N° d'ordre : 1234

THÈSE

Présentée pour obtenir

LE GRADE DE DOCTEUR EN SCIENCES
DE L'UNIVERSITÉ PARIS-SUD XI

Spécialité: Mathématiques

par

Richard AOUN

Application des marches aléatoires à l'étude des sous-groupes des groupes linéaires

Soutenue le 27 mai 2011 devant la Commission d'examen:

M.	Yves BENOIST	(Examinateur)
M.	Philippe BOUGEROL	(Rapporteur)
M.	Emmanuel BREUILLARD	(Directeur de thèse)
M.	Bertand DEROIN	(Examinateur)
M.	Yves GUIVARC'H	(Rapporteur)
M.	Gregory MARGULIS	(Examinateur)
M.	Marc PEIGNÉ	(Examinateur)

Thèse préparée au
Département de Mathématiques d'Orsay
Laboratoire de Mathématiques (UMR 8628), Bât. 425
Université Paris-Sud 11
91 405 Orsay CEDEX

Résumé

Dans cette thèse, nous utilisons et contribuons à la théorie des produits de matrices aléatoires afin d'étudier des propriétés génériques des éléments et des sous-groupes des groupes linéaires. Notre premier résultat donne une version probabiliste de l'alternative de Tits : nous montrons que si M_n et M'_n sont deux marches aléatoires indépendantes sur un groupe linéaire de type fini non virtuellement résoluble alors presque sûrement les deux marches finiront par engendrer un sous-groupe libre non abélien à deux générateurs. Cela répond par l'affirmative à une question de Guivarc'h [Gui90] et de Gilman, Miasnikov et Osin [GMO10]. Plus précisément, nous montrons que la probabilité que M_n et M'_n n'engendrent pas un sous-groupe libre décroit exponentiellement vite vers zéro. Notre outil principal est la théorie des produits de matrices aléatoires. Durant la preuve, nous établissons de nouveaux théorèmes limites dans cette théorie, d'une part en généralisant des résultats connus dans le cadre des produits de matrices à valeurs dans les corps archimédiens à tout corps local, d'autre part en donnant des résultats qui sont nouveaux même sur $\mathbb{R}$. Par exemple, nous montrons que sous des hypothèses naturelles sur la marche aléatoire, les composantes suivant K de M_n dans la décomposition KAK deviennent asymptotiquement indépendantes avec vitesse exponentielle. Dans la deuxième partie de la thèse, nous utilisons ces résultats pour étudier la transience des sous-variétés algébriques des groupes algébriques. Un de nos résultats peut être formulé comme suit : soit Γ un groupe non élémentaire de $SL_2(\mathbb{R})$, μ une probabilité adaptée sur Γ ayant un moment exponentiel, alors pour toute sous-variété algébrique propre $\mathcal{V}$ de $SL_2(\mathbb{R})$, la probabilité que la marche aléatoire appartienne à $\mathcal{V}$ décroit exponentiellement vite vers zéro. Par conséquent, la sous-variété algébrique $\mathcal{V}$ est transiente pour la marche aléatoire. Nous généralisons cet énoncé au cas où la marche aléatoire est adaptée sur un groupe Zariski dense des points réels d'un groupe algébrique défini et déployé sur $\mathbb{R}$. Ces résultats sont à comparer avec des travaux récents de Kowalski [Kow08] et de Rivin [Riv08], [Riv10].

Mots-clefs : Marches aléatoires, produits de matrices aléatoires, théorie des groupes, théorie des probabilités, alternative de Tits.

Application of random walks to the study of subgroups of linear groups

Abstract

In this thesis, we use and contribute to the theory of random matrix products in order to study generic properties of elements and subgroups of linear groups. Our first result gives a probabilistic version of the Tits alternative : we show that two independent random walks M_n and M'_n on a non virtually solvable finitely generated linear group will eventually generate a non abelian free subgroup. This answers a question of Guivarc'h [Gui90] and Gilman, Miasnikov and Osin [GMO10]. We show in fact that the probability that M_n and M'_n do not generate a free subgroup decreases exponentially fast to zero. Our methods rely deeply on random matrix products theory. During the proof we give some new limit theorems concerning this theory, some of them will be the generalization of known results for matrices taking value in archimedean fields to arbitrary local fields, others will be new even over $\mathbb{R}$. For example, we show that under natural assumptions on the random walk, the K-parts of M_n in the KAK decomposition become asymptotically independent with exponential speed. Next, we use these properties to study the transience of algebraic subvarieties in algebraic groups. One of our results can be formulated as follows: let Γ be a non elementary subgroup of $SL_2(\mathbb{R})$, μ a probability measure with an exponential moment whose support generates Γ, then for every proper algebraic subvariety $\mathcal{V}$ of $SL_2(\mathbb{R})$, the probability that the random walk lies in $\mathcal{V}$ decreases exponentially fast to zero. This shows that every proper algebraic subvariety is transient for the random walk. We generalize this result to the case where the support of the

probability measure generates a Zariski dense subgroup of the real points of an algebraic group defined and split over $\mathbb{R}$. These results share common flavor with recent works of Kowalski [Kow08] and Rivin [Riv08], [Riv10].

Keywords: random walks, random matrix product, group theory, probability theory, Tits alternative.

À mes parents,
Marie-Thérèse et Ghassan Aoun

Remerciements

Si cette thèse voit le jour, c'est grâce à plusieurs personnes que je tiens à remercier ici.

Tout d'abord, mon directeur de thèse Emmanuel Breuillard. Toute ma reconnaissance pour être toujours disponible, toujours prêt à m'écouter (souvent pendant des heures) et à m'aider quand ça bloque. Il m'a motivé en me posant de très jolis problèmes et questions mathématiques. Il était assez patient et compréhensif au début quand je n'avais pas de suffisantes connaissances mathématiques. Ses conseils, sa disponibilité, sa relecture minutieuse des textes que j'ai écrits ont fait que cette thèse ait pu arriver à son terme. J'admire sa façon de faire les mathématiques et j'espère que j'ai pu m'en inspirer un peu. L'avoir eu comme directeur de thèse est une des meilleures choses qui me soient arrivées.

Je remercie infiniment Philippe Bougerol et Yves Guivarc'h pour avoir accepté de rapporter la thèse. Yves a toujours été à mon écoute lors de mes missions à Rennes. Ses articles sont pour moi une grande source d'inspiration. Je le remercie chaleureusement pour ses conseils et son hospitalité. Sans le savoir, Philippe a contribué à ma thèse grâce à son excellent livre "Product of random matrices and application to Schrodinger operators". C'est grâce à ce livre que j'ai appris les fondements de la théorie des produits de matrices aléatoires.
J'exprime toute ma graditude pour les membres de Jury. J'ai eu l'occasion de discuter plusieurs fois avec Bertrand Deroin, je le remercie pour sa disponibilité. Marc Peigné m'a invité à parler à Tours, je le remercie chaleureusement. Yves Benoist a toujours répondu à mes questions sur les décompositions de Cartan, je le remercie pour son aide. Enfin, je suis honoré par la présence de Grégory Margulis dans mon Jury.

Avant d'arriver en thèse, j'ai fait mon M1 et M2 en France. La première année ne fut pas si facile, de nombreuses personnes m'ont aidé à la surmonter avec succès. A titre mathématique, je remercie Stéphane Fishler, Renée Elkik et Pierre Lorenzon pour leur soutien, encouragement en M1 et les très jolis cours d'algèbre. En M2 j'ai donné des TD à des étudiants de Supelec qui prennent des cours de L3 à Orsay, je remercie Renée Elkik et Dominique Hulin pour cette opportunité. Merci à Jean-François Le Gall, Elisabeth Gassiat, Mylène Maida, Pascal Massart, Thomas Duquesne pour les cours de M2 et les conseils d'orientation.

Pendant mes trois années de thèse, j'ai eu l'opportunité de faire des missions en France et à l'étranger. Je remercie l'école doctorale et surtout David Harari et Pierre Pansu pour cette occasion. Merci à Françoise Dalbo responsable du GDR Platon pour les belles conférences organisées et l'opportunité d'y participer. Durant ma thèse j'ai eu l'occasion de discuter avec des mathématiciens que je tiens à remercier : Anne Broise, Bertrand Deroin, Marc Peigné, Sara Brofferio, Yves Benoist. Je remercie Emile Le Page, Frédéric Mathéus, Frédérique Watbled pour leur chaleureux accueil à Vannes, Fernando Alcalde pour son accueil à Bilbao et Sylvie Ruette pour m'avoir invité à parler dans le séminaire de théorie ergodique à Orsay. Merci à mes profs au Liban : Charbel Klayani, Georges Bou Abdo, Toni Sayah pour toutes les discussions fructueuses et votre accueil

au Liban.

Si l'ambiance dans les bâtiments 425 et 430 est si agréable, c'est en partie dû aux secrétaires Christine Bailleul, Fabienne Jacquemin, Martine Justin, Nathalie Carrière et Valérie Lavigne, que je remercie chaleureusement. Merci pour votre gentillesse et votre disponibilité. Merci à l'équipe informatique et surtout à Laurent Dang pour ta précieuse aide pour la page Web et pour nos discussions sur la vie en général.
L'ambiance conviviale entre les doctorants a joué aussi un rôle important. Miaofen Chen, merci pour ton aide en algèbre, ton sourire rassurant et ta grande amitié. Ta compagnie au bureau est ce qui me manquera le plus. Hatem Hajri, notre amitié depuis le M2 m'est assez importante, bonne chance mon ami. Nicolas de Saxcé, j'admire ta culture mathématique et non mathématique, merci pour toutes les jolies discussions. Ramla Abdellatif, merci pour toutes les agréables conversations et pour être toujours disponible quand j'avais besoin d'aide. Bernardo da Costa, merci pour ton aide en latex et pour toutes les belles discussions. Merci aussi à Aurélien Poiret et Dominique Bontemps. Je vous souhaite tous le succcès dans votre vie professionnelle et personnelle.

Une pensée à tous mes amis au foyer franco-libanais et à mes amis au Liban, plus spécialement à Charbel, Carine, Richard, Giovanni, Sylvana, Youssef, Layal, Sr Maya, Nancy, Wissam, Jad, Aimée, Pamela qui ont rendu mes séjours au Liban si agréable.

Le plus grand merci est à mes parents Marie-Thérèse et Ghassan. Si je suis là, c'est grâce à vous. Vous êtes le plus beau cadeau du ciel.
Une pensée aussi à toute ma famille : ma grand-mère, mes tantes et mes oncles.

Enfin, merci à toi Dieu car tu m'a manifesté ton grand amour.

Table des matières

Chapitre 1

Introduction

Cette thèse s'inscrit dans le cadre des applications de la théorie des produits de matrices aléatoires aux sous-groupes des groupes linéaires. Notre but est d'utiliser une approche probabiliste (les marches aléatoires) afin de comprendre le comportement des éléments génériques des groupes linéaires (i.e. des sous-groupes de $GL_n(K)$, K un corps). Les questions de généricité dans les groupes ont suscité plusieurs travaux de recherche : en théorie probabiliste des groupes finis, citons par exemple [ET65], [ET67a], [ET67b], [ET68], [ET70], [ET71], [Dix69], [Dia88], [Bab89], [LS96], [Sha99], [SC04] ; en théorie combinatoire des groupes [Gro93], [Gro03], [Cha95], [AO96], [Arz97], [Arz98], [KMSS03], [Żuk03]. Citons aussi les travaux récents de Kowalski [Kow08], Rivin [Riv08], [Riv09], [Riv10] et Gilman, Miasnikov et Osin [GMO10]. Outre l'intérêt de telles études en théorie des groupes, elles jouent un rôle important en cryptanalyse moderne (voir par exemple [AAG99] et [MU08]).

La thèse est structurée ainsi :

1. L'introduction présente la problématique et énonce les résultats importants de la thèse.
2. Le Chapitre 2 reprend pour l'essentiel l' article "Random subgroups of linear groups are free" [Aoua] accepté pour publication à Duke Mathematical Journal. Pour cette raison ce chapitre est rédigé en Anglais.
3. Le Chapitre 3 reprend pour l'essentiel un autre article "Transience of algebraic varieties in algebraic groups and application to generic Zariski density" [Aoub].
4. Le Chapitre 4 traite les produits de matrices aléatoires sur un groupe algébrique réductif défini sur un corps local.

