int s(g,x) d\mu(g) d\nu(x) > 0 \)

**Proof of Theorem 4.28:** Since \( \rho \) is contracting, \( V_{\rho} \) is a line. Indeed, if \( \{\eta_n; n \in \mathbb{N}\} \) is a sequence in \( G \) such that \( \{\rho(\eta_n); n \in \mathbb{N}\} \) is contracting then it is easy to see that \( \{\rho(\eta_n); n \in \mathbb{N}\} \) is also contracting. \( V_{\rho} \) is then a one dimensional subspace. Therefore, for some \( \alpha \in \Theta_\rho \), \( \frac{a(n)}{a_1(n)} = \frac{\alpha(A_n)}{\alpha(A_1)} \) and in general for \( i \in \{2, \ldots, d\} \), \( \frac{a(n)}{a_1(n)} \) is of the form \( 1/ \prod_{\beta \in \Theta_\rho} \beta^{\eta_n} (A_n) \) with \( m_\beta \in \mathbb{N} \) for every \( \beta \in \Pi \). By Holder inequality, it suffices to treat the case where \( \frac{a_1(n)}{a_1(n)} = 1/\alpha(A_n) \) for some \( \alpha \in \Theta_\rho \). As in Proposition 4.26, we decompose \( \alpha \) into fundamental weights: \( \alpha = \prod_{i=1}^s w_{\beta_i} \), with \( s \in \mathbb{N}^* \), \( \eta_i \in \mathbb{Z} \) for every \( i = 1, \ldots, s \). We denote \( \{\rho_{\beta_i}, V_{\beta_i}\} \) the fundamental representation associated to \( \eta_i \). Using (31) of the same proposition, we get for every \( i = 1, \ldots, s \), \( a(\rho_{\beta_i}, A, K) \)-good norm on \( V_i \) such that:

\[
\left| \frac{a(n)}{a_1(n)} \right| = \prod_{i=1}^s \left( \frac{\|\rho_{\beta_i}(A_n)x_{\beta_i}\|}{\|x_{\beta_i}\|} \right)^{-\eta_n} \leq \sup_{x \in X} \exp(-s_*(S_n, x))
\]

where \( X = \oplus_{i=1}^s P(V_{\beta_i}) \) and \( s \) is the cocycle defined on \( G \times X \) by:

\[
s(g, ([x_1], \ldots, [x_s])) = \sum_{i=1}^s n_{\beta_i} \log \frac{\|\rho_{\beta_i}(g) x_i\|}{\|x_i\|}
\]

To apply Lemma 4.12, we must verify that for some \( \tau > 0 \),

\[
E(\exp(\tau \sup_{x \in X} |s(X, x)|)) < \infty \tag{34}
\]

and

\[
\lim_{n \to \infty} \frac{1}{n} \sup_{x \in X} E(-s(S_n, x)) < 0 \tag{35}
\]

By Lemma 4.25, there exists \( \tau > 0 \) such that for every \( i = 1, \ldots, s \), \( E(\|\rho_{\beta_i}(X_1)\|^{\tau}) < \infty \). Holder inequality applied recursively ends the proof of (34). Now we concentrate on proving (35). Since \( P(V_{\beta_i}) \) is compact for every \( i = 1, \ldots, s \), it suffices to show that for all sequences \( \{x_{1,n}; n \geq 0\}, \ldots, \{x_{s,n}; n \geq 0\} \) converging to non zero elements of \( V_{\beta_1}, \ldots, V_{\beta_i} \):

\[
\lim_{n \to \infty} \frac{1}{n} s(S_n, ([x_{1,n}], \ldots, [x_{s,n}])) = \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^s n_{\beta_i} \log \left( \frac{\|\rho_{\beta_i}(S_n) x_{i,n}\|}{\|x_{i,n}\|} \right) > 0
\]

Fix such sequences \( \{x_{1,n}; n \geq 0\}, \ldots, \{x_{s,n}; n \geq 0\} \). By Corollary 4.10 the limit above exists and is independent of the sequences taken. Indeed, it is equal to the sum of the corresponding Lyapunov exponents. Denote by \( L \) this limit. Fix a \( \mu \)-invariant probability measure \( \nu \) on \( X \), which exists by compactness of \( X \). Again by Corollary 4.10,

\[
L = \lim_{n \to \infty} \frac{1}{n} s(S_n(\omega), x) = \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^s n_{\beta_i} \log \frac{\|\rho_{\beta_i}(S_n(\omega)) x_i\|}{\|x_i\|} \text{ for } \mathbb{P} \otimes \nu - \text{almost all } (\omega, x)
\]
Consider the dynamical system $E = G^N \times X$, the distribution $\eta = \mathbb{P} \otimes \nu$ on $E$, the shift $\theta : E \to E$, $((g_0, \ldots), x) \mapsto ((g_1, \ldots), g_0.x)$. Since $\nu$ is $\mu$-invariant, $\eta$ is $\theta$-invariant. We extend the definition domain of $s$ from $G \times X$ to $G^N \times X$ by setting $s(\omega, x) := s(g_0, x)$ if $\omega = (g_0, \ldots)$. Since $\mu$ has an exponential moment, $s \in L_1(\eta)$. In consequence, we can apply the ergodic theorem (see [Bre68, Theorem 6.21]) which shows that $\frac{1}{n} \sum_{i=0}^n s \circ \theta^i(\omega, x)$ converges for $\eta$-almost every $(\omega, x)$ to a random variable $Y$ whose expectation is $\iint s(g, x) d\mu(g) d\nu(x)$. Since $s$ is a cocycle, $s(S_n(\omega), x) = \sum_{i=0}^n s \circ \theta^i(\omega, x)$. Hence,

$$\lim_{n \to \infty} \frac{1}{n} s(S_n(\omega), x) = Y \quad ; \quad \mathbb{E}_\eta(Y) = \iint s(g, x) d\mu(g) d\nu(x)$$

But we have shown above that $Y$ is almost surely constant, because it is the sum of the corresponding Lyapunov exponents, and that it equal to $L$. Hence,

$$L = \iint s(g, x) d\mu(g) d\nu(x)$$

$L$ is positive if conditions (1) and (2) of Lemma 4.30 are fulfilled. Since $\mu$ has a moment of order one, condition (1) is readily satisfied.

Condition (2): we must verify that for $\mathbb{P} \otimes \nu$-almost all $(\omega, x)$,

$$s(S_n(\omega), x) = \sum_{i=1}^n n_{\beta_i} \log \frac{||\rho_{\beta_i}(S_n(\omega)) x_i||}{||x_i||} \xrightarrow{n \to \infty} + \infty \quad (36)$$

By Proposition 4.9, the $\mathbb{P} \otimes \nu$-almost everywhere behavior at infinity of $s(S_n(\omega), x)$ is the same as the $\mathbb{P}$-almost everywhere behavior of:

$$\sum_{i=1}^n n_{\beta_i} \log ||\rho_{\beta_i}(S_n)|| = \log ||\alpha(A_n)||$$

The last equality follows from the expression of $\alpha$ in terms of the fundamental weights and from Corollary 4.23. Hence, we reduced the problem to proving that $||\alpha(A_n)|| \xrightarrow{n \to \infty} + \infty$ for every $\alpha \in \Theta_\rho$. $\rho(\Gamma_\mu)$ is strongly irreducible because $\Gamma_\mu$ is Zariski dense in $G$, $\rho$ is an irreducible representation of $G$ and $G$ is connected. Since by the hypothesis $\rho(\Gamma_\mu)$ is contracting, we can apply Theorem 4.5: $||.||$ being $(\rho, A, K)$-good norm, $|a_1(n)| = ||\rho(S_n)||$. Hence a.s. every limit point of $\frac{\alpha(S_n)}{a_1(n)}$ is a rank one matrix. In particular, $\frac{a_2(n)}{a_1(n)}, \ldots, \frac{a_d(n)}{a_1(n)}$ converge a.s. to zero. Equivalently, for every weight $\chi \neq \chi_\rho$ of $V$, $|\chi_\rho(A_n) / \chi(A_n)|$ tends a.s. to infinity. From the expression of $\chi$ in terms of $\chi_\rho$, this is equivalent to say that for every $\alpha \in \Theta_\rho$, $|\alpha(A_n)|$ tends to infinity.

The following theorem shows that the ratio between the first two components in the Cartan decomposition is exponentially small.