Commençons par rappeler le cadre des marches aléatoires sur les groupes et par préciser dans quel sens une propriété donnée sera considérée comme générique.
Soit Γ un groupe discret, μ une probabilité sur Γ, $\{X_n; n \geq 1\}$ une suite de variables aléatoires de loi μ définies sur un espace probabilisé $(\Omega, \mathcal{F}, \mathbb{P})$ [1]. Pour tout $n \in \mathbb{N}^*$, nous définissons le $n^{\text{ème}}$ rang de la marche aléatoire par

1. Par exemple, nous pouvons prendre pour Ω l'ensemble des trajectoires, $\Omega = \Gamma^{\mathbb{N}}$, $\mathbb{P} = \mu^{\otimes \mathbb{N}}$ et $\mathcal{F}$ la tribu produit.

$$M_n = X_1 \cdots X_n$$

La loi de M_n est la $n^{\text{ème}}$ convolée μ^n de μ où $\mu^n = \mu^{n-1} \star \mu$ et $\nu \star \mu$ est la mesure image de la probabilité $\nu \otimes \mu$ par l'application $\Gamma \to \Gamma : (x, y) \mapsto xy$.
Si Γ est de type fini, nous pouvons considérer une partie génératrice finie symétrique S et une probabilité ayant S comme support, alors la marche aléatoire $\{M_n; n \geq 1\}$ n'est autre que la marche aléatoire sur le graphe de Cayley [2] de Γ.
Soit (P) une propriété sur Γ (par exemple $\Gamma = SL_3(\mathbb{Z})$, $\mathcal{V}$ une sous-variété algébrique propre de $SL_3(\mathbb{R})$ et (P) = "ne pas appartenir à $\mathcal{V}$"). Nous voulons voir si un élément au hasard dans Γ vérifie (P). Pour cela, nous étudions la probabilité

$$p_n = \mathbb{P}\left(M_n \text{ ne vérifie pas } (P)\right)$$

Une façon de voir que (P) est générique est de dire que p_n converge vers 0 quand n tend vers l'infini. Une assertion plus forte, du type p_n converge exponentiellement vite vers zéro, implique par le lemme de Borel-Cantelli que pour presque toute trajectoire $\{M_n; n \geq 1\}$, il existe un rang n_0 à partir duquel M_n verifie (P). C'est dans ce sens que nous dirons qu'un élément au hasard dans Γ vérifie (P).
Divers auteurs ont adopté ce point de vue et se sont intéressés à des questions semblables, en particulier Kowalski [Kow08] et Rivin [Riv08] qui démontrent entre autres qu'une matrice "au hasard" dans $SL_n(\mathbb{Z})$ a son polynôme caractéristique irréductible. Kowalski montre dans [Kow08] que la probabilité p_n décroit exponentiellement vite vers zéro et Rivin montre dans [Riv09] que la borne de décroissance exponentielle est effective. Les techniques utilisées par ces auteurs relèvent essentiellement du crible arithmétique et des arguments de marches aléatoires sur les groupes finis dont le trou spectral et la propriete τ (voir [ZL]) .

Dans cette thèse, le groupe Γ est linéaire, c'est-à-dire un sous-groupe de $GL_d(K)$ pour $d \geq 2$ et K est un corps quelconque. Ainsi, M_n n'est autre qu'un produit de matrices aléatoires définies sur K. Pour étudier les produits de matrices aléatoires sur un corps quelconque, on peut souvent se ramener à étudier les produits de matrices aléatoires sur un corps local [3]. Cette théorie débute dans les années 1960-1970 avec Furstenberg, Kesten [FK60], [Fur63] et est poursuivie dans les années 1970-1990 par l'école française : Bougerol, Guivarc'h, Le Page et Raugi [Gui80], [LP82], [BL85], [GR85], [GR86], [Bou86], [Bou87], [LP89], [Gui90], [Rau97], [Gui08] et russe [GM89], [GG96].
Elle étudie entre autres le comportement de M_n en norme, en direction, dans les décompositions de Cartan et d'Iwasawa. Ses applications sont diverses : à l'étude des opérateurs de Schrodinger [BL85], à l'étude des équations stochatisques [Kes73], [LP83], [Bou87],[dSGLP04], [Gui06], à la classification des mesures stationnaires sur les espaces homogènes [BQ09], à la démographie [Coh79], à l'étude des fractions continues [BAG01], en dynamique holomorphe [DD], aux graphes expanseurs [BG09], à l'étude des sous-groupes des groupes linéaires [Gui90].

Cette thèse fait partie de la dernière catégorie. Outre les résultats que nous obtenons concernant les questions de généricité dans les groupes linéaires, nous démontrons de

2. Le graphe de Cayley de Γ pour la partie génératrice S est le graphe ayant pour sommets les éléments de Γ et tel que $x \in \Gamma$ est relié à $y \in \Gamma$ si et seulement si $x^{-1}y \in S$.

3. $\mathbb{R}$, $\mathbb{C}$, une extension finie de $\mathbb{Q}_p$ ou le corps des séries formelles de Laurent sur un corps fini.

nouveaux théorèmes limites concernant la théorie des produits de matrices aléatoires.

Les questions de généricité qui nous intéresseront tout au long de la thèse sont les suivantes.

- Nous donnons dans le Chapitre 2 une version probabiliste de l'alternative de Tits. Soit K un corps, $d \geq 2$, Γ un sous-groupe de type fini de $GL_d(K)$ non virtuellement résoluble. Nous nous interesserons à un raffinement de l'aternative de Tits[Tit72], i.e. savoir si deux elements génériques de Γ engendrent un sous-groupe libre à deux générateurs.
  Pour cela nous considérons deux marches aléatoires indépendentes M_n et M'_n sur Γ, et nous intéressons à la décroissance exponentielle de la probabilité

$$\mathbb{P}(\langle M_n, M'_n \rangle \text{ non libre})$$

  De plus, est-ce que le sous-groupe $\langle M_n, M'_n \rangle$ est quasi-isométriquement (voir Définition 2.5.6) plongé dans Γ ?
- Dans le Chapitre 3, nous considérons un groupe Γ Zariski dense dans le groupe des points réels d'un groupe algébrique semi-simple $\mathbf{G}$ défini sur $\mathbb{R}$. Soit $\mathcal{V}$ une variété algébrique propre de $\mathbf{G}$. Intuitivement, on s'attend qu'un élément générique de Γ n'appartient pas à $\mathcal{V}$. A-t-on la décroissance exponentielle de la probabilité

$$\mathbb{P}(M_n \in \mathcal{V}) \quad ?$$

  Par Borel-Cantelli, si tel est le cas, alors $\mathcal{V}$ est transiente pour la marche aléatoire.
- Soient $\mathbf{G}$ comme dans le point précédent, Γ_1, Γ_2 deux sous-groupes Zariski denses dans le groupe G des points réels de $\mathbf{G}$. Nous nous intéresserons, toujours dans le Chapitre 3, à savoir si un élément générique de Γ_1 et un élément générique de Γ_2 engendrent un sous-groupe Zariski dense. Pour cela, cela nous considérons deux marches aléatoires M_n et M'_n respectivement sur Γ_1 et Γ_2 et nous estimons la probabilité

$$\mathbb{P}(\langle M_n, M'_n \rangle \text{ n'engendrent pas un sous-groupe Zariski dense})$$

Nous exposerons les résultats obtenus dans les Sections 1.1 et 1.2 de cette introduction en expliquant le lien qui existe entre les trois points précédents. Les preuves se trouvent dans les Chapitres 2 et 3. Les méthodes que nous utilisons sont totalement différentes de celles employées par Kowalski et Rivin (voir ci-dessus).

Citons brièvement les questions qui nous intéresseront concernant la théorie des produits de matrices aléatoires.

- En théorie des produits de matrices aléatoires, est toujours mis en contraste le comportement de M_n et de sa matrice transposée (dans la base canonique) M_n^t. Quand K est un corps local, alors sous des hypothèses naturelles sur la mesure de probabilité, nous montrons que M_n et M_n^t sont avec probabilité exponentiellement proche de 1 des éléments proximaux. Leurs points attractifs respectifs v_{M_n} et $v_{M_n{}^t}$ seront exprimés en termes de la décomposition de Cartan. Nous nous posons la question de savoir si v_{M_n} et $v_{M_n^t}$ sont asymptotiquement indépendants avec vitesse exponentielle et de voir aussi s'ils convergent à la même vitesse. Une telle

information permet d'obtenir une convergence exponentielle et une indépendance asymptotique des composantes suivant K dans la décomposition KAK de M_n.
– Les principaux théorèmes limites des produits de matrices aléatoires sont établis dans le cadre des corps archimédiens. Nous étudierons leur extension à tout corps local.

L'exposition de ces résultats est réservée à la Section 1.3 de cette introduction et les preuves aux Chapitres 2 (Section 2.4) et 4.

1.1 Une version probabiliste de l'alternative de Tits

Le premier résultat de cette thèse concerne une version probabiliste de l'alternative de Tits et répond par l'affirmative à une question de Guivarc'h [Gui90, §2.10] et de Gilman, Miasnikov, Osin [GMO10, Problem 7.2]. Rappelons tout d'abord, l'énoncé de la célèbre alternative de Tits :

Theorem 1.1.1. *[Tit72] Soit K un corps, $d \geq 2$, Γ un sous-groupe de type fini de $GL_d(K)$ non virtuellement résoluble*[4]*. Alors Γ contient un sous-groupe libre non abélien à deux générateurs.*

Question naturelle : deux éléments au hasard du groupe Γ engendrent-ils un sous-groupe libre ? Un des résultats que nous démontrerons au chapitre 2 est l'énoncé suivant :

Théorème 1.1.2. *(2.1.1) Soit K un corps, $d \geq 2$, Γ un sous-groupe de $GL_d(K)$ de type fini non virtuellement résoluble, S une partie génératrice finie symétrique de Γ*[5]*, μ une mesure de probabilité sur S, $\{M_n, n \in \mathbb{N}^*\}$ et $\{M'_n, n \in \mathbb{N}^*\}$ deux marches aléatoires indépendantes. Alors il existe $\rho \in]0,1[$ tel que pour tout n assez grand :*

$$\mathbb{P}(\langle M_n, M'_n \rangle \text{ libre et quasi-isométriquement plongé dans } \Gamma) \geq 1 - \rho^n$$

En particulier, presque sûrement, pour n assez grand, le groupe engendré par M_n et M'_n est libre non abélien et quasi-isométriquement plongé dans Γ.

1.1.1 Historique du problème, motivations et applications

Un théorème de Guivarc'h

Dans [Gui90], Guivarc'h a démontré le théorème suivant :

Théorème 1.1.3. *[Gui90, Théorème 3] Soit Γ un groupe linéaire de type fini non virtuellement résoluble, μ une probabilité supportée sur une partie génératrice finie symétrique, $\{M_n, n \in \mathbb{N}^*\}$ et $\{M'_n, n \in \mathbb{N}^*\}$ deux marches aléatoires indépendantes. Alors presque sûrement, il existe des sous-suites aléatoires d'entiers $\{n_k, k \in \mathbb{N}\}$, $\{n'_k, k \in \mathbb{N}\}$, des*

4. Γ est virtuellement résoluble s'il admet un sous-groupe d'indice fini qui soit résoluble
5. Cette condition peut être raffinée par : μ a un moment exponentiel et le plus petit semi-groupe contenant le support de μ est un groupe. Voir le Chapitre 2 pour les détails.

entiers p_k et p'_k non nuls tel que pour k assez grand, le groupe engendré par ${M_{n_k}}^{p_k}$ et ${M'_{n'_k}}^{p'_k}$ est libre

Ce théorème constitue déja une amélioration, et en fait une preuve probabiliste, de l'alternative de Tits. La preuve de Guivarc'h ne donne aucune indication sur les sous-suites aléatoires $\{n_k; k \in \mathbb{N}\}$ et $\{n'_k; k \in \mathbb{N}\}$ puisque leur existence est démontrée via le théorème de récurrence de Poincarré [Gui90, Lemme 2]. Dans le même article, Guivarc'h demande si les estimées fines des produits de matrices aléatoires ne suffisent pas à démontrer que presque sûrement, le groupe engendré par M_n et M'_n est libre pour n assez grand, c'est-à-dire si on peut se passer des sous-suites $\{n_k; k \in \mathbb{N}\}$ et $\{n'_k; k \in \mathbb{N}\}$ et des entiers p_k et p'_k. Le Théorème 1.1.2 répond par l'affirmative à cette question.

Les travaux de Gilman, Miasnikov, Osin et les applications en cryptanlyse moderne

Dans un travail récent [GMO10], Gilman, Miasnikov et Osin ont démontré un théorème analogue au Théorème 1.1.2 pour les groupes hyperboliques. Leur théorème peut être énoncé comme suit :

Théorème 1.1.4. *[GMO10, Théorème 2.1] Soit Γ un groupe hyperbolique non élémentaire*[6]*. Soit μ une mesure de probabilité supportée sur une partie génératrice finie symétrique et $\{M_n; n \geq 1\}$, $\{M'_n; n \geq 1\}$ deux marches aléatoires indépendentes. Alors il existe $\rho \in]0,1[$ tel que pour tout n assez grand :*

$$\mathbb{P}(\langle M_n, M'_n\rangle \text{ libre et quasi-isométriquement plongé dans } \Gamma) \geq 1 - \rho^n$$

On dit que le groupe Γ a la propriété FB (free basis : pour la liberté du sous-groupe $\langle M_n, M'_n\rangle$) et QI (le sous-groupe $\langle M_n, M'_n\rangle$ est quasi-isométriquement plongé) si ces propriétés ont lieu avec probabilité tendant vers 1 de façon exponentielle.

Dans [GMO10, Problem 7.2], les auteurs demandent si les propriétés FB et QI sont vérifiées pour le groupe $SL_d(\mathbb{Z})$, $d \geq 3$ qui n'est pas hyperbolique. Notre Théorème 1.1.2 répond par l'affirmative à cette question et étend les propriétés FB et QI à tout groupe linéaire non virtuellement résoluble.

D'après les articles [MU07] et [MU08], les propriétés FB et QI sont importantes en cryptanalyse moderne et peuvent être utilisées pour faire une attaque sur le cryptosystème AAG [AAG99].

Application en dynamique holomorphe

Des idées proches de celles développées dans le chapitre 2 ont été appliquées par Bertrand Deroin et Romain Dujardin dans [DD] pour introduire la notion de courant

6. Un groupe hyperbolique est dit élémentaire s'il contient un sous-groupe d'indice fini cyclique.

de bifurcation dans le cadre d'une famille holomorphe de représentations d'un groupe de type fini Γ de $PSL_2(\mathbb{C})$.

1.2 Transience des variétés algébriques

Dans la seconde partie de la thèse, nous nous intéressons à la transience des sous-variétés algébriques propres dans les groupes algébriques semi-simples. Dans cette section, nous travaillons dans le corps des nombres réels.
Soit $\mathbf{G}$ un groupe algébrique défini sur $\mathbb{R}$, G le groupe de ses points réels et Γ un sous-groupe Zariski dense de G. Considérons une mesure de probabilité μ adaptée[7] sur Γ et $\mathcal{V}$ une variété algébrique propre de $\mathbf{G}$.

Questions :
- Est-il vrai que la variété $\mathcal{V}$ est transiente pour la marche aléatoire $\{M_n; n \geq 1\}$ associée, c'est à dire que presque sûrement la marche aléatoire ne visite $\mathcal{V}$ qu'un nombre fini de fois ?
- La probabilité $\mathbb{P}(M_n \in \mathcal{V})$ décroit-elle exponentiellement vite vers zéro ?
- Si P est un polynôme non constant défini sur l'algèbre des fonctions polynomiales sur $\mathbf{G}$, peut-on estimer $|P(M_n)|$?

1.2.1 Motivations et historique

Première motivation : le Théorème de Kesten. Ce dernier implique que la probabilité de retour à l'identité dans Γ décroit exponentiellement vite. Il est donc naturel de se poser la question de la décroissance d'autres parties plus grandes du groupe. Dans le cas particulier des sous-groupes, une vaste littérature existe : par exemple [Bek90] et en particulier [DlHGCS99, Theorem 51] où est prouvé que la probabilité que la marche aléatoire sur Γ retourne à un sous-groupe H décroit exponentiellement vite si et seulement si le graphe de Scheirer de Γ/H est non moyennable. Dans cette thèse, nous nous intéresserons à la probabilité de retour dans les sous-variétés algébriques.

Deuxième motivation : les graphes expanseurs (voir par exemple [BG08], [BG09], [BG10], [Var]). Dans [BG10], les auteurs montrent qu'il existe une infinité de nombres premiers p de densité un, telle que la famille des graphes de Cayley de $SL_2(\mathbb{Z}/p\mathbb{Z})$ forme une famille d'expanseurs. Une étape cruciale de la preuve est de montrer que la probabilité de retour d'une marche aléatoire sur $SL_2(\mathbb{Z}/p\mathbb{Z})$ en un sous-groupe décroit exponentiellement vite et uniformément en les sous-groupes. De plus, dans [BG09, Corollary 1.1.], l'énoncé suivant est démontré : considérons le groupe $\Gamma = SL_d(\mathbb{Z})$ $(d \geq 2)$ et S une partie symétrique finie de Γ qui engendre un sous-groupe Zariski dense, μ la probabilité uniforme sur S, $\{M_n; n \geq 1\}$ la marche aléatoire associée, alors pour toute variété algébrique propre $\mathcal{V}$ de $SL_d(\mathbb{C})$, la probabilité $\mathbb{P}(M_n \in \mathcal{V})$ décroit exponentiellement vite vers zéro.
Il est donc intéressant de pouvoir généraliser de tels résultats à tout groupe Zariski dense

7. i.e. tel que le groupe engendré par le support de μ soit Γ

de $SL_d(\mathbb{R})$ et de pouvoir trouver une approche probabiliste évitant ainsi les réductions modulo p et les arguments de combinatoire additive qu'utilisent Bourgain et Gamburd.

Troisième motivation : raffiner le Théorème 1.1.2. Soit $\mathbf{G}$ un groupe algébrique semi-simple défini sur $\mathbb{R}$, G le groupe de ses points réels, Γ un groupe Zariski dense dans G, μ une probabilité adaptée sur Γ, $\{M_n; n \geq 1\}$ et $\{M'_n; n \geq 1\}$ deux marches aléatoires indépendantes. D'après le Théorème 1.1.2, presque sûrement, le groupe engendré par M_n et M'_n est libre (sous conditions naturelles sur μ). En nous basant sur l'énoncé de l'alternative de Tits [Tit72], il est naturel de se demander si ce groupe est Zariski dense. Comme nous le verrons dans le Chapitre 3, cette question est intimement liée à la probabilité de retour d'une marche aléatoire sur $\Gamma \times \Gamma$ à une sous-variété algébrique propre de $\mathbf{G} \times \mathbf{G}$.

1.2.2 Résultats et applications

Nous obtenons entre autres les théorèmes suivants :

Théorème 1.2.1. *(3.1.1) Soit μ une probabilité sur $SL_2(\mathbb{R})$ dont le support engendre un groupe non élémentaire*[8]*. Nous supposons aussi que μ a un moment exponentiel*[9]*. Si $\{M_n, n \geq 0\}$ est la marche aléatoire associée, alors pour toute variété algébrique propre $\mathcal{V}$ de $SL_2(\mathbb{R})$,*

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

Plus précisément, si P est un polynôme non constant en les entrées des matrices de $SL_2(\mathbb{R})$, il existe $\lambda > 0$ tel que :

$$\frac{1}{n} \log |P(M_n)| \underset{n\to+\infty}{\longrightarrow} \lambda$$

La dernière convergence est au sens presque sûre. De plus, une inégalité de grandes déviations est valide : pour tout $\epsilon > 0$, il existe $\rho(\epsilon) \in]0,1[$ tel que pour tout n assez grand :

$$\mathbb{P}\left(\left|\frac{1}{n} \log |P(M_n)| - \lambda\right| \geq \epsilon\right) \leq \rho(\epsilon)^n \tag{1.1}$$

Dans le cadre plus général d'un groupe algébrique déployé sur $\mathbb{R}$, nous obtenons le résultat suivant :

Théorème 1.2.2. *(3.1.2) Soient $\mathbf{G}$ un groupe algébrique semi-simple défini et déployé sur $\mathbb{R}$*[10]*, G le groupe de ses points réels et Γ un sous-groupe Zariski dense de G. Alors pour toute variété algébrique propre $\mathcal{V}$ de $\mathbf{G}$, il existe une mesure de probabilité μ adaptée sur Γ (voir la Remarque 1.2.3 suivante) telle que :*

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

8. i.e. non virtuellement résoluble ou aussi Zariski dense.

9. μ a un moment exponentiel s'il existe $\tau > 0$ tel que $\int ||g||^\tau d\mu(g) < \infty$, où $||.||$ est une norme quelconque sur $End(\mathbb{R}^d)$.

10. Par exemple, $\mathbf{G} = \mathbf{SL}_d$, $d \geq 2$.

Une inégalité de grandes déviations similaire à (1.1) est aussi valable.

Remarque 1.2.3. *Pour qu'une mesure de probabilité μ adaptée sur Γ ayant un moment exponentiel vérifie l'inégalité (1.2), il faut que le vecteur de Lyapunov associé (voir Définition 3.5.8) soit suffisamment générique, i.e. évite un certain nombre d'hyperplans déterminés par la variété $\mathcal{V}$.*

Concernant le groupe $\mathbf{G} = \mathbf{SL_d}$ nous obtenons le théorème suivant :

Théorème 1.2.4. *(3.1.5) Soit $d \geq 2$, Γ un sous-groupe Zariski dense de $SL_d(\mathbb{R})$, μ une mesure de probabilité adaptée sur Γ ayant un moment exponentiel. Alors pour toute variété algébrique propre $\mathcal{V}$ de $\mathbb{R}^d$ et pour tout $x \in \mathbb{R}^d \setminus \{0\}$,*

$$\limsup_{n\to+\infty} \Big[\mathbb{P}(M_n x \in \mathcal{V})\Big]^{\frac{1}{n}} < 1$$

Concernant la transience des sous-groupes algébriques, nous obtenons le résultat suivant :

Théorème 1.2.5. *(3.1.6) Soit $\mathbf{G}$ un groupe algébrique semi-simple défini sur $\mathbb{R}$, G le groupe de ses points réels supposé sans facteurs compacts, Γ un groupe Zariski dense de G et μ une mesure de probabilité adaptée sur Γ ayant un moment exponentiel. Alors pour tout sous-groupe algébrique $\mathbf{H}$ propre de $\mathbf{G}$ défini sur $\mathbb{R}$,*

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

Application à la généricité de la Zariski densité

Rivin [Riva] s'est intéressé à la question suivante : considérons le groupe $SL_d(\mathbb{Z})$ et prenons $g \in SL_d(\mathbb{Z})$. Est-il vrai que si h est pris "au hasard" dans $SL_d(\mathbb{Z})$ alors le groupe $\langle g, h\rangle$ engendré par g et h est Zariski dense dans $SL_d(\mathbb{R})$? Formellement, voici le résultat obtenu par Rivin

Théorème 1.2.6. *[Riva, Corollary 2.11] Soit $\mathbf{G} = \mathbf{SL_d}$ et $\Gamma = SL_d(\mathbb{Z})$, $d \geq 2$. Soient la mesure de probabilité uniforme sur une partie génératrice finie symétrique de Γ et $\{M_n, n \geq 1\}$ la marche aléatoire associée. Alors il existe $g \in \Gamma$, une constante $c(g) \in]0,1[$ tels que*

$$\mathbb{P}(\langle g, M_n\rangle \textit{soit Zariski dense}) \geq 1 - c(g)^n$$

Il est délicat de passer du groupe engendré par une matrice fixe et une marche aléatoire donné par le théorème précédent au groupe engendré par deux marches aléatoires. Dans cette direction, nous obtenons, en utilisant le Théorème 1.2.2, le résultat suivant. Celui ci complète le Théorème 1.1.2 et répond partiellement à la dernière question posée dans la section des motivations :

Théorème 1.2.7. *(3.7.4) Soit* $\mathbf{G}$ *un groupe algébrique semi-simple défini et déployé sur* $\mathbb{R}$*,* G *le groupe de ses points réels,* Γ_1*,* Γ_2 *deux groupes Zariski denses de* G[11]*. Alors il existe deux mesures de probabilité* μ_1 *et* μ_2 *respectivement sur* Γ_1 *et* Γ_2 *telles que*

$$\mathbb{P}(\langle M_{1,n}, M_{2,n}\rangle \text{ est Zariski dense et libre}) \geq 1 - c^n$$

où $c \in]0,1[$ *et* $\{M_{1,n}; n \geq 0\}$ *et* $\{M_{2,n}, n \geq 0\}$ *sont deux marches aléatoires indépendantes associées respectivement à* μ_1 *et* μ_2*.*

Remarque 1.2.8. *Ce résultat est partiel. Nous conjecturons que le théorème précédent est vrai pour toutes mesures de probabilité* μ_1 *et* μ_2 *ayant un moment exponentiel. Cependant les techniques de produits de matrices aleatoires ne semblent pas suffisantes pour traiter toutes les mesures et que probablement un rafinement des techniques de crible arithmétique [Kow08] permettra de montrer cela.*

1.3 Produits de matrices aléatoires sur un corps local

Dans le chapitre 4, nous donnons les principaux résultats obtenus concernant la théorie des produits de matrices aléatoires. Ils ont été dans l'intégralité obtenus dans le chapitre 2 mais dans un contexte un peu moins général : grosso modo les resultats du Chapitre 2 concernent les groupes semisimples déployés seulement, et le cas general est traité dans le Chapitre 4. Certains sont des généralisations de résultats connus dans le cadre du corps des nombres réels à tout corps local et d'autres sont nouveaux même sur $\mathbb{R}$. Ces résultats sont des points clés pour la preuve du Théorème 1.1.2 et des résultats cités dans la Section 1.2. Dans cette section, nous donnons quelques résultats de la deuxième catégorie.
Notons cependant que dans le Chapitre 2 nous traitons un corps local quelconque et dans le Chapitre 4 nous nous restreignons pour des raisons techniques aux corps locaux de caractéristique zéro.
Une bonne référence pour les produits de matrices aléatoires sur $\mathbb{R}$ ou $\mathbb{C}$ est le livre de Bougerol et La Croix [BL85].

1.3.1 Historique

Toutes nos variables aléatoires sont définies sur un espace probabilisé $(\Omega, \mathcal{F}, \mathbb{P})$. Le symbole p.s. signifie presque sûrement et $\mathbb{E}$ désigne l'espérence par rapport à la probabilité $\mathbb{P}$.

Soient d un entier ≥ 2, μ une mesure de probabilité sur $GL_d(\mathbb{R})$, $\{X_i; i \geq 1\}$ une suite de variables aléatoires indépendantes de loi μ. Soit Γ_μ le plus petit semi-groupe fermé de $GL_d(\mathbb{R})$ contenant le support de μ. Pour tout $n \in \mathbb{N}^*$, notons

$$S_n = X_n \cdots X_1$$

11. En particulier, le théorème est applicable pour $\mathbf{G} = \mathbf{SL_d}$, $\Gamma_1 = \Gamma_2 = SL_d(\mathbb{Z})$

Considérons la base canonique $(e_1, \cdots, e_d)$ de $\mathbb{R}^d$. Pour $g \in GL_d(\mathbb{R})$, g^t désigne la transposée de g dans cette base. Rappelons la décomposition d'Iwasawa dans $GL_d(\mathbb{R})$:

$$GL_d(\mathbb{R}) = KAN$$

avec K le groupe orthogonal, A le groupe des matrices diagonales à coefficients strictement positifs et N le groupe des matrices triangulaires supérieures avec 1 sur la diagonale. Notons pour tout $n \in \mathbb{N}^*$, $S_n = K_n A_n N_n$ la décomposition d'Iwasawa de S_n dans $GL_d(\mathbb{R})$.