**Theorem 4.31** (Exponential contraction in $KAK$). With the same hypotheses as in Theorem 4.28, there exists $\lambda > 0$ such that for all $\epsilon > 0$:

$$\limsup_{n \to \infty} \left[ \mathbb{E}(\frac{a_i(n)}{a_1(n)}) \right]^{\frac{1}{n}} \leq 1 - \lambda \epsilon \quad ; \quad i = 2, \ldots, d$$

**Proof.** Let $i \in \{2, \ldots, d\}$. Since $|a_i(\rho(a))| \leq |a_1(\rho(a))|$ for every $a \in A^+$, it suffices to show the theorem for all $\epsilon > 0$ small enough. Write

$$\frac{a_i(n)}{a_1(n)} = \frac{a_i(n)}{a_1(n)} \times \frac{a_i(n)}{a_1(n)} \times \frac{a_i(n)}{a_1(n)}$$
Fix $\gamma > 0$. By Propositions 4.27 and 4.28 and Holder inequality, we have for some $\lambda > 0$, every $0 < \epsilon < \min\{\epsilon(\gamma); \frac{1}{\lambda}\}$ and $n > n(\gamma)$:

$$\mathbb{E}(\frac{a_i(n)}{a_1(n)})^\epsilon \leq (1 + 3\gamma\epsilon)^\epsilon(1 - 3\gamma\epsilon)^\epsilon \leq (1 + \gamma\epsilon)^2(1 - \lambda\epsilon) \leq 2(1 + \gamma^2\epsilon)(1 - \lambda\epsilon)$$

We have used the inequality $(1 + x)^r \leq 1 + rx$ true for every $x \geq -1$ and $r \in [0, 1]$ and the inequality $(x + y)^2 \leq 2(x^2 + y^2)$ true for every $x, y \in \mathbb{R}$. It suffices to choose $\gamma = \frac{\epsilon_0}{\lambda\epsilon}$ for instance.

We will see in Section 4.5 that in order to work with non Zariski-connected algebraic groups, it is convenient to work with the Cartan decomposition of the ambient group $SL_d(k)$ (see Section 3.2). The following corollary will be useful. It is the analog of Theorem 4.31 for the KAK decomposition in $SL_d(k)$ (rather than in $G$).

**Corollary 4.32** (Ratio in the $A$-component for the KAK decomposition of $SL_d(k)$). For $g \in SL_d(k)$, we denote by $g = k(g)a(g)u(g)$ an arbitrary but fixed Cartan decomposition of $g$ in $SL_d(k)$ as described in Section 3.2. We write $a(g) = \text{diag}(a_1(g), ..., a_d(g))$ in the canonical basis of $k^d$.

With these notations and with the same assumptions as in Theorem 4.28, we have for some $\lambda > 0$ and every $\epsilon > 0$,

$$\limsup_{n \to \infty} \mathbb{E}\left(\frac{|a_i(n)|^\epsilon}{|a_1(n)|^\epsilon}\right) \leq 1 - \gamma\epsilon \quad ; \quad i = 2, ..., d$$

**Proof.** To simplify notations we omit $\rho$, so that $G$ is seen as a linear algebraic subgroup of $SL_d(k)$. Let $S_n = K_nA_nU_n$ be the Cartan decomposition of $S_n$ in $G$ (Section 4.3) and $S_n = \hat{K}_n\hat{A}_n\hat{U}_n$ its Cartan decomposition in $SL_d(k)$ (Section 3.2). Recall that $A_n$ is a diagonal matrix $\text{diag}(a_1(n), ..., a_d(n))$ in the basis of weights while $\hat{A}_n$ is a diagonal matrix $\text{diag}(a_1(n), ..., a_d(n))$ in the canonical basis of $k^d$. We will use the canonical basis and norm of $k^d$ (Section 4.2.1).

Theorem 4.31 shows that for some $\lambda > 0$, every $\epsilon > 0$ and all large $n$,

$$\mathbb{E}\left(\frac{|a_i(n)|^\epsilon}{|a_1(n)|^\epsilon}\right) \leq (1 - \gamma\epsilon)^n \quad ; \quad i = 2, ..., d \quad (37)$$

Since $K_n, \hat{K}_n$ belong to compact subgroups in both decompositions, there exist $C_1, C_2 > 0$ such that for every $n$: $C_2||A_n|| \leq ||\hat{A}_n|| \leq C_1||A_n||$ and $C_2||A_n|| \leq ||A_n|| \leq C_1||\hat{A}_n||$.

By the definition of the KAK decomposition in $SL_d(k)$, we have a.s. $||\hat{A}_n|| = |\hat{a}_1(n)|$ and $||A_n|| = |a_1(n)a_i(n)|$. For KAK in $G$, there exists a constant $C_3 > 0$ such that: $\frac{1}{C_3}|a_1(n)| \leq ||A_n|| \leq C_3|a_1(n)|$ and for $\mathbb{P}$-almost every $\omega$ there exists $i(\omega) \in \{2, ..., l\}$ such that:

$$\frac{1}{C_3}|a_1(n)a_i(\omega)(n)| \leq ||\bigwedge^2 A_n(\omega)|| \leq C_3|a_1(n)a_i(\omega)(n)|$$

Hence

$$\mathbb{E}\left(\frac{|\hat{a}_2(n)|^\epsilon}{|a_1(n)|^\epsilon}\right) = \mathbb{E}\left[\frac{||\bigwedge^2 S_n||}{||S_n||^\epsilon}\right] = \mathbb{E}\left[\frac{||\bigwedge^2 \hat{A}_n||}{||A_n||^\epsilon}\right] \leq (C_1C_3/C_2)^\epsilon \sum_{i=2}^d \mathbb{E}\left(\frac{|\hat{a}_1(n)|^\epsilon}{|a_1(n)|^\epsilon}\right)$$

By (37), this is less or equal than constant $(1 - \gamma\epsilon)^n$. Since $|\hat{a}_2(g)| \geq |a_i(g)|$ for $i > 2$ and every $g \in SL_d(k)$, the proof is complete.
4.4.2 Exponential convergence and asymptotic independence in KAK

We recall that the norm on $V$ we are working with is $(\rho,A,K)$-good (it is the one given by Theorem 4.22). We recall also that the direct sum $V = \oplus \chi V_\chi$ is good. When $k$ is archimedean, this norm is induced by a scalar product so that we can choose an orthonormal basis in each $V_\chi$. Let $(e_1,\ldots,e_d)$ be the corresponding basis of $V$, $e_1$ is in particular a highest weight vector. Then, the norm on $V$ becomes $\|x\|^2 = \sum_{i=1}^d |x_i|^2$, $x = \sum_{i=1}^d x_i e_i \in V$. When $k$ is non archimedean, one can choose a basis in each $V_\chi$ such that the norm induced becomes the Max norm. If $(e_1,\ldots,e_d)$ is the corresponding basis of $V$, then $\|x\| = \text{Max}(\|x_i\|; i = 1,\ldots,d)$ for every $x = \sum_{i=1}^d x_i e_i \in V$.

Let $\rho^* : G \to GL(V^*)$ be the contragredient representation of $G$ on $V^*$, that is $\rho^*(g)(f) = f(\rho(g^{-1})x)$ for every $g \in G$, $f \in V^*$, $x \in V$. For $g \in G$ and $f \in V^*$, $g,f$ will simply refer to $\rho^*(g)(f)$. Consider the norm operator on $V^*$, it is easy to see that it is $(\rho^*,A,K)$-good. As explained in the preliminaries, $\|\cdot\|$ induces a distance $\delta(\cdot,\cdot)$ on the projective space $P(V)$. The same holds for $P(V^*)$.

Finally we recall the following notations: $M_n = X_1\ldots X_n$, $S_n = X_1\ldots X_n$ where $X_i; i \geq 1$ are independent random variables of law $\mu$. The KAK decomposition of $S_n$ in $G$ is denoted by $S_n = K_n A_n U_n$, with $K_n, U_n \in K$ and $A_n \in A^+$ (we have fixed a privileged way to construct the Cartan decomposition). We write $\rho(A_n) = \text{diag}(a_1(n),\ldots,a_d(n))$ in the basis of weights. When it comes to the random walk $\{M_n; n \in \mathbb{N}\}$ we simply write $M_n = k(M_n)a(M_n)u(M_n)$ its KAK decomposition.