Nous notons $P(\mathbb{R}^d)$ l'espace projectif de $\mathbb{R}^d$ et $[x]$ la projection de $x \in \mathbb{R}^d \setminus \{0\}$ dans $P(\mathbb{R}^d)$. Notons $\delta(\cdot,\cdot)$ la distance de Fubini-Study sur $P(\mathbb{R}^d)$:

$$\delta([x],[y]) = \frac{||x \wedge y||}{||x||||y||} \quad ; \quad [x],[y] \in P(\mathbb{R}^d)$$

Définition 1.3.1. *Soit Γ un sous-semi-groupe de $GL_d(\mathbb{R})$. On dit que Γ est fortement irréductible si et seulement si Γ ne fixe pas une réunion finie d'espace vectoriels propres. Il est dit proximal s'il contient un élément proximal, c'est-à-dire une matrixe ayant une valeur propre unique de module maximal.*

Guivarc'h avait démontré le théorème suivant :

Théorème 1.3.2. *[Gui90, Théorème 6'] Si μ a un moment exponentiel et Γ_μ agit de façon fortement irréductible et proximale, alors $N_n^t e_1$ converge p.s. vers une variable aléatoire T. De plus la vitesse de convergence est exponentielle dans le sens suivant : il existe $\epsilon > 0$, $\rho \in]0,1[$ tel que pour tout n assez grand :*

$$\mathbb{E}(|N_n^t e_1 - T|^\epsilon) \leq \rho^n$$

De plus, il montre que $K_n[e_1]$ et $N_n^t e_1$ sont asymptotiquement indépendants dans le sens suivant :

Lemme 1.3.3. *[Gui90, Lemme 8]Il existe des variables aléatoires indépendantes Z et T sur $P(\mathbb{R}^d)$, des constantes $C, \epsilon >$, $\rho \in]0,1[$ tels que pour toute fonction ϕ ϵ-holdérienne sur $X = P(\mathbb{R}^d) \times \mathbb{R}^d$, on ait :*

$$\left| \mathbb{E}\left(\phi(K_n[e_1], N_n^t e_1)\right) - \mathbb{E}\left(\phi(Z,T)\right) \right| \leq C||\phi||_\epsilon \rho^n$$

où

$$||\phi||_\epsilon = \underset{x,y \in X}{Sup} \frac{|\phi(x) - \phi(y)|}{d^\epsilon(x,y)}$$

où d est la distance naturelle sur X induite par δ.

1.3.2 Nos résultats

Une partie de la thèse est réservée à prouver les énoncés analogues aux Théorème 1.3.2 et Lemme 1.3.3 pour la décomposition de Cartan au lieu de la décomposition d'Iwasawa et dans le cadre d'un corps local arbitraire.

Considérons donc un corps local k de caractéristique zéro, $d \geq 2$, μ une mesure de probabilité sur $GL_d(k)$. Notons comme ci-dessus Γ_μ le plus petit semi-groupe fermé de $GL_d(k)$ contenant le support de μ.

Considérons la base canonique $(e_1, \cdots, e_d)$ de k^d et rappelons la décomposition KAK ou de Cartan correspodante.
Pour $k = \mathbb{R}$ ou $\mathbb{C}$, on considère la norme euclidienne (resp. hermitienne) sur k^d. Soit $K = O_d(\mathbb{R})$ (resp. $U_n(\mathbb{C})$) le groupe orthogonal (resp. unitaire), $A = \{diag(a_1, ..., a_d);\ a_i > 0\ \forall i = 1, ..., d\}$, $A^+ = \{diag(a_1, ..., a_d) \in A; a_1 \geq ... \geq a_d > 0\}$. Alors on a la décomposition suivante : $GL_d(k) = KA^+K$. Cela résulte de la décomposition polaire classique et de la théorie de réduction des matrices symétriques définies positives.

Quand k est non archimédien, on note Ω_k l'anneau des entiers et π une uniformisante (générateur de l'idéal maximal de Ω_k). Soient $K = GL_d(\Omega_k)$, $A = \{diag(\pi^{n_1}, ..., \pi^{n_d});\ n_i \in \mathbb{Z}\ \forall i = 1, ..., d\}$ et $A^+ = \{diag(\pi^{n_1}, ..., \pi^{n_d}) \in A;\ n_1 \leq ... \leq n_d\}$. Si l'on considère la norme suivante sur V : $||x|| = Max\{|x_i|; i = 1, ..., d\}$, $x \in V$, on peut prouver que K est le groupe des isométries de V. Avec ces notations, la décomposition suivante est valable : $GL_d(k) = KA^+K$. Cela résulte du théorème des facteurs invariants (voir par exemple [CR06, Théorème 16.6 page 94]) [12].

La décomposition de $g \in GL_d(k)$ dans le produit KAK n'est pas unique, cependant nous pouvons en fixer une de façon que la section $G \to KAK$ soit mesurable (dans le cas archimédien, il s'agit de diagonaliser une matrice symétrique définie positive de façon mesurable, il suffit d'appliquer l'algorithme du rang et dans le cas non archimédien, il s'agit d'opérations élémentaires sur les matrices (voir [CR06, Théorème 16.6 page 94] ou l'exemple ci-dessous pour le cas de $GL_2(\mathbb{Q}_p)$). Notons $S_n = K_n A_n U_n$ la décomposition qui correspond à S_n.

12. A titre d'exemple, illustrons cette décomposition pour $G = GL_2(Q_p)$, p étant un nombre premier. Dans ce cas $K = GL_2(\mathbb{Z}_p)$ et on peut prendre p comme uniformisante et donc $A^+ = \{diag(p^{n_1}, p^{n_2}); n_1 \leq n_2 \in \mathbb{Z}\}$. Démontrons alors la décomposition de Cartan. Soit $g = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$ une matrice de G. Quitte à multiplier g à droite par la matrice $a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in K$, on peut supposer que soit x_1 soit x_2 est de plus petite valuation parmi $\{x_1, x_2, y_1, y_2\}$. Quitte à multiplier à gauche par a, on peut supposer que x_1 de plus petite valuation. En multipliant g à gauche par la matrice $\begin{pmatrix} 1 & 0 \\ -x_2 x_1^{-1} & 1 \end{pmatrix} \in K$, on obtient une matrice du type $\begin{pmatrix} x_1 & y_1 \\ 0 & y_2' \end{pmatrix}$ avec $v(x_1) \leq v(y_2')$. Par une opération similaire, on se ramène à $\begin{pmatrix} x_1 & 0 \\ 0 & y_2' \end{pmatrix}$. Finalement, on utilise que $Q_p^\times = p^{\mathbb{Z}} \mathbb{Z}_p^\times$ où $\mathbb{Z}_p^\times$ est le groupe des unités p-adiques de $\mathbb{Z}_p$ (formé des éléments de valeur absolue 1).

Soit $P(k^d)$ l'espace projectif de k^d muni de la distance de Fubini-Study $\delta(\cdot,\cdot)$.

L'analogue du Théorème 1.3.2 pour la décomposition KAK est l'assertion suivante :

Théorème 1.3.4. *(2.4.33, 2.4.38, 3.5.15, 4.1.1) [Convergence exponentielle dans la décomposition KAK] Si μ a un moment exponentiel et Γ_μ agit de façon fortement irréductible et proximale, il existe une variable aléatoire Z sur $P(k^d)$ de loi l'unique mesure de probabilité μ^t-invariante*[13] *sur $P(k^d)$, une fonction $\rho : \mathbb{R} \longrightarrow]0,1[$ telle que pour tout $\epsilon > 0$ et tout n assez grand, on ait :*

$$\mathbb{E}\left(\delta(U_n^t[e_1], Z)^\epsilon\right) \leq \rho(\epsilon)^n \tag{1.3}$$

En particulier, $U_n^t[e_1]$ converge p.s. vers Z.

Remarque 1.3.5. *Quand nous considérons la marche aléatoire sur les k-points d'un groupe réductif défini sur k, nous obtenons un résultat analogue pour la décomposition KAK de M_n dans le groupe en question (voir le Théorème 2.4.33 et le Chapitre 4).*

Remarque 1.3.6. *Pour $k = \mathbb{R}$ et $k = \mathbb{C}$, la convergence p.s. dans le théorème précédent était déjà connue (voir par exemple [BL85, Proposition 3.2 page 51]). Par contre, l'estimée (1.3) est nouvelle.*

Remarque 1.3.7. *Dans le cas $k = \mathbb{R}$, nous donnons deux preuves du Théorème 1.3.4. La première démonstration (Théorème 2.4.38) marche pour tout corps local, la deuxième (Théorème 3.5.15) est spécifique aux corps archimédiens et utilise le produit scalaire.*

L'analogue du Lemme 1.3.3 pour la décomposition de Cartan est le résultat suivant :

Théorème 1.3.8. *(2.4.36, 2.4.39, 4.1.2)[Indépendance asymptotique dans la décomposition KAK] Avec les mêmes hypothèses que le Théorème 1.3.4, les variables $K_n[e_1]$ et $U_n^t[e_1]$ sont asymptotiquement indépendantes dans le sens suivant. Il existe des variables aléatoires indépendantes Z et T sur $P(k^d)$ de lois respectives l'unique mesure de probabilité μ-invariante sur $P(k^d)$ (resp. μ^t-invariante) vérifiant : pour tout $\epsilon > 0$, pour toute fonction ϵ-holdérienne ϕ sur $X = P(k^d) \times P(k^d)$, il existe $\rho(\epsilon) \in]0,1[$ tel que pour n assez grand :*

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

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

La preuve passe par prouver le résultat suivant concernant la convergence exponentielle des directions $M_n[x]$, $x \in k^d \setminus \{0\}$.

Theorem 1.3.9. *(2.4.16) [Convergence exponentielle en direction] Avec les mêmes hypothèses que le Théorème 1.3.4, il existe une variable aléatoire Z sur $P(k^d)$ de loi l'unique mesure de probabilité μ-invariante sur $P(k^d)$ vérifiant : pour tout $\epsilon > 0$, il existe une constante $\rho(\epsilon) \in]0,1[$ telle que pour tout n assez grand :*

$$\mathbb{E}\left(\delta(M_n[x], Z)^\epsilon\right) \leq \rho(\epsilon)^n$$

En particulier, pour tout $[x] \in P(k^d)$, $M_n[x]$ converge p.s. vers Z

13. loi de X_1^t

Remarque 1.3.10. *Pour $k = \mathbb{R}$ et $k = \mathbb{C}$, la convergence p.s. dans le théorème précédent était déjà connue (voir par exemple [BL85, Théorème 3.1 page 160]). Cependant, la vitesse de convergence est nouvelle.*

Finalement, une analyse de la partie A de la marche aléatoire M_n dans la décomposition KAK est aussi faite dans le Chapitre 4.

Chapitre 2

Les sous-groupes génériques des groupes linéaires sont libres

Random subgroups of linear groups are free

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.

Keywords: Tits alternative, random matrix products, random walks, group theory, probability theory.

Sommaire

2.1 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 $GL(n,\mathbb{Z})$, $SL(n,\mathbb{Z})$ or $Sp(n,\mathbb{Z})$ has irreducible characteristic polynomial and has the full symmetric group S_n as Galois group. 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 speaking, if μ is a probability measure on a discrete group Γ, we denote by Γ_μ the smallest semigroup containing the support of μ ; we consider a sequence $\{X_n; n \geq 0\}$ of independent random variables on Γ with the same law μ, defined on a probability space $(\Omega, \mathcal{F}, \mathbb{P})$ [1]. The n^{th} step of the random walk M_n is defined by $M_n = X_1 \cdots X_n$. We will also consider the reversed random walk : $S_n = X_n \cdots X_1$.
The main purpose of this paper is to show the following statement, which answers a question of Guivarc'h [Gui90, §2.10] :

Theorem 2.1.1. *Let K be a field, V a finite dimensional vector space over K, Γ a finitely generated non virtually solvable subgroup of $GL(V)$ equipped with two probability measures μ and μ' 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 μ and μ'. 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) and quasi isometrically (QI) embedded in Γ. More precisely, there exists $\rho \in]0,1[$ such that for all large n,*

$$\mathbb{P}\left(\langle M_n, M'_n\rangle \text{ is free and QI embedded in } \Gamma\right) \geq 1 - \rho^n \tag{2.1}$$

For the definition of the QI embedding, see Definition 2.5.6. The conditions of Theorem 2.1.1 are fulfilled when the support of μ (resp. μ') is a finite symmetric generating set, say S (resp. S') of Γ. 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 μ (resp. μ'). In this statement we could have taken S_n instead of M_n.

1. For example one can take $\Omega = \Gamma^{\mathbb{N}}$, $\mathbb{P} = \mu^{\otimes\mathbb{N}}$ the probability measure for which the coordinates w_i are independent with law μ and $\mathcal{F}$ the σ-algebra generated by the coordinate maps w_i.

Let μ be a probability measure on Γ. Define a countable family of independent random walks $(M_{n,i})_{i\in\mathbb{N}^*}$, $i \in \mathbb{N}^*$. From the proof of Theorem 2.1.1, we will deduce the following stronger statement :

Corollary 2.1.2. *There exists $C > 0$ such that a.s., for all large n, $M_{n,1}, \cdots, M_{n,\lfloor exp(Cn)\rfloor}$ generate a free group on $l_n = \lfloor exp(Cn)\rfloor$ generators*

In a recent preprint Gilman, Miasnikov and Osin considered the same problem for hyperbolic groups and proved in [GMO10, Theorem 2.1] a theorem entirely analogous to our Theorem 2.1.1 in that setting. Namely, let Γ be a non-elementary hyperbolic group, S a symmetric generating set, μ the uniform probability measure on S, $(M_n)_{n\in\mathbb{N}^*}$, $(M'_n)_{n\in\mathbb{N}^*}$ two independent random walks associated to μ, then there exists $\rho \in]0,1[$ such that :

$$\mathbb{P}\left(\langle M_n, M'_n\rangle \text{ is free and QI embedded in } \Gamma\right) \geq 1 - \rho^n$$

In [GMO10, Problem 7.2], the authors asked if the same holds for the group $SL_d(\mathbb{Z})$, $d \geq 3$, which is well-known not to be hyperbolic. Our Theorem 2.1.1 deals with an arbitrary finitely generated non virtually solvable linear group and in particular answers positively the question for $SL_d(\mathbb{Z})$.
The proof of Gilman, Miasnikov and Osin shows many similarities with ours : they show that generic elements of a hyperbolic group are in ping-pong position with respect to the Gromov boundary, while we show that generic elements of a linear group are in ping-pong position with respect to some projective linear representation. Our techniques however are fairly distinct from theirs : apart from combining geometric and algebraic ingredients, we also rely heavily on ergodic theory and in particular on the theory of random matrix products.

Other related results can be found in the recent paper of Rivin [Riv10]. He proved the following (see [Riv10, Corollary 2.11]) : let $g \in SL_d(\mathbb{Z})$, μ the symmetric probability measure on a finite symmetric generating set, $\{M_n, n \in \mathbb{N}^*\}$ the corresponding random walk, then for every $g \in \Gamma$, there exist $\rho(g) \in]0,1[$ such that for all large n,

$$\mathbb{P}(\langle g, M_n\rangle \text{ is Zariski dense }) \geq 1 - \rho^n$$

This says that heuristically if h is random in Γ, then the subgroup $\langle g, h\rangle$ is Zariski dense. Using this theorem, he proved (see [Riv10, Theorem 4.2]) that a generic subgroup H of the outer automorphism group of the free group F_d on d generators contains a subgroup whose image under the natural map to $GL_d(\mathbb{Z})$ is a non-abelian free group F and that and a generic element of H is hyperbolic.
Rivin's method uses expanding properties of the finite quotients of arithmetic groups mod p and the fast equidistribution of random walks on these finite groups.

As explained above, our main result shares a common flavor with the works by Rivin [Riv08], [Riv10] and Kowalski [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],[Riv10] and [Kow08] use

reduction modulo prime numbers and deal with subgroups of arithmetic groups $G(\mathbb{Z})$, 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 λ_1 and λ_2 and the known bounds on $\lambda_1 - \lambda_2$ rely on the ergodic theorem and are thus non effective.

Remark 2.1.3. *In Guivarch's proof of the Tits alternative in [Gui90] he showed that S_{n_k} et $S'_{n'_k}$ can be turned into ping-pong players (see Section 2.3 for a definition of these terms) in a suitable linear representation for some subsequences 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.*

Remark 2.1.4. *A closely related theorem was announced by Cowling and Dorofaeff [CD97, Theorem 5,1] who gave a sketch of the proof, similar to the one we are presenting here.*

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). Unlike the case of real and complex matrices, where good accounts on the theory exist in the literature ([GR85],[BL85], [Lia04], etc...), when the local field is non-archimedean, then the current literature ([Gui89], [Gui08]) does not cover all the limit theorems one expects. So, in this paper, we will develop most of the theory from scratch in the context of general local fields, without distinguishing between the archimedean and non-archimedean cases. Sometimes our statements will be just an adaptation of results known over the reals to arbitrary local fields while in some other places, they are new even over $\mathbb{R}$. This is the case for Theorem 2.4.33 which shows the exponential convergence of the K-components of the KAK decomposition, and for Theorems 2.4.36 and 2.4.39, which prove the asymptotic independence of the directional components of the KAK decomposition. Such result are analogs for the Cartan decomposition of earlier results of Guivarch for the Iwasawa decomposition, which can be found in [Gui90]. We refer the reader to Section 2.4 for the statements of these results. Let us only state here one of them regarding the asymptotic independence in the KAK decomposition.

Theorem 2.1.5 (Asymptotic independence in KAK with exponential rate)**.** *Let k be a local field, $\mathbf{G}$ a k-algebraic group assumed to be semi-simple and k-split, (ρ, V) an irreducible k-rational representation of $\mathbf{G}$. Consider a probability measure μ on $G = \mathbf{G}(k)$ with an exponential moment (see Definition 2.4.24) such that Γ_μ 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 μ, $S_n = X_n \cdots X_1$ the associated random walk. Denote by $S_n = K_n A_n U_n$ a KAK decomposition of S_n in G (see Section 2.4.3). Denote by $e_1 \in V$ (resp. $e_1^* \in V^*$) a highest weight vector for the action of A on V via ρ (resp. ρ^* the contragredient representation). Then the random variables $K_n[e_1]$ and $U_n^{-1} \cdot [e_1^*]$ 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 μ-invariant (resp. μ^{-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 ϵ-Holder function ϕ on $P(V) \times P(V^*)$ and all large enough n, we have :

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

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 : $g \cdot f(x) = f(g^{-1}x)$ for every $g \in G$, $f \in V^*$, $x \in V$. We have denoted by μ^{-1} the law of X_1^{-1} and by $||\phi||_\epsilon$ the Holder constant of ϕ :

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

where δ 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 2.3.2) holds : in this case, G need not be assumed Zariski connected any longer (see Theorem 2.4.39). In Chapter 4 we prove the above result the above result holds without assuming that the Zariski closure of Γ_μ is semi-simple and k-split, but assuming instead proximality and strong irreducibility.

2.1.1 Outline of the paper

In Section 2.2, we split the proof of our main theorem, i.e. Theorem 2.1.1, into two parts : an arithmetic part (Theorem 2.2.14) and a probabilistic part (Theorem 2.2.11). 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 2.5 using the results of Section 2.4.

In Section 2.3, we recall a classical method, known as ping-pong, to show that a pair of linear automorphisms generate a free group.

Section 2.4 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 [Gui89], 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 [Gui90] 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 2.4.16 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 2.4.18 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 μ-invariant measure has some regularity.
- Theorem 2.4.33 shows that the K-components of the random walk M_n in the Cartan decomposition converge exponentially fast.
- Theorem 2.4.36 proves that the K-components of the random walk M_n in the Cartan decomposition become independent asymptotically.

Theorem 2.4.18 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 2.4.16, 2.4.33 and 2.4.36 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 Secion 2.4.2. The analog of Theorem 2.4.36 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 2.4.18 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 2.4.12, a result giving control on the growth of cocyles 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 2.4.14, which says that, under the usual assumptions, for every given 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 2.4.33 is based on this approach as well and makes key use of the cocyle lemma, Lemma 2.4.12 and of Proposition 2.4.14. Theorem 2.4.16 is also an important ingredient in the proof of 2.4.33. Finally the proof of Theorem 2.4.36 combines all of the above.

We note that two Cartan decompositions will be considered in Section 2.4, 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 2.4.28). If this Zariski closure is not Zariski connected, further technicalities arise. They will be dealt with in Section 2.4.5 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 2.4.12.

Section 2.5 is devoted to the proof of Theorem 2.2.11, i.e. the probabilistic part of

our main result, using the results of Section 2.4.

Acknowledgments This work is part of the author's Ph.D. thesis at Université Paris-Sud, Orsay. 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.

2.2 Preliminary reductions

In this section we reduce the proof of Theorem 2.1.1 to its probabilistic part, i.e. Theorem 2.2.11 below.

2.2.1 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 2.2.1 (Random walks on groups)**.** *Let Γ be a discrete group, μ a probability measure on Γ, $(X_i)_{i\in\mathbb{N}^*}$ a family of independent random variables on Γ with the same law μ. For each n, we define the n^{th} step of the following random walks by :*

$$M_n = X_1 \cdots X_n \quad ; \quad S_n = X_n \cdots X_1$$

The product being the group law of Γ. We denote by Γ_μ the smallest semigroup containing the support of μ.

Remark 2.2.2. *For our main Theorem 2.1.1, there will be no difference taking the natural (M_n) or the reversed random walk (S_n) as explained in the Remark 2.2.6 below. Note however that the asymptotic behavior of the two walks is not the same in general.*

When Γ is a finitely generated group, Γ is a metric space for the word length distance : for each symmetric generating set S containing 1, define : $l_S(g) = Min\{r; g = s_1 \cdots s_r;\ s_i \in S\ \forall i = 1, \cdots, r\}$.
The following defines then a distance on Γ : $d_S(g, g') = l_S(g'^{-1}g)\ \ g, g' \in \Gamma$.

Definition 2.2.3 (Exponential moment on finitely generated groups)**.** *Let μ be a probability measure on a finitely generated group Γ. Let S be as above. We say that μ has an exponential moment if there exists $\tau > 0$ such that :*

$$\int exp\left(\tau l_S(g)\right) d\mu(g) < \infty$$

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, Γ a finitely generated non virtually solvable subgroup of $GL(V)$ equipped with two probability measures μ and μ' 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 walks associated respectively to μ and μ'. 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,*

$$\limsup_{n\to\infty} \frac{1}{n} \log\ \mathbb{P}\left(\langle M_n, M'_n\rangle \text{ is not free}\right) < 0 \tag{2.2}$$

Remark 2.2.4. *The assumptions on μ (resp. μ') of the theorem are clearly fulfilled if the support of μ (resp. μ') is a finite, symmetric generating set of Γ*

Remark 2.2.5. *The bound (2.2) implies that there exists $\rho \in]0,1[$ such that for n large enough,*

$$\mathbb{P}\left(\langle M_n, M'_n\rangle \text{is not free}\right) \leq \rho^n \tag{2.3}$$

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 (2.3).

Remark 2.2.6. *There is no difference taking $(M_n)_{n\in\mathbb{N}^*}$ or the reversed random walk in Theorem 2.1.1. In fact, the increments are independent and have the same law which implies that $(X_1, \cdots, X_n)$ has the same law as $(X_n, \cdots, X_1)$ for every integer n, hence (2.2) is unchanged if we replaced M_n by S_n.*

2.2.2 Outline of the proof of Theorem 2.1.1

A local field (i.e. a commutative locally compact field) is isomorphic either to $\mathbb{R}$ or $\mathbb{C}$ (archimedean 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 archimedean, we denote by $|\cdot|$ the Euclidean absolute value. When k is not archimedean, we denote by Ω_k its discrete valuation ring, π a generator of its unique maximal ideal, q the degree of its residual field, $v(\cdot)$ a discrete valuation and consider the following ultrametric norm : $|\cdot| = q^{-v(\cdot)}$.

When we consider a finitely generated **linear group** Γ, 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, Γ can be considered as a metric space with the topology of $End_d(k)$ induced on Γ. This justifies the two parts of our proof : the arithmetic part (Theorem 2.2.14) which consists in finding a suitable local field containing K and the probabilistic one (Theorem 2.2.11) consisting in using limit theorems for random walks on linear groups over local field. Theorem 2.2.14 will be borrowed from [MS81] and Theorem 2.2.11 is the main part of this paper. Before stating them and showing how they provide a proof of Theorem 2.1.1, we give some basic definitions :

Definition 2.2.7. *(Strong irreducibility and contraction properties)*
• ***Strong irreducibility*** *: let K be a field, V a vector space over K and Γ a subgroup of $GL(V)$. The action of Γ on V is said to be strongly irreducible if Γ does not fix a finite union of proper subspaces of V. This is equivalent to saying that Γ 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 Γ is strongly irreducible if and only if $\overline{\Gamma}$ is.*
• ***Contraction for local fields*** *: Let $(k, |\cdot|)$ be a local field, V a vector space over k and Γ a subgroup of $GL(V)$. We choose any norm $||\cdot||$ on $End(V)$. We say that a sequence $(\gamma_n)_{n\in\mathbb{N}} \subset \Gamma^{\mathbb{N}}$ is contracting, if $r_n\gamma_n$ converges, via a subsequence, to a rank one endomorphism for every (or equivalently one) suitable normalization $(r_n)_{n\in\mathbb{N}}$ of k such that $||r_n\gamma_n|| = 1$. It is equivalent to say that the projective transformation $[\gamma_n] \in PGL(V)$ 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 ρ of Γ 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 2.4.5.

Lemma 2.2.8 (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 Γ contains a proximal element then it is contracting. If Γ acts irreducibly on V and is contracting then it contains a proximal element.*

Proof. If $\gamma \in \Gamma$ is proximal, then its maximal eigenvalue λ belongs to the field k and the corresponding eigendirection is defined on k. The latter has a γ-invariant supplementary hyperplane defined on k. Consequently, in a suitable basis, γ 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 Γ, $\{r_n; n \in \mathbb{N}\}$ 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 γ_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 $g\gamma_n$ 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 Γ on V is irreducible. Consequently, there exists $g \in \Gamma$ such that $gx_0 \notin Ker(h)$. But $gx_0 = Im(gh)$ and $Ker(h) = Ker(gh)$; whence gh is proximal.