Theorem 4.33 (Exponential convergence in KAK). Suppose that $\mu$ has an exponential local moment and that $\rho(\Gamma_\mu)$ is contracting. Denote by $x_\mu$ a highest weight vector ($e_1$ for example), then for all $\epsilon > 0$:

$$\limsup_{n \to \infty} \left[ \mathbb{E}(\delta'(k(M_n)|x_\mu|, Z_1)) \right]^{1/\epsilon} < 1 ; \limsup_{n \to \infty} \left[ \mathbb{E}(\delta'(U_n^{-1}e_1,|x_\mu|, Z_2)) \right]^{1/\epsilon} < 1$$

where $Z_1$ (resp. $Z_2$) is a random variable on $P(V)$ (resp. $P(V^*)$) with law $\nu$ (resp. $\nu^*$) -the unique $\mu$ (resp. $\mu^{-1}$) -invariant probability measure.

Remark 4.34. From the previous theorem, we deduce by applying the Borel Cantelli lemma that $k(M_n)|x_\mu|$ converges almost surely while $k(S_n)|x_\mu| = k(S_n)|x_\mu|$ converges only in law. This can also be directly derived from Corollary 4.7.

Proof. For simplicity, we write $S_n, K_n, A_n, U_n$ instead of $\rho(S_n), \rho(A_n), \rho(U_n)$. By the canonical identification between $V$ and $(V^*)^*$, $(e_1)^*$ will refer to $e_1$. Let $Z \in P(V^*)$ be the almost sure limit of $S_n^{-1}[f]$, for every $[f] \in P(V^*)$, obtained by Theorem 4.16. Since for every $i = 1,\ldots,d$, $A_n^{-1} e_i^* = a_i(n)e_i^*$ and $S_n = K_n A_n U_n$, we have for every $f \in V^*$ of norm one, such that $e_1(K_n^{-1}f) \neq 0$:

$$S_n^{-1}f = e_1(K_n^{-1}f) a_1(n) U_n^{-1}e_1 + \sum_{i=2}^d O(a_i(n))$$

$$U_n^{-1}e_1^* = \frac{1}{e_1(K_n^{-1}f)} S_n^{-1}f a_1(n) + \frac{1}{e_1(K_n^{-1}f)} \sum_{i=2}^d O(a_i(n) a_1(n))$$

Recall that $\delta([x],[y]) = \frac{|x \wedge y|}{||x|| ||y||}$: $[x],[y] \in P(V^*)$. Hence

$$\delta(U_n^{-1}e_1^*, Z) \leq \frac{1}{|e_1(K_n^{-1}f)|} \left( \frac{|S_n^{-1}f|}{|a_1(n)|} \delta(S_n^{-1}f, Z) + \sum_{i=2}^d O(|a_i(n)| a_1(n)) \right)$$

Since $|a_1(n)| = |S_n|$ and $|f| = 1$, $|S_n^{-1}f| = \text{Sup}_{|x|=1} |f(S_n x)| \leq |a_1(n)|$. Hence

$$\delta(U_n^{-1}e_1^*, Z) \leq \frac{1}{|e_1(K_n^{-1}f)|} \left( \delta(S_n^{-1}f, Z) + \sum_{i=2}^d O(|a_i(n)| a_1(n)) \right)$$

(38)
Let \( C(k) = \frac{1}{\sqrt{d}} \) (resp. \( C(k) = 1 \)) when \( k \) is archimedean (resp. non archimedean). The choice of the norm on \( V \) implies that a.s. there exists \( i = i(n, \omega) \in \{1, \ldots, d\} \), such that \( |e_i(K_n^{-1}.e_i^*)| \geq C(k) \)
Indeed, in the non archimedean case, \( 1 = ||K_n.e_i|| = \text{Max}(|K_n.e_i(e_i^*)|; i = 1, \ldots, d) \). Hence for some random \( i = i(n, \omega) \), \( |e_i(K_n^{-1}.e_i^*)| = |K_n.e_i(e_i^*)| = 1 \) and in the archimedean case, \( 1 = ||K_n.e_i|| = \sum_{i=1}^d |K_n.e_i(e_i^*)|^2 = \sum_{i=1}^d |e_i(K_n^{-1}.e_i^*)|^2 \). Hence one can write for every \( \epsilon > 0 \):

\[
E(\delta'(U_n^{-1}.[e_i^*], Z)) \leq \frac{1}{C(k)} \sum_{i=1}^d E(\delta'(S_n^{-1}.[e_i^*], Z) + \frac{1}{C(k)} \sum_{i=2}^d E(|a_i(n)|) \epsilon)
\]  

(39)

In (39), for every \( i = 1, \ldots, d \), on the event \( \{e_i(K_n^{-1}.e_i^*) \geq C(k)\} \), we apply (38) with \( f = e_i \). Since \( \epsilon > 0 \) can be taken smaller than one, \( C(k) \epsilon \geq C(k) \) and \( (x+y)^\epsilon \leq x^\epsilon + y^\epsilon \) for every \( x, y \in \mathbb{R}_+ \). We get then:

\[
E(\delta'(U_n^{-1}.[e_i^*], Z)) \leq \frac{1}{C(k)} \sum_{i=1}^d E(\delta'(S_n^{-1}.[e_i^*], Z)) + \frac{1}{C(k)} \sum_{i=2}^d E(|a_i(n)|) \epsilon
\]  

(40)

Theorem 4.31 shows that: \( E(|\phi(n)/a_1(n)|) \) is sub-exponential for \( i = 2, \ldots, d \).

Theorem 4.16 shows that for every \( i = 1, \ldots, d \), \( E(\delta'(S_n^{-1}.[e_i^*], Z)) \) is sub-exponential. In the same way, we show the exponential convergence of \( k(M_n)[x_p] \).

We have shown that \( U_n^{-1}.[x_p^*] \) converges a.s. and \( K_n[x_p] \) in law. In the following theorem, we show that these two variables become independent at infinity, with exponential “speed”. This is Theorem 1.5 from the introduction. We recall its statement.

**Theorem 4.35** (Asymptotic independence in the KAK decomposition). With the same assumptions as in Theorem 4.33, there exist independent random variables \( Z \in P(V^*) \) and \( T \in P(V) \) such that for every \( \epsilon > 0 \), every \( \epsilon \)-holder (real) function \( \phi \) on \( P(V^*) \times P(V) \) and all \( n \):

\[
|E(\phi(U_n^{-1}.[x_p^*], K_n[x_p])) - E(\phi(Z, T))| \leq ||\phi||_\epsilon \rho(\epsilon)^n
\]

where

\[
||\phi||_\epsilon = \text{sup}_{[x],[y],[x'],[y']} |\phi([x],[x']) - \phi([y],[y'])| \delta^\epsilon([x],[y]) + \delta^\epsilon([x'],[y'])
\]

**Proof.** Let \( \epsilon > 0 \). The analog of Theorem 4.33 for \( U_n^{-1}.[x_p^*] \) does not hold for \( K_n[x_p] \) because it converges only in law. However, we have the following nice estimate: for some \( \rho(\epsilon) \in [0,1] \) and all \( n \) large enough:

\[
E[\delta'(K_n[x_p], k(X_n ... X_{\lfloor \frac{n}{\Delta} \rfloor})[x_p])] \leq \rho(\epsilon)^n
\]  

(41)

Indeed, by independence \( (X_1, \ldots, X_n) \) has the same law as \( (X_n, \ldots, X_1) \) for every \( n \in \mathbb{N}^* \). Therefore, for every \( n \in \mathbb{N}^* \):

\[
E[\delta'(K_n[x_p], k(X_n ... X_{\lfloor \frac{n}{\Delta} \rfloor})[x_p])] = E[\delta'(k(M_n)[x_p], k(M_{n-\lfloor \frac{n}{\Delta} \rfloor+1})[x_p])]
\]

It suffices now to apply twice the first convergence of Theorem 4.33 and the triangle inequality.

Now let \( \phi \) be an \( \epsilon \)-holder function on \( P(V^*) \times P(V) \), \( (X_p')_{p \in \mathbb{N}} \) increments with law \( \mu \) independent from \( (X_n)_{n \in \mathbb{N}} \). We similarly write \( M_n = X_1 ... X_{n} \).