□

Definition 2.2.9 (Exponential local moment on linear groups)**.** *Let k be a local field, d an integer ≥ 2, Γ be a subgroup of $SL_d(k)$, $||\cdot||$ a norm on $End_d(k)$, μ a probability*

measure on Γ. *We say that* μ *has an exponential local moment if for some* $\tau > 0$,

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

Remark 2.2.10 (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* $\int exp(\tau d_X(\overline{g}, \overline{I_d})) d\mu(g) < \infty$ *where* $X = SL_d(k)/K$ *is the symmetric space associated to* $SL_d(k)$ *(see Section 2.4.2 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 μ on $SL_d(k)$, Γ_μ denotes the smallest **closed** semigroup containing the support of μ.

Theorem 2.2.11 (Probabilistic part)**.** *Let* k *be a local field,* $d \geq 2$, μ, μ' *two probability measures on* $SL_d(k)$ *having an exponential local moment and such that* Γ_μ *and* $\Gamma_{\mu'}$ *be strongly irreducible and contracting* ***subgroups****. We assume their Zariski closure to be* k*-split and their connected component semi-simple. We denote by* $(M_n)_{n \in \mathbb{N}^*}$ *(resp.* $(M'_n)_{n \in \mathbb{N}^*}$*) the random walks associated to* μ *(resp.* μ'*). Then a.s. for all* n *large enough, the group* $\langle M_n, M'_n \rangle$ *generated by* M_n *and* M'_n *is free. More precisely,*

$$\limsup_{n \to \infty} \frac{1}{n} \log \ \mathbb{P}\left(\langle M_n, M'_n \rangle \textit{is not free}\right) < 0 \tag{2.4}$$

Remark 2.2.12. *The assumptions* $\overline{\Gamma_\mu}$ *semi-simple and* k*-split can be dropped :* Γ_μ *being strongly irreducible, the Zariski connected component of* $\overline{\Gamma_\mu}$ *is immediately reductive and everything we will do in Section 2.4.4 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 2.4.4 and 2.4.3, however similar decompositions hold in the general case. To keep the exposition as simple as possible we kept these conditions. However, in Chapter 4 we will consider the general case.*

Remark 2.2.13. $\{w \in \Omega; \langle M_n(w), {M_n}'(w) \rangle$ *is not free*$\}$ *is measurable because it is the countable union of inverse images of Zariski closed subsets of* $G \times G'$, *where* G *(resp.* G'*) is the Zariski closure of* Γ_μ *(resp.* $\Gamma_{\mu'}$*).*

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

Theorem 2.2.14 (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,* Γ *be a* K*-Zariski dense subgroup. Then there exists a local field* k *containing* K, *a vector space* V *over* k *and a* k*-algebraic absolutely strongly irreducible representation* $\rho : G \longrightarrow SL(V)$ *such that* $\rho(\Gamma)$ *is contracting and the Zariski component of* $\rho(G)$ *is a semi-simple group.*

Remark 2.2.15. *A classical lemma of Tits -[Tit72]- says (or at least implies) the same as Theorem 2.2.14 except that* ρ *is a representation of a finite index subgroup of* G. *This is insufficient for us because the random walk lives in all of* Γ. *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 2.2.14 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 ρ takes value in $PGL(V)$, and this is not enough for our purposes.

End of the proof of Theorem 2.1.1 modulo Theorem 2.2.11

We will only prove here the freeness of the group generated by M_n and M'_n, i.e. equation (2.1) without the QI embedding part which will be proved at the end of the article. Let $\Gamma = \Gamma_\mu = \Gamma_{\mu'}$. Since Γ 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 Γ. Let G be the Zariski closure of Γ. Then, we can apply Theorem 2.2.14. It gives a local field k, a k-rational absolutely strongly irreducible representation (ρ, 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 ; ρ remains absolutely strongly irreducible. We are now in the situation of Theorem 2.2.11 : we have a probability measure $\rho(\mu)$ (image of μ under ρ) on some $SL_d(k)$ such that $\Gamma_{\rho(\mu)}$ is strongly irreducible and contracting (because it contains $\rho(\Gamma)$ which is Zariski dense). Moreover, the connected component of its Zariski closure H is semi-simple and k-split. To apply Theorem 2.2.11 we only have to check that $\rho(\mu)$ has an exponential local moment knowing that μ has an exponential moment. Indeed, if $g = s_1^{n_1(g)} \cdots s_r^{n_r(g)} \in Supp(\mu)$ is a minimal expression of g in terms of the generators of a symmetric finite generating set S of Γ, then $l_S(g) = |n_1(g)| + \cdots + |n_r(g)|$ whence $||\rho(g)|| \leq \left[Max\{\log||\rho(s)|| \vee \log||\rho(s^{-1})||; s \in S\}\right]^{l_S(g)}$. Consequently, if $\mathbb{E}\left(exp(\tau l_S(X_1))\right)$ is finite, then for some $\tau' > 0$, $\mathbb{E}\left(||\rho(X_1)||^{\tau'}\right)$ is also finite. We can now apply Theorem 2.2.11 : 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.

□

2.3 Generating free subgroups in linear groups

In Theorem 2.2.11 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].

2.3.1 The ping-pong method

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

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

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 **ϵ-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 ϵ-neighborhood of $H_g \subset P(V)$ into the ϵ-ball around v_g. We say that $[g]$ is **ϵ-very contracting** if both $[g]$ and $[g^{-1}]$ are ϵ-contracting.
- $[g]$ is called (r,ϵ)**- proximal** ($r > 2\epsilon > 0$) if it is ϵ-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,ϵ)**-very proximal** if both $[g]$ and $[g]^{-1}$ are (r,ϵ)-proximal.
- A pair of projective transformations $a, b \in PSL(V)$ is called **a ping-pong pair** if both a and b are (r,ϵ)-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 $a_1, \cdots, a_m$ is called a ping-pong m-tuple if all a_i's are (r,ϵ)-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 2.3.1 (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 $a_1, \cdots, a_m$ is a ping-pong m-tuple then $\langle a_1, \cdots, a_m\rangle$ is free.*

2.3.2 The Cartan decomposition

Let $d \geq 2$, $V = k^d$ and $(e_1, \cdots, e_d)$ its canonical basis.
The attracting points and repelling hyperplanes are not unique. In this article, they will be defined via the Cartan decomposition in $SL(V)$ [2]. 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 $(e_1, \cdots, e_d)$. Let $K = SO_d(k)$ (resp. $SU_n(\mathbb{C})$) be the orthogonal (resp. unitary) group, $A = \{diag(a_1, \cdots, a_d);\ a_i > 0\ \forall i = 1, \cdots, d;\ \prod_{i=1}^d a_i = 1\}$, $A^+ = \{diag(a_1, \cdots, a_d) \in A; a_1 \geq \cdots \geq a_d > 0\}$. 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 $A = \{diag(\pi^{n_1}, \cdots, \pi^{n_d});\ n_i \in \mathbb{Z}\ \forall i = 1, \cdots, d; \sum_{i=1}^d n_i = 0\}$; $A^+ = \{diag(\pi^{n_1}, \cdots, \pi^{n_d}) \in A;\ n_1 \leq \cdots \leq n_d\}$. If we consider the Max norm on V : $||x|| = Max\{|x_i|; i = 1, \cdots, d\}$, $x \in V$, 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, Theorem 16.6 page 94] and the example of Section 1.3.2 of the introduction for the case $SL_2(\mathbb{Q}_p)$). One can also see it as a particular case of the Cartan decomposition for algebraic groups (see Section 2.4.3).

2. A similar decomposition holds for $GL(V)$, see Section 1.3.2 for example.

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 $g = k(g)a(g)u(g)$ "its" KAK decomposition with $a(g) = diag\,(a_1(g), \cdots, a_d(g))$. Till the end of the paper, we write $v_g = k(g)[e_1]$ and $H_g = \left[Span\langle u(g)^{-1}e_2, \cdots, u(g)^{-1}e_d\rangle\right]$. 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 2.3.2. *[BG03] Let $\epsilon > 0$. If $|\frac{a_2(g)}{a_1(g)}| \leq \epsilon^2$, then $[g]$ is ϵ-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 $H_g = \left[Span\langle u(g)^{-1}e_2, \cdots, u(g)^{-1}e_d\rangle\right]$. Let $x \in V$ such that $d(x, H_g) > \epsilon$. We want to prove that $d(g[x], v_g) < \epsilon$. Notice that $H_g = Ker\,(u(g)^{-1} \cdot e_1^*(\cdot))$. Hence $\frac{|u(g)^{-1} \cdot e_1^*(x)|}{||x||} > \epsilon$. 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 $|a_1(g)| \geq \cdots \geq |a_d(g)|$, $||a(g)u(g)x \wedge e_1|| \leq |a_2(g)|||x||$. Moreover, $||a(g)u(g)x|| \geq |a_1(g)|\,|u(g)^{-1} \cdot e_1^*(x)|$. Hence,

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

□

2.4 Random matrix products in local fields

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

• When μ is a probability on a group G, we consider both random walks $M_n = X_1 \cdots X_n$ and $S_n = X_1 \cdots X_n$ as defined in Section 2.2. Γ_μ is the smallest closed semigroup containing the support of μ.

2.4.1 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 2.4.2, 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 2.4.16) and the exponential decay of the probability of hitting a hyperplane (Theorem 2.4.18). A key ingredient in the proofs is our cocycle lemma, Lemma 2.4.12, which is a rather general statement giving control on the size of a cocycle in an abstract context. Another important tool will be Proposition 2.4.14, 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 2.4.27).

In Section 2.4.3, 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 2.4.4 and Section 2.4.5, we establish limit theorems for the components of the Cartan decomposition of the random walk. The main results are Theorem 2.4.31 (exponential contraction of the A-component), Theorem 2.4.33 (exponential convergence of the K-components) and Theorem 2.4.36 (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 2.4.28). In fact, in order to study the Cartan decomposition in the ambient $SL_d(k)$, 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 2.4.32). The case when the Zariski closure is connected is easier and is dealt with in Section 2.4.4, while the general case is handled in Section 2.4.5.

2.4.2 Convergence in direction

Generalization of well-known results in an non archimedean setting

This section does not require any prior knowledge on algebraic groups.
Let $B = (e_1, \cdots, e_d)$ 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, $||x|| = Max\{|x_i|; i = 1, \cdots, d\}$ for every $x \in V$, when k is non archimedean.
Recall that by Section 2.3, there exist a compact subgroup K acting by isometries on V, a subgroup A^+ consisting of diagonal matrices such that : $SL_d(k) = KA^+K$ (Cartan decomposition). For $g \in SL_d(k)$, we denote by $g = k(a)a(g)u(g)$ a privileged decomposition of g in this product.

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

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

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

$$\delta([x],H) = \frac{||f(x)||}{||f||||x||} \quad ; x \in V \setminus \{0\}$$

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

Definition 2.4.1. *If G is a group acting on a topological space X, μ (resp. ν) a probability measure on G (resp. X), ν is said to be μ-invariant if $\mu \star \nu = \nu$, which means that for every borel function on X, $\iint f(g \cdot x) d\mu(g) d\nu(x) = \int f(x) d\nu(x)$.*

Definition 2.4.2 (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 μ are defined recursively by :*

$$\lambda_1 + \cdots + \lambda_i = \lim \frac{1}{n} \mathbb{E}(\log || \bigwedge^i S_n ||) = \lim \frac{1}{n} \log || \bigwedge^i S_n ||$$

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

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

Lemma 2.4.4. *[Fur63] Let G be a topological semigroup acting on a 2^{nd} countable locally compact space X. Consider a sequence $\{X_n, n \geq 1\}$ of independent random elements of G with a common distribution μ defined on $(\Omega, A, \mathbb{P})$. We denote $\lambda = \sum_{n=0}^{\infty} 2^{-n-1} \mu^n$. If ν is a μ-invariant probability measure on X then there exists a random probability measure ν_ω on X such that for $\mathbb{P} \otimes \lambda$-almost every (ω, g), the sequences of probability measures $X_1(\omega) \cdots X_n(\omega) g\, \nu$ converge weakly to ν_ω as n goes to infinity.*

Using Lemma 2.4.4, 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 2.4.5. *Suppose that Γ_μ is strongly irreducible. Then, for p=index(Γ_μ), there exists a random subspace $V(\omega)$ of V of dimension p such that : a.s. for every $(r_n)_{n \in \mathbb{N}^*} \in k^{\mathbb{N}}$ 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 $f \in V^*$,*

$$\mathbb{P}\left(f|_{V(\omega)} \equiv 0\right) = 0$$

When Γ_μ is contracting, $p = 1$ and there exists a unique μ-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 ν.