Let \( Z = \lim U_n^*[x_p] \) and \( T = \lim k(M_n)[x_p] \) (a.s. limits given by Theorem 4.33). The random variables \( T \) and \( Z \) are in particular independent. We write:

\[
E(\phi(U_n^{-1}.[x_p^*], K_n[x_p])) - E(\phi(Z, T)) = \Delta_1 + \Delta_2 + \Delta_3 + \Delta_4
\]

where

\[
\Delta_1 = E(\phi(U_n^{-1}.[x_p^*], K_n[x_p])) - E(\phi(U_{\lfloor \frac{n}{\Delta} \rfloor}^{-1}.[x_p^*], K_n[x_p]))
\]

(28)
\[\Delta_2 = \mathbb{E}\left(\varphi(U_{n-1}^{-1}\left[s_{r,\tilde{r}}, K_n[u,\rho]\right]) - \mathbb{E}\left(\varphi(U_{n}^{-1}\left[s_{r,\tilde{r}}, k(X_n\ldots X_{n-1}^{-1})[x,\rho]\right])\right)\right]\]

\[\Delta_3 = \mathbb{E}\left(\varphi(U_{n-1}^{-1}\left[s_{r,\tilde{r}}, k(M_n^{-1}\left|\tilde{r}\right.))\right][x,\rho]) - \mathbb{E}\left(\varphi(Z, k(M_n^{-1}\left|\tilde{r}\right.))\right]\right)\]

\[\Delta_1 = \mathbb{E}\left(\varphi(Z, k(M_n^{-1}\left|\tilde{r}\right.))\right) - \mathbb{E}\left(\varphi(Z, T)\right)\]

In \(\Delta_3\), we have replaced \(k(X_n\ldots X_{n-1}^{-1})\) with \(k(M_n^{-1}\left|\tilde{r}\right.))\) because, on the one hand they have the same law and on the other hand, the processes \(k(X_n\ldots X_{n-1}^{-1})\) and \(U_{n-1}^{-1}\) that appear in the last term of the right hand side of \(\Delta_2\) are independent.

- By Theorem 4.33, there exist \(\rho_1(\epsilon), \rho_2(\epsilon) \in [0, 1]\) such that: \(|\Delta_1| \leq ||\phi||, \rho_1(\epsilon)^n + ||\phi||, \rho_1(\epsilon)^{\frac{n}{2}}; |\Delta_3| \leq ||\phi||, \rho_1(\epsilon)^{\frac{n}{2}}\) and \(|\Delta_4| \leq ||\phi||, \rho_2(\epsilon)^{\frac{n}{2}}\).

- By (41), \(\Delta_2 \leq ||\phi||, \rho_3(\epsilon)^{n}\).

\[\square\]

4.5 Estimates in the Cartan decomposition - the non-connected case

Recall that \(k\) is a local field, \(G\) a \(k\)-algebraic group, \(G\) its \(k\)-points which we assume to be \(k\)-split. We denote by \(G^0\) its Zariski-connected component which we assume to be semi-simple and by \(G^0\) its \(k\)-points. Finally, \(\rho\) is a \(k\)-rational representation of \(G\) into some \(SL_d(k)\). We write \(V = k^d\) and \(P(V)\) the projective space.

In other terms, we consider the same situation as in Section 4.3 except that \(G\) is no longer assumed connected, a fortiori \(\rho(G)\). The KAK and KAN decompositions do not necessarily hold for the algebraic groups \(G, \rho(G)\) but are valid for \(G^0\) or \(\rho(G^0)\). However, one can still use the KAK decomposition of the ambient group \(SL(V)\).

We use then the notations and conventions of Section 3.2 regarding the Cartan decomposition in \(SL_d\). We consider the canonical basis \((e_1, \ldots, e_d)\) and canonical norm on \(V = k^d\) (see Section 4.2.1). For each \(g \in SL_d(k)\), we denote by \(g = k(g)u(g)\) an arbitrary but fixed Cartan decomposition in \(SL_d(k)\) and write \(a(g) = diag(a_1(g), \ldots, a_d(g))\). We consider a probability measure \(\mu\) on \(G\) such that \(\Gamma_{\mu}\) is Zariski dense in \(G\). As usual, we denote by \(S_n = X_n\ldots X_1\) the right random walk.

The aim of this section is to prove that the main results of Section 4.4 hold for the Cartan decomposition in \(SL_d(k)\) rather than merely in \(G\). Our first task will be to prove the following theorem, which is the analog of Theorem 4.31 for the KAK decomposition in \(SL_d(k)\).

**Theorem 4.36.** Assume that the representation \(\rho|_{G^0}\) is irreducible. Let \(\mu\) be a probability measure on \(G\) having an exponential local moment (see Definition 4.24) and such that \(\rho(\Gamma_{\mu})\) is contracting. Then for every \(\epsilon > 0\),

\[
\limsup_{n \to \infty} \left[ \mathbb{E}\left(\frac{a_2(\rho(S_n))}{a_1(\rho(S_n))}\right)^\epsilon \right]^{\frac{1}{\epsilon}} < 1
\]

Our next task will be to adapt the proof of Theorem 4.33 (exponential convergence in the KAK decomposition) and Theorem 4.35 (asymptotic independence in the KAK decomposition) to the Cartan decomposition of \(SL_d(k)\). This can be done easily using Theorem 4.36. Indeed it will be sufficient to replace \(x,\rho\), highest weight of \(\rho\) with \(e_1\) (which is the highest weight for the natural representation of \(SL_d(k)\) on \(k^d\)) and KAK in \(G\) with KAK in \(SL_d(k)\). By writing the Cartan decomposition of \(\rho(S_n)\) in \(SL_d(k)\) as \(\rho(S_n) = K_nA_nU_n\), we obtain:

**Theorem 4.37.** With the same assumptions as in Theorem 4.36, there exist random variables \(Z_1 \in P(V)\) and \(Z_2 \in P(V^*)\) such that

\[
\limsup_{n \to \infty} \left[ \mathbb{E}(\delta'(k(M_n)[e_1], Z_1)) \right]^{\frac{1}{2}} < 1 \quad \text{and} \quad \limsup_{n \to \infty} \left[ \mathbb{E}(\delta'(U_n^{-1}[e^*_1], Z_2)) \right]^{\frac{1}{2}} < 1
\]

29
We identify $\epsilon > 0$ is contracting. Then for every $\phi \in \mathcal{E}$ being sub-multiplicative, we have by independence:

**Definition 4.39.**
Let $\tau$.

**Corollary 4.41.**
Suppose that $\phi \in \mathcal{E}$.

**Theorem 4.38.**
With the same hypotheses as in Theorem 4.36, there exists independent random variables $Z \in P(V^*)$ and $T \in P(V)$, $\rho \in [0, 1]$, $n_0 > 0$ such that, for every $\epsilon > 0$, every $\epsilon$-holder (real) function $\phi$ on $P(V^*) \times P(V)$, every $n > n_0$ we have:

$$
|E(\phi(U_{n-1}.e_1^*), [K_n e_1|)] - E(\phi(Z, T))| \leq ||\phi||_p^n
$$

where

$$
||\phi||_p = \sup_{[x], [x'] \in \mathcal{E}} |\phi([x], [x']) - \phi([y], [y'])| / \delta^*(||x||_1, 2) + \delta^*(||x'||_1, 2)
$$

Before proving Theorem 4.36, we give some easy but important facts.

**Definition 4.39.**
Let $\tau = \inf \{n \in \mathbb{N}^*; S_n \in G^0\}$ i.e. the first time the random walk $(S_n)_{n \in \mathbb{N}}$ hits $G^0$. Recursively, for every $n \in \mathbb{N}$, $\tau(n + 1) = \inf \{k > \tau(n); S_k \in G^0\}$

For every $n \in \mathbb{N}^*$, $\tau(n)$ is a.s. finite. Indeed, by the Markov property it suffices to show that $\tau$ is almost surely finite: let $\pi$ be the projection $G \to G/\Gamma^0$, $\tau$ is then the first time the finite states Markov chain $\pi(S_n)$ -it is in fact a random walk because $G^0$ is normal in $G$ - returns to identity.

**Lemma 4.40.**
If $\mu$ is a probability measure on $G$ with an exponential local moment (see Definition 4.24), then the distribution $\eta$ of $S_\tau$ also has an exponential local moment.

**Proof.** We identify $G$ with a closed subgroup of $GL_r(k)$.

For every $\alpha > 0$:

$$
E(||S_\tau||^\alpha) = \sum_{k \in \mathbb{N}^*} E(||S_k||^\alpha; 1 = \tau = k) \leq \sum_{k \in \mathbb{N}^*} \sqrt{E(||S_k||^{2\alpha})} \sqrt{P(\tau = k)}
$$

(42)

where we used the Cauchy-Schwartz inequality on the right hand side. Since $\mu$ has an exponential moment, there exists $\alpha_0 > 0$ such that: $1 \leq E(||X_1||^{2\alpha_0}) = C < \infty$. Impose $\alpha < \alpha_0$. Since $x \mapsto x^{\alpha^\alpha}$ is convex, the Jensen inequality gives: $E(||X_1||^{2\alpha}) \leq E(||X_1||^{2\alpha_0})^{\alpha/\alpha_0} = C^{\alpha/\alpha_0}$. The norm being sub-multiplicative, we have by independence: $E(||S_k||^{2\alpha}) \leq \left(E(||X_1||^{2\alpha})\right)^k$ for every $k \in \mathbb{N}^*$.

Hence

$$
E(||S_k||^{2\alpha}) \leq (C^{\alpha/\alpha_0})^k ; \quad k \in \mathbb{N}^*
$$

(43)

On the other hand, recall that $\tau$ is the first time the finite states Markov chain $\pi(S_n)$ returns to identity. The Perron-Frobenius theorem implies that $\pi(S_n)$ becomes equidistributed exponentially fast so that $P(\tau > k)$ is exponentially decaying. In particular, there exists a constant $\lambda > 0$ such that

$$
P(\tau = k) \leq \exp(-\lambda k)
$$

(44)

Combining (42), (43) and (44) gives with $D = C^{\alpha/\alpha_0}$:

$$
E(||S_\tau||^\alpha) \leq \sum_{k \in \mathbb{N}^*} D^{\alpha \lambda k/2} \exp(-\lambda k/2)
$$

It suffices to choose $\alpha > 0$ small enough such that the latter sum is finite ($\alpha < \lambda / \log(D)$ works). □

**Corollary 4.41.**
Suppose that $\mu$ has an exponential local moment, $\rho|\Gamma^0$ is irreducible and $\rho(\Gamma_\mu)$ is contracting. Then for every $\epsilon > 0$,

$$
\limsup_{n \to \infty} \left[ E\left(\frac{a_2}{a_1} \left(\rho(S_{\tau(n)})\right)^{1/2}\right) \right]^{1/2} < 1
$$

30
Proof. The variables \( \{\tau(i + 1) - \tau(i); \ i \geq 1\} \) are independent and have the same law \( \tau = \tau(1) \). Hence, the process \( (S_{\tau(n)})_{n \in \mathbb{N}} \) has the same law as the usual right random walk on \( G^0 \) associated to the probability measure \( \eta \).

- First, we show that \( \Gamma_\eta \) is Zariski dense in \( G^0 \). We claim that \( \Gamma_\eta = \Gamma_\mu \cap G^0 \). Indeed, recall that \( \Gamma_\eta \) is the smallest closed semigroup (for the natural topology of \( \text{End}_d(k) \)) induced by that of \( k \) in \( G^0 \) containing the support of \( \eta \). Hence, \( M \in \Gamma_\eta \) if and only if for every neighborhood \( O \) of \( M \) in \( G^0 \), \( P(\exists n \in \mathbb{N}^*; S_{\tau(n)} \in O) > 0 \). On the other hand, \( G^0 \) is open in \( G \) because \( G/G^0 \) is finite. Thus, \( M \in \Gamma_\mu \cap G^0 \) if and only if for every neighborhood \( O \) of \( M \) in \( G^0 \), \( P(\exists n \in \mathbb{N}^*; S_{\tau(n)} \in O) > 0 \) or equivalently \( P(\exists n \in \mathbb{N}^*; S_{\tau(n)} \in O) = 1 \). This shows indeed that \( \Gamma_\eta = \Gamma_\mu \cap G^0 \).

Since \( \Gamma_\mu \) is Zariski-dense in \( G \) and \( G^0 \) is Zariski-open in \( G \), we deduce that \( \Gamma_\eta \) is Zariski dense in \( G^0 \).

- Next, we show that \( \rho(\Gamma_\eta) \) is contracting. Indeed, by Lemma 2.8, \( \rho(\Gamma_\mu) \) has a proximal element, say \( \rho(\gamma) \) with \( \gamma \in \Gamma_\mu \), then \( \rho(\gamma)^{|G/G^0|} = \rho(\gamma^{|G/G^0|}) \) is also proximal with \( \gamma^{|G/G^0|} \) in \( \Gamma_\mu \cap G^0 = \Gamma_\eta \). Hence \( \rho(\Gamma_\eta) \) is proximal whence, again by Lemma 2.8, contracting.

In consequence, we are in the following situation: \( G^0 \) is the group of \( k \)-points of a connected algebraic group and \( \eta \) is a probability measure on \( G^0 \) such that the semigroup \( \Gamma_\eta \) is Zariski dense in \( G^0 \). Moreover, by Lemma 4.40, \( \eta \) has an exponential local moment. Finally \( \rho\mid_{G^0} \) is an irreducible representation of \( G^0 \) such that \( \rho\mid_{G^0}(\Gamma_\eta) \) is contracting. An appeal to Corollary 4.32 ends the proof. \( \square \)

**Lemma 4.42.** Let \( \ell = \mathbb{E}(\tau) \).

(i) The Lyapunov exponent associated to the random walk \( \rho(S_{\tau(n)}) \) (or in other terms to the distribution \( \rho(\eta) \)) is \( \lambda_1 \), where \( \lambda_1 \) is the first Lyapunov exponent associated to \( \rho(S_n) \).

(ii) For every \( \epsilon > 0 \), there exist \( \rho(\epsilon) \in [0, 1] \), \( n(\epsilon) \in \mathbb{N}^* \) such that for \( n > n(\epsilon) \):

\[
P\left(\frac{1}{n} \tau(n) - \ell > \epsilon\right) \leq \rho(\epsilon)^n
\]

**Proof.** The stopping time \( \tau(n) \) is the sum of the independent, \( \tau \)-distributed random variables \( \{\tau(i + 1) - \tau(i); i \geq 1\} \). By the usual strong law of large numbers, a.s. \( \lim_{n \to \infty} \frac{\tau(n)}{n} = \ell \), so that, \( \frac{1}{n} \log ||S_{\tau(n)}|| = \frac{\log ||S_{\tau(n)}||}{\tau(n)} \times \frac{\tau(n)}{n} \) converges almost surely towards \( \lambda_1 \ell \). Item (ii) is an application of a classical large deviation inequality for i.i.d sequences: Lemma 4.43 below. To apply the latter, we should check that for some \( \xi > 0 \), \( \mathbb{E}(\exp(\xi \tau)) < \infty \). Indeed, by (44), there exists \( \xi > 0 \) such that for every \( y \in \mathbb{R}_+ \): \( P(\tau > y) \leq \exp(-\xi y) \). Hence, for every \( t > 0 \), write:

\[
\mathbb{E}(\exp(\epsilon \tau)) = \int_0^\infty \mathbb{P}(\exp(\epsilon \tau) > x) \, dx = 1 + \int_1^\infty \mathbb{P}\left(\tau > \frac{\log(x)}{\ell}\right) \, dx \leq 1 + \int_1^\infty \exp\left(-\frac{\xi \log(x)}{\ell}\right) \, dx
\]

The latter is finite as soon as \( \ell < \frac{1}{\xi} \). \( \square \)

The following lemma is classical in the theory of large deviations and is a particular case of the well-known Cramer Theorem. One can see [Str84], Lemma 3.4 Chapter 3 for example.

**Lemma 4.43** (Large deviations theorem for i.i.d. sequences). Let \( (X_n)_{n \in \mathbb{N}} \) be a sequence of independent, identically distributed random variables. If for some \( \xi > 0 \), \( \mathbb{E}(\exp(\xi |X_1|)) < \infty \), there exists a positive function \( \phi \) on \( \mathbb{R}_+^* \) such that for every \( \epsilon > 0 \):

\[
P\left(\frac{1}{n} \sum_{i=1}^n X_i - \mathbb{E}(X_1) \geq \epsilon\right) \leq \exp(-n\phi(\epsilon))
\]

Moreover, one can take \( \phi(\epsilon) = \sup_{0 < t < \xi} \{t(\epsilon - \psi(t))\} \) where \( \psi(t) = \log\left(\mathbb{E}(\exp(t(X_1 - \mathbb{E}(X_1))))\right) \).
Proof of Theorem 4.36: To simplify notations we omit ρ, so that G in seen as a subgroup of $SL_d(k)$. Let $N \in \mathbb{N}^+$, $\epsilon > 0$, $0 < \epsilon' < l$ to be chosen in terms of $\epsilon$. By definition of the KAK decomposition in $SL_d(k)$, what we want to prove is that for all $\epsilon > 0$ small enough

$$
\limsup_{N \to \infty} \mathbb{E} \left[ \left( \frac{||A^2 S_N||}{||S_N||^2} \right)^\epsilon \right] < 1
$$

Let $n = \lfloor \frac{N}{2} \rfloor$, so that for $N \geq N_1(\epsilon') = \frac{l(l+\epsilon')}{2}$, $n(l - \epsilon') \leq N \leq n(l + \epsilon')$. We wish to have $\tau(n)$ and $N$ in the same interval with high probability.