Theorem 2.4.6. *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 2.4.5. A general lemma of Furstenberg (see for example [BL85], Proposition 2.3 page 49) says that every μ-invariant probability measure on $P(V)$ is proper, i.e. does not charge any projective hyperplane. Now, fix a μ-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 $x \notin Ker(A(\omega))$, $M_{n_k}(\omega) \cdot [x]$ converges to $A(\omega) \cdot [x]$. Since ν is proper, we deduce that $M_{n_k}(\omega) g\nu$ converges weakly towards $A(\omega) g\nu$ for every $g \in SL_d(k)$. On the other hand, by Lemma 2.4.4, there exists a random probability measure ν_ω on $P(V)$ (whose expectation is ν) such that $M_n(\omega) g\nu$ converges weakly towards ν_ω for λ-almost every $g \in SL_d(k)$, where λ 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 λ-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 λ is $\Gamma_\mu \cup \{I_d\}$, hence

$$A(\omega) g\nu = \nu_\omega \quad \forall g \in \Gamma_\mu \cup \{I_d\} \tag{2.5}$$

Let $V(\omega)$ be the linear span of $\{x \in V; [x] \in Supp(\nu_\omega)\}$. (2.5) 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 Γ_μ. By definition of the index, the rank of $A(\omega)$ is at least p. The index of Γ_μ being p, there exists $\{h_n; n \geq 1\}$ in Γ_μ, $\{s_n; n \geq 1\}$ in k such that $s_n h_n$ converges to an endomorphism h of rank p. (2.5) shows that :

$$A(\omega) g h_n \nu = \nu_\omega \quad \forall g \in \Gamma_\mu;\ n \geq 1$$

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

$$A(\omega) g h \nu = \nu_\omega$$

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 ν-almost every $[x] \in P(V)$, $A(\omega) g h_n [x]$ would converge to $A(\omega) gh[x]$ so that $\nu_\omega = A(\omega) g h_n \nu$ would converge to $A(\omega) gh\nu$. 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 ν,

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

Hence $\{gx; g \in \Gamma_\mu; x \in Im(h)\}$ would be contained in the kernel of $A(\omega)$. Since it is Γ_μ-invariant, this contradicts the irreducibility assumption on Γ_μ. We have then proved that $V(\omega)$ is a p-dimensional subspace of V and is the image of every limit point of $r_n M_n$, where $||r_n M_n|| = 1$. By Lemma 2.4.4, $\nu = \int \nu_\omega \, d\mathbb{P}(\omega)$. Therefore,

$$\begin{aligned} \mathbb{P}(f|_{V(\omega)} \equiv 0) &= \mathbb{P}\left(f(y) = 0 \ \forall y \in Supp(\nu_\omega)\right) \\ &\leq \mathbb{E}\left(\int \mathbb{1}_{f(y)=0} \, d_{\nu_\omega([y])}\right) \\ &= \nu\left(Ker(f)\right) \end{aligned}$$

Since ν is proper, this is equal to zero.
Finally, if Γ_μ is contracting, then $p = 1$ by definition and $[V(\omega)]$ is reduced to a point $Z(\omega) \in P(V)$. Since, by Lemma 2.4.4, $\nu = \int \delta_{Z(\omega)}\, d\mathbb{P}(\omega)$, we deduce that the distribution of Z is ν and hence ν is unique. □

Corollary 2.4.7 (Convergence in KAK). *Suppose that Γ_μ acts strongly irreducibly on V. Then the subspace $(k(M_n)e_1, \cdots, k(M_n)e_p)$ converges a.s. to a random subspace $V(\omega)$ of dimension $p = index(\Gamma_\mu)$. Similarly, the same holds for the subspace $(U_n^{-1}\cdot {e_1}^*, \cdots, U_n^{-1}\cdot {e_p}^*)$. Moreover, a.s. $\lim_{n\to\infty} \frac{a_{p+1}(M_n)}{a_1(M_n)} = 0$ and $Inf_n \frac{a_p(M_n)}{a_1(M_n)} > 0$. The latter two assertions hold for S_n.*

Remark 2.4.8. *It is clear that we can replace $U_n^{-1}\cdot e_1^*, \cdots, U_n^{-1}\cdot e_p^*$ with $U_n^t e_1, \cdots, U_n^t e_p$ 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 $a_1(M_n), \cdots, a_d(M_n)$ be the diagonal components of $a(M_n)$. Since K acts by isometries on V, $|a_1(M_n)| = ||M_n||$. Hence, for p=index (Γ_μ), Theorem 2.4.5 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 ω, we have :

$$\frac{M_n(\omega)}{a_1(M_n(\omega))} = k(M_n(\omega))\; diag\left(1, \cdots, \frac{a_d(M_n(\omega))}{a_1(M_n(\omega))}\right)\; u(M_n(\omega))$$

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

$$A(\omega) = K_\infty(\omega) diag\,(1, \cdots, \alpha_d(\omega))\, U_\infty(\omega)$$

Since $A(\omega)$ is almost surely of range p, almost surely, $\alpha_{p+1}(\omega) = \cdots = \alpha_d(\omega) = 0$ and $\alpha_2(\omega), \cdots, \alpha_p(\omega)$ are non zero elements of $[0, 1]$ when k is archimedean and of Ω_k when k is non archimedean ; proving the last assertion of the corollary.
Since the image of $A(\omega)$ is $V(\omega)$,

$$V(\omega) \subset Span\langle K_\infty(\omega)e_1, \cdots, K_\infty(\omega)e_p\rangle$$

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 $(k(M_n)e_1, \cdots, k(M_n)e_p)$ towards $V(\omega)$.
Now notice that Γ_μ acts strongly irreducibly on V if and only if $\Gamma_{\mu^{-1}}$ acts strongly irreducibly on V^*. Moreover, Γ_μ has the same index as $\Gamma_{\mu^{-1}}$ viewed as a subgroup of $SL(V^*)$ (it is just formed by the transposed matrices of Γ_μ). Hence the same proof as above holds by looking at $S_n^{-1} = X_1^{-1}\cdots X_n^{-1}$ acting on V^*- instead of $M_n = X_1\cdots X_n$ acting on V. □

Proposition 2.4.9. *If Γ_μ acts strongly irreducibly on V, then for any sequence $\{x_n; n \geq 0\}$ in V converging to a non zero vector :*

$$a.s \qquad inf_{n\in\mathbb{N}^*} \frac{||S_n x_n||}{||S_n||} > 0 \tag{2.6}$$

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. $k = \mathbb{C}$).

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

By Corollary 2.4.7, a.s. $inf_{n\in\mathbb{N}^*} \frac{a_p(n)}{a_1(n)} > 0$.
We claim that a.s.

$$Inf_{n\in\mathbb{N}^*} \sum_{i=1}^p | < x_n, U_n^* e_i > |^2 \ > \ 0 \tag{2.7}$$

Indeed, by Corollary 2.4.7, the subspace $(U_n^* e_1, \cdots, U_n^* e_d)$ converges a.s. to a subspace $V(\omega)$. Let $\Pi_{V(\omega)}$ be the orthogonal projection on $V(\omega)$. Hence $\sum_{i=1}^p | < U_n^* e_i, x_n > |^2 \xrightarrow[n\to\infty]{\text{a.s.}} ||\Pi_{V(\omega)}(x)||^2$. By Theorem 2.4.5 : $\mathbb{P}\left(\Pi_{V(\omega)}(x) = 0\right) = 0$. The claim is proved.

When k is non archimedean,

$$\begin{aligned} \frac{||S_n x_n||}{||S_n||} &= \frac{1}{|a_1(n)|} Max\{|a_i(n)||U_n^{-1} \cdot e_i^*(x_n)| \, ; i = 1, \cdots, d\} \\ &\geq \frac{|a_p(n)|}{|a_1(n)|} Max\{|U_n^{-1} \cdot e_i^*(x_n)|; \ i = 1, \cdots, p\} \end{aligned}$$

Again, by Corollary 2.4.7, $inf_{n\in\mathbb{N}^*} \frac{|a_p(n)|}{|a_1(n)|} > 0$ and it suffices to show that, a.s,

$$Inf_{n\in\mathbb{N}^*} \ Max\{|U_n^{-1} \cdot e_i^*(x_n)|; \ i = 1, \cdots, p\} > 0 \tag{2.8}$$

Indeed, let $V(\omega)$ be the limiting subspace of $(U_n^{-1} \cdot e_1^*, \cdots, U_n^{-1} \cdot e_p^*)$ and U_∞ a limit point of U_n. $Max\{|U_n^{-1} \cdot e_i^*(x_n)|; \ i = 1, \cdots, p\}$ converges then a.s., via a subsequence, to $Max\{|(U_\infty)^{-1} \cdot e_i^*)(x)|; \ i = 1, \cdots, p\}$. The following claim shows that this is in fact independent from the subsequence and equals $Sup\{\frac{|f(x)|}{||f||}; \ f \in V(\omega)\}$, which is a.s. positive because by Theorem 2.4.5, $\mathbb{P}\left(f(x) = 0 \ \forall f \in V(\omega)\right) = 0$.
Claim : Let V be a vector space of dimension $d \geq 2$ with basis $(e_1, \cdots, e_d)$, E a subspace of the dual V^* of dimension $p < d$, $B = (f_1, \cdots, f_p)$ a basis of the dual E. We suppose that B is in the orbit of $(e_1^*, \cdots, e_p^*)$ under the natural action of $K = SL_d(\Omega_k)$ on $(V^*)^p$. In other words, assume that there exists $g \in K$ such that $f_i = g e_i^*$ for every $i = 1, \cdots, p$. Then for every non zero vector $x \in V$,n

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

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, $|f(x)| \leq Max\{|\lambda_i|, i = 1, \cdots, p\} Max\{|f_i(x)|; i = 1, \cdots, p\}$. But, $f_i = g e_i^*$ with $g \in K$ which implies that $g^{-1} f = \sum_{i=1}^p \lambda_i e_i^*$ so that $||f|| = ||g^{-1} f|| = Max\{|\lambda_i|; i = 1, \cdots, p\}$. Hence $|f(x)| \leq ||f|| \ Max\{|f_i(x)|; i = 1, \cdots, p\}$. □

Corollary 2.4.10. *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 *;*

$$\frac{1}{n}\log||S_n x_n|| \xrightarrow[n\to\infty]{a.s.} \lambda_1 \quad ; \quad Sup_{x\in V\setminus\{0\}} \frac{1}{n}\mathbb{E}(\log\frac{||S_n x||}{||x||}) \underset{n\to\infty}{\longrightarrow} \lambda_1$$

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 : $\frac{1}{n}\mathbb{E}(\log\ ||S_n x_n||) \underset{n\to\infty}{\longrightarrow} \lambda_1$. 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 μ, 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. □

A cocycle lemma - Application 1 : "weak" large deviations

Definition 2.4.11. *Let* G *be a topological semigroup acting on a topological space* X. *We assume the map* $(g,x) \longmapsto g\cdot x$ *to be continuous. A continuous map* $G\times X \xrightarrow{s} \mathbb{R}$ *is said to be an additive cocycle if* $s(g_1g_2,x) = s(g_1, g_2\cdot x) + s(g_2,x)$ *for any* $g_1, g_2 \in G$, $x \in B$.

Lemma 2.4.12 (Cocycle lemma)**.** *Let* G *be a topological semigroup acting on a topological space* X, s *a cocycle on* $G\times X$, μ *a probability measure on* G *satisfying for* $r(g) = sup_{x\in X}|s(g,x)|$ *: there exists* $\tau > 0$ *such that*

$$\mathbb{E}\left(exp(\tau r(X_1))\right) < \infty \tag{2.9}$$

- *If*

$$\lim_{n\to\infty}\ \frac{1}{n}Sup_{x\in X}\ \mathbb{E}(s(S_n,x)) < 0,$$

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

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

- *If*

$$\lim_{n\to\infty}\ \frac{1}{n}Sup_{x\in X}\ \mathbb{E}(s(S_n,x)) = 0,$$

then for all $\gamma > 0$, *there exist* $\epsilon(\gamma) > 0$, $n(\gamma) \in \mathbb{N}^*$ *such that for every* $0 < \epsilon < \epsilon(\gamma)$ *and* $n > n(\gamma)$,

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

Remark 2.4.13. *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 $Q_n = Sup_{x\in X}\ \mathbb{E}\Big[exp[\epsilon\,(s(S_n,x))]\Big]$. Q_n being sub-multiplicative, for every p,

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

Using the inequality

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

we get for $\tau' = \frac{\tau}{3}$, $0 \leq \epsilon \leq \tau'$,

$$\limsup_{n\to\infty}\frac{1}{n}\log\ Q_n \leq \frac{1}{p}\log\Big(1 + \epsilon\underbrace{Sup_{x\in X}\mathbb{E}(s(S_p,x))}_{a_p} + \frac{\epsilon^2}{2\tau'}\mathbb{E}\big(exp\,(\tau r(S_p))\,\big)\Big)$$

Let $C = \mathbb{E}\big(exp\,(\tau(r(X_1)))\,\big) < \infty$. The cocycle property implies that $r(g_1g_2) \leq r(g_1) + r(g_2)$ for every $g_1, g_2 \in G$, whence $\mathbb{E}\big(exp\,(\tau(r(S_p)))\,\big) \leq C^p$. Hence, for every integer p,

$$\limsup_{n\to\infty}\frac{1}{n}\log\ Q_n \leq \frac{1}{p}\log\ \left(1 + \epsilon a_p\ + \frac{\epsilon^2}{2\tau'}C^p\right) \tag{2.10}$$

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

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

(2.10) becomes : for every integer p,

$$\limsup_{n\to\infty}\frac{1}{n}\log\ Q_n \leq \log\,(1 + \epsilon\frac{a_p}{p} + \frac{\epsilon^2}{2\tau'}\frac{C^p}{p}) \tag{2.11}$$

• Suppose first that $\frac{a_p}{p}$ converges to $\lambda' < 0$ as p goes to infinity. The quantity a_p being subadditive, $\frac{a_p}{p}$ 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 (2.11) with $p = p_0$ and choose $\epsilon > 0$ small enough such that : $\frac{a_{p_0}}{p_0}\epsilon + \epsilon^2\frac{C^{p_0}}{2\tau' p_0} \leq -\lambda\epsilon \iff 0 < \epsilon \leq \frac{-\tau' a_{p_0}}{C^{p_0}}$.