Let $A_n$ be the event "{\{\tau(n) \in [n(l - \epsilon'); n(l + \epsilon')]\}}". By Lemma 4.42, there exists $\rho(\epsilon') \in [0, 1]$ such that $\mathbb{P}(A_n) \geq 1 - \rho(\epsilon')^n$. We have then:

$$
\mathbb{E}\left[ \left( \frac{||A^2 S_N||}{||S_N||^2} \right)^\epsilon \right] \leq \mathbb{E}\left( \frac{||A^2 S_N||^\epsilon}{||S_N||^{2\epsilon}} \right) + \mathbb{P}(\Omega \setminus A_n) \leq \mathbb{E}\left( \frac{||A^2 S_N||^\epsilon}{||S_N||^{2\epsilon}} \right) + \rho(\epsilon')^n
$$

The first inequality is due to the fact that $\frac{||A^2 S_n||^\epsilon}{||S_n||^{2\epsilon}} \leq 1$. Since $n \geq N/(l + \epsilon') \geq N/2l$, $\rho(\epsilon')^n \leq \left( \rho(\epsilon')^{\frac{N}{l}} \right)^N$. Hence it suffices to estimate $(I)$.

$$(I) \leq \mathbb{E}\left( \frac{||A^2 S_N||^\epsilon}{||S_N||^{2\epsilon}} I_{N \geq \tau(n); A_n} \right) + \mathbb{E}\left( \frac{||A^2 S_N||^\epsilon}{||S_N||^{2\epsilon}} I_{N < \tau(n); A_n} \right)
$$

$(III)$ is treated similarly as $(II)$. Since $||A^2 g|| \leq ||g||^2$, $\frac{1}{||g||} \leq ||g^{-1}||$, $||g^{-1}|| \leq ||g||^{d-1}$ for every $g \in SL_d(k)$, we have:

$$(II) \leq \mathbb{E}\left( \frac{||X_N|| \ldots ||X_{\tau(n)+1}||^{2d\epsilon}}{||S_{\tau(n)}||^{2\epsilon}} \right)$$

$$\sum_{k=0}^\infty \mathbb{E}\left( ||X_N|| \ldots ||X_{k+1}||^{4d\epsilon} \right) I_{N \geq \tau(n)} I_{\tau(n)=k} \mathbb{E}\left( \frac{||A^2 S_{\tau(n)}||^{2\epsilon}}{||S_{\tau(n)}||^{4\epsilon}} \right)
$$

The bound (45) is obtained by the Cauchy-Schwartz inequality, (46) follows from the fact that on the event $A_n$, $\tau(n) \in [n(l - \epsilon'); n(l + \epsilon')]$. Finally (47) is due to the sub-multiplicativity of the norm and the independence of $X_N, \ldots, X_{k+1}$.

Since $\mu$ has an exponential local moment, for $\epsilon$ small enough, $1 \leq \mathbb{E} \left( ||X_1||^{4d\epsilon} \right) = C(\epsilon) < \infty$. Moreover, $n(l - \epsilon') < N < n(l + \epsilon')$, hence $\sum_{k=n(l-\epsilon')}^{n(l+\epsilon')} \mathbb{E} \left( ||X_1||^{4d\epsilon} \right) \leq 2n\epsilon'C(\epsilon)^{2n\epsilon'} \leq C(\epsilon)^{3n\epsilon'}$, for $n \geq n(\epsilon')$ large enough. Hence,

$$(II)^2 \leq C(\epsilon)^{3n\epsilon'} \mathbb{E}\left( \frac{||A^2 S_{\tau(n)}||^{2\epsilon}}{||S_{\tau(n)}||^{4\epsilon}} \right)
$$
Finally, by Corollary 4.41, there exists \( \rho(\epsilon) \in ]0,1[ \) such that for all \( n \) large enough:

\[
\mathbb{E} \left( \frac{\left\| A^2 \tau_{r(n)} \right\|^2}{\left\| \tau_{r(n)} \right\|^4} \right) = \mathbb{E} \left( \frac{a_2(\rho(S_{r(n)}))}{a_1(\rho(S_{r(n)}))} \right)^2 \leq \rho(\epsilon)^n
\]

Choose \( 0 < \epsilon' < \frac{-\log(\rho(\epsilon))}{3 \log(C(\epsilon))} \) so that for \( \rho = C(\epsilon)^{\epsilon'}\rho(\epsilon) \in ]0,1[ \), \((II)^2 \leq \rho^n \leq \left( \rho^{\epsilon'} \right)^N\).

\[\square\]

5 Proof of Theorem 2.11

In this section, we complete the proof of Theorem 2.11 and Corollary 1.2.

Now let \( \mu \) be a probability measure on \( SL_d(k) \) such that \( \Gamma_\mu \) is a strongly irreducible and contracting closed subgroup. We denote by \( G \) the \( k \)-Zariski closure of \( \Gamma_\mu \) in \( SL_d(k) \), which we assume to be \( k \)-split and its Zariski-connected component semi-simple. We can apply the results of the previous Section 4.5 with this \( G \) and \( \rho \) the natural action of \( G \) on \( V = k^d \). We use the same notation and conventions as in Section 3, regarding attracting points and repelling hyperplanes.

We will show that

\[
\limsup_{n \to \infty} \frac{1}{n} \log \mathbb{P} (\langle S_n, S_n' \rangle \text{ do not form a ping-pong pair} < 0.
\]

Applying Lemma 3.1, this will end the proof of Theorem 2.11. It will follow from the following two propositions.

**Proposition 5.1.** There exists \( \epsilon \in ]0,1[ \) such that for every \( r \in ]\epsilon,1[ \):

\[
\limsup_{n \to \infty} \frac{1}{n} \log \mathbb{P} (S_n, S_n' \text{ are not } (\epsilon^n, r^n)\text{- very proximal}) < 0
\]

**Proposition 5.2.** For every \( t \in ]0,1[ \):

\[
\limsup_{n \to \infty} \frac{1}{n} \log \mathbb{P} (\delta(v_{S_n \pm 1}, H_{S_n \pm 1}) \leq t^n) < 0
\]

**Proof of Proposition 5.1:** it will follow from Proposition 5.3 and Lemma 5.4. First, we recall Lemma 3.2 which says that a large ratio between the first two diagonal components in the \( KAK \) decomposition implies contraction. More precisely, let \( \epsilon > 0 \). If \( \frac{a_2(g)}{a_1(g)} \leq \epsilon^2 \), then \([g] \) is \( \epsilon \)-contracting. Moreover, one can take \( v_g = [k(g)e_1] \) to be the attracting point and \( H_g \), the projective hyperplane spanned by \( u^{-1}(g)e_i \) for \( i = 2,...,d \), to be the repelling hyperplane.

We deduce the following proposition:

**Proposition 5.3.** There exists \( \epsilon_0 \in ]0,1[ \) such that for every \( \epsilon \in ]\epsilon_0,1[ \),

\[
\limsup_{n \to \infty} \frac{1}{n} \log \mathbb{P} (S_n \text{ and } S_n' \text{ are not } \epsilon^n\text{- very contracting}) < 0
\]

**Proof.** It suffices to consider \( S_n, S_n' \) and \( S_n^{-1}, S_n^{-1} \) separately and show the corollary without the word “very”.

\* For the random walk \( (S_n) \) Theorem 4.36 shows that there exists \( \epsilon_1 \in ]0,1[ \) such that for all large \( n \) we have \( \mathbb{E} \left( \frac{a_2(n)}{a_1(n)} \right) \leq \epsilon_1^t \).
By the Markov inequality, for every $\epsilon \in [\epsilon_1, 1]$,
$$
\mathbb{P}\left( \frac{a_2(n)}{a_1(n)} \geq \epsilon^n \right) \leq \left( \frac{\epsilon_1}{\epsilon} \right)^n
$$

By Lemma 3.2, for every $\epsilon \in [\sqrt{\epsilon_1}, 1]$ we have $\mathbb{P}(S_n)$ is not $\epsilon^n$-contracting) $\leq \left( \frac{\epsilon_1}{\epsilon} \right)^n$.

- For the random walk $(S_{n-1})$: The assumption $\Gamma_n$ is a group implies that $\Gamma_{n-1} = \Gamma_n$ so that the action of $\Gamma_{n-1}$ on $V$ is strongly irreducible and contracting. In consequence, we can apply the same reasoning as the previous paragraph by replacing $\mu$ with $\mu^{-1}$. This gives $\epsilon_2 \in [0, 1]$ such that for every $\epsilon \in [\sqrt{\epsilon_1}, 1]$, $\mathbb{P}(S_{n-1})$ is not $\epsilon^n$-contracting) is sub-exponential.

Similarly if we denote by $\epsilon_3$, $\epsilon_4$ the quantities relative to $S'_n$ and $S'_{n-1}$, then it suffices to choose $\epsilon_0 = \max\{\sqrt{\epsilon_i}; i = 1, ..., 4\}$

Recall that for $g \in SL_d(k)$, $v_g = k(g)e_1$ and $H_g = \{Span(u(g)^{-1}e_2, ..., u(g)^{-1}e_d)\}$.

**Lemma 5.4. For every $t \in [0, 1]$,**
$$
\limsup_{n \to \infty} \frac{1}{n} \log \mathbb{P}(v_{S_n}, H_{S_n}) \leq t^n < 0
$$
The same holds for $S_{n-1}$, $S'_n$ and $S'_{n-1}$.

**Proof.** Consider the random walk $(S_n)_{n \in \mathbb{N}}$. Let $t \in [0, 1]$. Recall that if $H = Ker f, f \in V^*$ then for any non zero vector $x$ of $V$, $\delta([x],[H]) = \frac{|f(x)|}{||x|| ||H||}$. Since $H_{S_n} = Ker(U_n^{-1}e_1)$, we must show that for every $t \in [0, 1]$,
$$
\limsup_{n \to \infty} \frac{1}{n} \log \mathbb{P}(||U_n^{-1}e_1(K_ne_1)|| \leq t^n) < 0
$$

- For every $\epsilon > 0$, let $\psi_\epsilon$ be the function defined on $\mathbb{R}$ by $\psi_\epsilon(x) = 1$ on $[-\epsilon, \epsilon]$; affine on $[-2\epsilon; -\epsilon] \cup [\epsilon, 2\epsilon]$ and zero otherwise, for every $x \in \mathbb{R}$.

One can easily verify that $\psi_\epsilon$ is $\frac{1}{\epsilon}$-Lipschitz.

Note also that
$$
1_{[-\epsilon, \epsilon]} \leq \psi_\epsilon \leq 1_{[-2\epsilon, 2\epsilon]}
$$

- Let $\eta$ be the function on $P(V) \times P(V^*)$ defined by $\eta([x],[f]) = \delta([x],[f]), Ker(f)) = \frac{|f(x)|}{||x|| ||f||}$ for every $[x],[f] \in P(V)$.

We consider the following metric on $P(V) \times P(V^*)$: $d((x, [f]), ([y],[g])) = \delta([x],[y]) + \delta([f],[g])$ for every $x, y \in V, f, g \in V^*$. Let $C(k) = \sqrt{2}$ when $k$ is archimedean and $C(k) = 1$ when $k$ is non archimedean. We claim that $\eta$ is $C(k)$-Lipschitz. Indeed, let $[x],[y] \in P(V), [f],[g] \in P(V^*)$. By Lemma 5.5 below there exist $C(k)$-Lipschitz functions $\phi$ on $P(V) \times P(V^*)$ such that for every $x, y \in V, f, g \in V^*$ in the unit sphere such that $||x - y|| \leq C(k) \delta([x],[y])$ and $||f - g|| \leq C(k) \delta([f],[g])$. By the triangle inequality, $\eta([x],[f]) - \eta([y],[g]) \leq |||f(x) - g(y)||| \leq |||f - g||| + ||x - y|| \leq C(k) \delta([f],[g]) + \delta(x, [g])$.

Define for $\epsilon > 0, \phi_\epsilon = \psi_\epsilon \circ \eta$. By the previous remarks, $\phi_\epsilon$ is $\frac{C(k)}{\epsilon}$-Lipschitz.

**Theorem 4.38** gives a $\rho \in [0, 1]$ and independent random variables $Z \in V$ and $T \in V^*$ such that for every Lipschitz function $\phi$ on $P(V) \times P(V^*)$, and $n$ large enough
$$
||\mathbb{E}(\phi(K_ne_1, [U_n^{-1}e_1])) - \mathbb{E}(\phi(Z, T))|| \leq ||\phi|| \rho^n
$$

where $||\phi||$ is the Lipschitz constant of $\phi$ as it was defined in Theorem 4.38.

Now we prove (49). For any $t \in [0, 1]$
$$
\mathbb{P}(||U_n^{-1}e_1(K_ne_1)|| \leq t^n) \leq \mathbb{E}(\phi_\epsilon([K_ne_1],[U_n^{-1}e_1]))
$$

$$
\leq \mathbb{E}(\phi_\epsilon(Z,T)) + ||\phi_\epsilon|| \rho^n
$$

$$
\leq \mathbb{P}(||T|| ||Z|| \leq 2t^n) + C(k) \rho^n t^n
$$

$$
\leq \mathbb{E}(\phi_\epsilon([K_ne_1],[U_n^{-1}e_1]))
$$

$$
\leq Sup(\mathbb{E}(\phi_\epsilon([Z],[H])) \leq C(k) \rho^n)
$$

34
The bound (53) follows from (51), while (52) and (54) use (50). Finally to get (55) we used the independence of \( Z \) and \( T \).

By Theorem 4.18, (55) is sub-exponential and the lemma is proved if \( t > \rho \), a fortiori for every \( t \in ]0,1[ \). \( \Gamma_\mu \) being a group, the action of \( \Gamma_\mu \) on \( V \) is strongly irreducible and contracting, hence the same proof as above holds for \( S_{n}^{-1} \). The roles of \( S_{n} \) and \( S_{n}' \) are interchangeable.

\[ \text{Lemma 5.5.} \quad \text{Let } C(k) = \sqrt{2} \text{ when } k \text{ is archimedean and } C(k) = 1 \text{ when } k \text{ is not. Then for any } [x], [y] \in P(V), \text{ there exist representatives in the unit sphere such that} \]

\[ \delta([x], [y]) \leq ||x - y|| \leq C(k)\delta([x], [y]) \]

(In particular, in the non archimedean case these are equalities). The same holds for \( V^* \).

\[ \text{Proof.} \quad \text{Let } x \text{ and } y \text{ be representatives of norm one of } [x] \text{ and } [y]. \text{ When } k = \mathbb{C}, \text{ denote by } < \ldots > \text{ the canonical scalar product on } k^d. \text{ Then } \delta([x], [y])^2 = 1 - |< x, y >|^2 = (1 - Re(< x, y >))(1 + Re(< x, y >)). \]

One can choose \( x \) and \( y \) in such a way that \( < x, y > \in \mathbb{R} \) and \( Re(< x, y >) \geq 0 \). The identity \( ||x - y||^2 = 2(1 - Re(< x, y >)) \) ends the proof. The case \( k = \mathbb{R} \) is similar.

When \( k \) is non archimedean, recall that by definition: \( \delta([x], [y]) = \text{Max}\{|< x, y_j - x_j y_i >; i \neq j \} \). The norm being ultrametric, for any \( i, j, |x_j y_j - x_j y_i| = |y_j (x_i - y_i) + y_i (y_j - x_j)| \leq ||x - y||. \) Hence \( \delta([x], [y]) \leq ||x - y||. \) For the other inequality, we distinguish two cases:

\begin{itemize}
  \item Suppose that there is an index \( m \) such that \( x_m \) and \( y_m \) are of norm one (i.e. in \( \Omega_k^* \)). By rescaling if necessary \( x \) and \( y \), one can suppose that \( x_m = y_m = 1 \). Without loss of generality we can assume that \( m = 1 \). Hence, \( \delta([x], [y]) \geq \text{Max}\{|x_i - y_i; \ i \geq 2\} = ||x - y||. \)
  \item Suppose that there is no index \( m \) such that \( x_m \) and \( y_m \) are of norm one. Let \( \imath_0 \) (resp. \( \imath_0 \)) be an index such that \( x_{\imath_0} \) (resp. \( y_{\imath_0} \)) is invertible: such indices exist because \( x \) and \( y \) are on the unit sphere. \( \imath_0 \neq \imath_0 \) and neither \( x_{\imath_0} \) nor \( y_{\imath_0} \) is of norm one. Hence, \( |x_{\imath_0} y_{\imath_0} - y_{\imath_0} x_{\imath_0}| = 1 \) and \( \delta([x], [y]) = 1 = ||x - y||. \)
\end{itemize}

\[ \square \]

**Proof of Proposition 5.2:**

Let \( t > 0 \). On the one hand for every given \( n \) \( S_n \) and \( M_n \) have the same law and on the other hand \( (X_1, ..., X_n) \) and \( (X'_1, ..., X'_n) \) are independent, hence

\[ \mathbb{P}\left( \delta(v_{S_n}, H_{S_n}^{-1}) \leq t^n \right) = \mathbb{P}\left( \delta \left( k(M_n)[e_1], H_{S_n}^{-1} \right) \leq t^n \right) \]

\[ \leq \text{Sup}\{\mathbb{P}(\delta(k(M_n)[e_1], H) \leq t^n) ; H \text{ hyperplane of } V\} \]

By Theorem 4.37 and the Markov inequality, there exist \( \rho_1, \rho_2 \in ]0,1[ \), a random variable \( Z \) in \( P(V) \) such that:

\[ \mathbb{P}(\delta(k(M_n)[e_1], Z) \geq \rho_1) \leq \rho_2^n \]

(57), (58) and the triangle inequality give:

\[ \mathbb{P}(\delta([v_{S_n}], [H_{S_n}]) \leq t^n) \leq \text{Sup}\{\mathbb{P}(\delta(Z,[H]) \leq t^n + \rho_1^n) ; H \text{ hyperplane of } V\} + \rho_2^n \]

Theorem 4.18 shows that the latter is exponentially small. We may of course exchange the roles of \( S_n \) and \( S_n' \). When we consider \( S_{n}^{-1} \) instead of \( S_n \) the same estimates hold. Indeed, as explained in the proof of Proposition 5.3, \( \Gamma_{\mu^{-1}} \) acts strongly irreducibly on \( V \) and contains a contracting sequence.

\[ \square \]

**Proof of Corollary 1.2:** let \( l \in \mathbb{N}^* \) and \( (M_{n,l})_{n \in \mathbb{N}^*}, ..., (M_{n,l})_{n \in \mathbb{N}^*}, ..., (M_{n,l})_{n \in \mathbb{N}^*} \) be \( l \) independent random walks associated to \( \mu \). Propositions 5.1 and 5.2 give \( \epsilon, r, \rho \in ]0,1[ \), \( n_0 \in \mathbb{N}^* \) such that for every \( n > n_0 \) and \( i, j \in \{1, ..., l\} \), \( \mathbb{P}(A_{n,i,j}) \leq \rho^n \) and \( \mathbb{P}(B_{n,i,j}) \leq \rho^n \), where \( A_{n,i,j} \) is the event “\( M_{n,i} \) and \( M_{n,j} \) are not \( (r^n, \epsilon^n)\)-very proximal” and \( B_{n,i,j} \) is the union of the \( 4 \) events: the attracting point
of $M_{n,i}^{\pm 1}$ is at most $\epsilon^n$-apart from the repelling hyperplane of $M_{n,j}^{\pm 1}$. Hence for every $l \in \mathbb{N}^*$ and $n > n_0$:

$$\mathbb{P}(M_{n,1}, \ldots, M_{n,l} \text{ do not form a ping-pong } l\text{-tuple}) \leq \sum_{i<j} \mathbb{P}(A_{i,j}) + \mathbb{P}(B_{i,j}) \leq l(l-1)\rho^n$$

Fix $n > n_0$ and let $\rho' \in ]\rho, 1[,$ $l_n = \lfloor \frac{1}{\rho'} \rfloor$. The previous estimate shows that if $(M_{k,1})_{k \in \mathbb{N}^*}, \ldots, (M_{k,l_n})_{k \in \mathbb{N}^*}$ are $l_n$ independent and identically distributed random walks, then the probability $\mathbb{P}(M_{n,1}, \ldots, M_{n,l_n} \text{ do not form a ping-pong } l_n\text{-tuple})$ decreases exponentially fast.

\[ \square \]

References

[BG03] E. Breuillard and T. Gelander. On dense free subgroups of Lie groups. J. Algebra, 261(2):448–467, 2003.

[BG07] E. Breuillard and T. Gelander. A topological Tits alternative. Ann. of Math. (2), 166(2):427–474, 2007.

[BL85] P. Bougerol and J. Lacroix. Products of random matrices with applications to Schrödinger operators, volume 8 of Progress in Probability and Statistics. Birkhäuser Boston Inc., Boston, MA, 1985.

[Bou68] N. Bourbaki. Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines. Actualités Scientifiques et Industrielles, No. 1337. Hermann, Paris, 1968.

[Bre68] L. Breiman. Probability. Addison-Wesley Publishing Company, Reading, Mass., 1968.

[BT72] F. Bruhat and J. Tits. Groupes réductifs sur un corps local. Inst. Hautes Études Sci. Publ. Math., (41):5–251, 1972.

[BT84] F. Bruhat and J. Tits. Groupes réductifs sur un corps local. II. Schémas en groupes. Existence d’une donnée radicielle valuée. Inst. Hautes Études Sci. Publ. Math., (60):197–376, 1984.

[CR06] C. Curtis and I. Reiner. Representation theory of finite groups and associative algebras. AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1962 original.

[Dek82] F. M. Dekking. On transience and recurrence of generalized random walks. Z. Wahrsch. Verw. Gebiete, 61(4):459–465, 1982.

[Fur63] H. Furstenberg. Noncommuting random products. Trans. Amer. Math. Soc., 108:377–428, 1963.

[GM89] I. Ya. Goldsheid and G. A. Margulis. Lyapunov exponents of a product of random matrices. Russian Math. Surveys, 44(5):11–71, 1989.

[GR85] Y. Guivarc’h and A. Raugi. Frontière de Furstenberg, propriétés de contraction et théorèmes de convergence. Z. Wahrsch. Verw. Gebiete, 69(2):187–242, 1985.

[Gui89] F. Guimier. Simplicité du spectre de Liapounoff d’un produit de matrices aléatoires sur un corps ultramétrique. C. R. Acad. Sci. Paris Sér. I Math., 309(15):885–888, 1989.

[Gui90] Y. Guivarc’h. Produits de matrices aléatoires et applications aux propriétés géométriques des sous-groupes du groupe linéaire. Ergodic Theory Dynam. Systems, 10(3):483–512, 1990.
[Hum75] J.E. Humphreys. *Linear algebraic groups*. Springer-Verlag, New York, 1975. Graduate Texts in Mathematics, No. 21.

[Kin73] J. F. C. Kingman. Subadditive ergodic theory. *Ann. Probability*, 1:883–909, 1973.

[Kow08] E. Kowalski. *The large sieve and its applications*, volume 175 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2008. Arithmetic geometry, random walks and discrete groups.

[LP82] E. Le Page. Théorèmes limites pour les produits de matrices aléatoires. 928:258–303, 1982.

[Mac71] I. G. Macdonald. *Spherical functions on a group of p-adic type*. Ramanujan Institute, Centre for Advanced Study in Mathematics, University of Madras, Madras, 1971. Publications of the Ramanujan Institute, No. 2.

[Mos55] G. D. Mostow. Self-adjoint groups. *Ann. of Math. (2)*, 62:44–55, 1955.

[Mos73] G. D. Mostow. *Strong rigidity of locally symmetric spaces*. Princeton University Press, Princeton, N.J., 1973. Annals of Mathematics Studies, No. 78.

[MS81] G. A. Margulis and G. A. Soifer. Maximal subgroups of infinite index in finitely generated linear groups. *J. Algebra*, 69(1):1–23, 1981.

[PR94] V. Platonov and A. Rapinchuk. *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA, 1994.

[Qui02a] J.-F. Quint. Cônes limites des sous-groupes discrets des groupes réductifs sur un corps local. *Transform. Groups*, 7(3):247–266, 2002.

[Qui02b] J.F. Quint. Divergence exponentielle des sous-groupes discrets en rang supérieur. *Comment. Math. Helv.*, 77(3):563–608, 2002.

[Riv08] I. Rivin. Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms. *Duke Math. J.*, 142(2):353–379, 2008.

[Riv09] I. Rivin. Walks on graphs and lattices—effective bounds and applications. *Forum Math.*, 21(4):673–685, 2009.

[Str84] D. W. Stroock. *An introduction to the theory of large deviations*. Universitext. Springer-Verlag, New York, 1984.

[Tit71] J. Tits. Représentations linéaires irréductibles d’un groupe réductif sur un corps quelconque. *J. Reine Angew. Math.*, 247:196–220, 1971.

[Tit72] J. Tits. Free subgroups in linear groups. *J. Algebra*, 20:250–270, 1972.