• 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, $\frac{a_p}{p} \leq \frac{\gamma}{2}$. Fix such p. For $\epsilon \leq \epsilon(\gamma)$ small enough, $\epsilon^2\frac{C^p}{2\tau' p} \leq \epsilon\frac{\gamma}{2}$. It suffices now to apply (2.11). □

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 $\frac{1}{n}\log||S_nx||$, for any non zero vector x of V. By Proposition 2.4.10 these quantities converge towards the first Lyapunov exponent λ_1. More precisely, for every $\epsilon > 0$, there exist $\rho = \rho(\epsilon) \in]0,1[$ and $n_0 = n_0(\epsilon)$ such that for $n \geq n_0$,

$$\mathbb{P}\left(\Big|\frac{1}{n}\log||S_n|| - \lambda_1\Big| \geq \epsilon\right) \leq \rho^n\ \ ;\ \ \mathbb{P}\left(\Big|\frac{1}{n}\log||S_nx|| - \lambda_1\Big| \geq \epsilon\right) \leq \rho^n \tag{2.12}$$

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

$$\mathbb{P}\left(\frac{||S_n||}{||S_n x||} \geq exp(n\epsilon)\right) \leq \rho^n \tag{2.13}$$

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 (2.13) using our cocycle Lemma 2.4.12. Moreover our bound will be uniform in x ranging over the unit sphere in V.

Proposition 2.4.14 (Weak large deviations)**.** *Suppose that μ has an exponential local moment and that Γ_μ 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 $n > n(\gamma)$:*

$$Sup_{x\in V;\, ||x||=1}\, \mathbb{E}\big[(\frac{||S_n||}{||S_n x||})^\epsilon\big] \leq (1+\epsilon\gamma)^n \tag{2.14}$$

In particular, for every $\epsilon > 0$,

$$\limsup_{n\to\infty} \Big[Sup_{x\in V;\, ||x||=1}\, \mathbb{P}\left(\frac{||S_n||}{||S_n x||} \geq exp(n\epsilon)\right)\Big]^{\frac{1}{n}} < 0 \tag{2.15}$$

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

$$Sup_{[x],[y]}\, \mathbb{E}\big[(\frac{||S_n x||||y||}{||S_n y||||x||})^\epsilon\big] \leq (1+\epsilon\gamma)^n \tag{2.16}$$

Indeed, $s(g,([x],[y])) = \log\, \frac{||gx||||y||}{||gy||||x||}$ defines an additive cocyle on $\Gamma_\mu \times (P(V)\times P(V))$, for the natural action of Γ_μ on $P(V)\times P(V)$. It suffices now to verify the hypotheses of Lemma (2.4.12). Since for every $g \in SL_d(k)$, $||g^{-1}|| \leq ||g||^{d-1}$, $\mathbb{E}\,(exp(\tau\, r(X_1))) \leq \mathbb{E}(||X_1||^\tau ||X_1^{-1}||^\tau) \leq \mathbb{E}(||X_1||^{\tau d})$. This is finite for τ small enough because μ has an exponential local moment. The condition (2.9) of Lemma 2.4.12 is then fulfilled. It suffices now to show that

$$\lim_{n\to\infty} Sup_{[x],[y]} \mathbb{E}\,(s(S_n,([x],[y]))) = 0$$

(≤ 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 :

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

This is true since by (the proof of) Corollary 2.4.10 :

$$\lim_{n\to\infty} \frac{1}{n}\mathbb{E}(\log||S_n x_n||) = \lim_{n\to\infty} \frac{1}{n}\mathbb{E}(\log||S_n y_n||) = \lambda_1 \tag{2.17}$$

Notice that $||g|| \asymp max\{||ge_i||;\ i = 1,\cdots,d\}$ for every $g \in GL(V)$. Hence, $Sup_{[x]}\, \mathbb{E}\big[(\frac{||S_n||||x||}{||S_n x||})^\epsilon\big] \preceq \sum_{i=1}^d Sup_{[x]}\, \mathbb{E}\big[(\frac{||S_n e_i||||x||}{||S_n x||})^\epsilon\big]$. Applying (2.16) shows (2.14).
Finally, we prove (2.15) : let $\epsilon > 0$, $\gamma > 0$ to be chosen in terms of ϵ. By (2.14) and the Markov inequality there exist $\epsilon'(\gamma) > 0, n(\gamma) > 0$ such that for $0 < \epsilon' < \epsilon'(\gamma)$ and $n > n(\gamma)$:

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

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

Application 2 : exponential convergence in direction

Proposition 2.4.15. *Suppose that μ has an exponential local moment and that Γ_μ 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 $n > n_0$:*

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

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

$$s\left(g, ([x],[y])\right) = \log \frac{\delta(g[x], g[y])}{\delta([x],[y])} \quad ; g \in \Gamma_\mu; ([x],[y]) \in X$$

It is easy to verify that s is an additive cocycle on $\Gamma_\mu \times X$ for the natural action of Γ_μ on X. It suffices now to check the hypotheses of Lemma 2.4.12.

By definition of the distance δ, we have for every $g \in SL_d(k)$, $([x],[y]) \in X$, $\log \frac{\delta(g[x],g[y])}{\delta([x],[y])} \leq 2d \log||g||$. Since μ has an exponential local moment, (2.9) of Lemma 2.4.12 is valid. It is left to check that we are in the first case of the lemma, i.e. $\lim \frac{1}{n} Sup_{([x],[y])\in X} \mathbb{E}\left(s(S_n,(x,y))\right) < 0$.

$$\begin{aligned}
\frac{1}{n} Sup_{([x],[y])\in X} \mathbb{E}\left(s(S_n,(x,y))\right) &\leq \frac{1}{n} Sup_{([x],[y])\in X} \mathbb{E}\left(\log \frac{||\bigwedge^2 S_n x \wedge y||}{||x \wedge y||}\right) + \\
&\quad \frac{2}{n} Sup_{[x]\in P(V)} \mathbb{E}\left(\log \frac{||x||}{||S_n x||}\right) \\
&\leq \frac{1}{n}\mathbb{E}(\log||\bigwedge^2 S_n||) + \frac{2}{n} Sup_{[x]\in P(V)} \mathbb{E}\left(\log \frac{||x||}{||S_n x||}\right) \qquad (2.18)
\end{aligned}$$

By definition of the Lyapunov exponent,

$$\frac{1}{n}\mathbb{E}(\log||\bigwedge^2 S_n||) \underset{n\to\infty}{\longrightarrow} \lambda_1 + \lambda_2$$

By (the proof of) Corollary 2.4.10,

$$\frac{1}{n} Sup_{[x]\in P(V)} \mathbb{E}\left(\log \frac{||x||}{||S_n x||}\right) \underset{n\to\infty}{\longrightarrow} -\lambda_1$$

Hence,

$$\lim \frac{1}{n} Sup_{([x],[y])\in X} \mathbb{E}\left(s(S_n,(x,y))\right) \underset{n\to\infty}{\longrightarrow} \lambda_2 - \lambda_1$$

Under the contraction and strong irreducibility assumptions on Γ_μ, this is negative by Theorem 2.4.6. □

We deduce the following

Theorem 2.4.16 (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 ν (resp. ν^*), the unique μ-invariant probability measure on $P(V)$ (resp. μ^{-1}-invariant on $P(V^*)$) such that for some $\lambda > 0$ and every $\epsilon > 0$:*

$$Sup_{[x]\in P(V)}\, \mathbb{E}\left(\delta(M_n[x], Z_1)^\epsilon\right) \leq (1-\lambda\epsilon)^n \tag{2.19}$$

$$Sup_{[f]\in P(V^*)}\, \mathbb{E}\left(\delta(S_n^{-1}\cdot[f], Z_2)^\epsilon\right) \leq (1-\lambda\epsilon)^n \tag{2.20}$$

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

Proof. It suffices to prove (2.19). Indeed, (2.20) is the consequence of the fact that the action of Γ_μ on V is strongly irreducible and contracting if and only if the action of $\Gamma_{\mu^{-1}}$ on V^* is. Moreover, if (2.19) and (2.20) hold then $M_n[x]$ (resp. $S_n^{-1}\cdot[f]$) 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 2.4.5. 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 :

$$\mathbb{E}\left(\delta(M_n[x], Z)^\epsilon\right) \leq \underbrace{\mathbb{E}\left(\delta(M_n[x], M_k[y])^\epsilon\right)}_{(I)} + \mathbb{E}\left(\delta(M_k[y], Z)^\epsilon\right) \tag{2.21}$$

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

$$\begin{aligned}(I) &= \int d\mu^{k-n}(\gamma)\, \mathbb{E}\left(\delta(M_n[x], M_n[\gamma y])^\epsilon\right) \\ &\leq Sup_{[a],[b]}\, \mathbb{E}(\delta(M_n[a], M_n[b])^\epsilon) \leq (1-\lambda\epsilon)^n \end{aligned} \tag{2.22}$$

Inserting (2.22) in (2.21) gives for every $[y] \in P(V)$, $k > n \geq n_0$:

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

Let ν be the unique μ-invariant probability measure on $P(V)$ (see Theorem 2.4.5). Integrating with respect to $d\nu([y])$ the two members of the previous inequality and applying Fubini theorem, we get for every $k > n \geq n_0$:

$$Sup_{[x]}\mathbb{E}(\delta(M_n[x], Z)^\epsilon) \leq (1-\lambda\epsilon)^n + \mathbb{E}\left(\int \delta([y], Z)^\epsilon\, d(M_k\nu)([y])\right) \tag{2.23}$$

Again by Theorem 2.4.5, a.s. $M_k\nu$ converges weakly towards the Dirac measure δ_Z when k goes to infinity. For w fixed and every $0 < \epsilon \leq 1$, $\delta(\,\cdot\,, Z(\omega))^\epsilon$ is a continuous function on $P(V)$. Hence, $\int \delta([y], Z)^\epsilon\, d(M_k\nu)([y])$ converges a.s. to $\delta(Z, Z)^\epsilon = 0$ when k goes to infinity. By the dominated convergence theorem, $\mathbb{E}\left(\int \delta([y], Z)^\epsilon\, d(M_k\nu)([y])\right) \underset{k\to\infty}{\longrightarrow} 0$. We conclude by letting k go to infinity in (2.23). Since $\epsilon \mapsto \delta(\cdot,\cdot)^\epsilon$ is decreasing, the corollary is true for every $\epsilon > 0$. □

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 ν, under contraction and strong irreducibility assumptions :

Theorem 2.4.17. *[Gui90] $k = \mathbb{R}$. Consider the same assumptions as in Proposition 2.4.15, then there exists $\alpha > 0$ such that :*

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

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

$$Sup\{ \mathbb{P}(\delta(Z, H) \leq \epsilon); \quad H \text{ hyperplane of } V\} \leq C\epsilon^{\alpha} \tag{2.24}$$

(2.24) gives in particular <u>for $k = \mathbb{R}$</u> : for every $0 < t < 1$:

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

The latter assertion will be important for us. Proving Theorem 2.4.17 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 2.4.17. Instead we give a direct proof of the last assertion, using our "weak large deviation" - Proposition 2.4.14.

Theorem 2.4.18. *Consider the same assumptions as in Proposition 2.4.15. Let Z be a random variable with law ν, the unique μ-invariant probability measure. Then, for all $t \in]0, 1[$,*

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

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

Lemma 2.4.19. *There exists a constant $C(k)$ such that for every $f \in V^*$, a.s. there exists $i = i(n, \omega) \in \{1, \cdots, d\}$ such that : $|f(M_n e_i)| \geq C(k)||M_n^{-1} \cdot f||$*

Proof. When k in archimedean, a.s. $||M_n^{-1} \cdot f||^2 = \sum_{i=1}^d |M_n^{-1} \cdot f(e_i)|^2$. Take $C(k) = \frac{1}{\sqrt{d}}$. When k in non archimedean, the norm on V^* is ultrametric. Hence, a.s. $||M_n^{-1} \cdot f|| = Max\{|M_n^{-1} \cdot f(e_i)|;\ i = 1, \cdots, d\}$. The lemma is then valid for $C(k) = 1$. □

Proof of Theorem 2.4.18. 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 "$\{||f(M_n e_i)|| \geq C(k)||M_n^{-1} \cdot f||\}$". By the previous lemma, $\mathbb{P}(\cup_{i=1}^d A_i) = 1$. Hence,

$$\mathbb{P}(\delta(Z, [H]) \leq t^n) \leq \sum_{i=1}^{d} \mathbb{P}(\delta(Z, [H]) \leq t^n;\ \mathbb{1}_{A_i}) \tag{2.25}$$

By Theorem 2.4.16, there exists $\rho_1 \in]0,1[$ such that for all large n :

$$Sup_{[x]\in P(V)}\, \mathbb{E}\left(\delta(M_n[x], Z)\right) \leq \rho_1^n$$

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

$$\mathbb{P}\left(\delta(M_n[x], Z) \geq \rho_2^n\right) \leq (\frac{\rho_1}{\rho_2})^n; \;\; \forall x \in V \setminus \{0\} \tag{2.26}$$

On each event A_i, we apply inequality (2.26) for $x = e_i$. Inserting this in (2.25) and using the triangle inequality, we get :

$$\mathbb{P}\left(\delta(Z,[H]) \leq t^n\right) \leq \sum_{i=1}^{d} \mathbb{P}\left(\delta(M_n[e_i],[H]) \leq \rho_2^n + t^n;\; \mathbb{1}_{A_i}\right) + \; d(\frac{\rho_1}{\rho_2})^n \tag{2.27}$$

On the event A_i,

$$\delta(M_n[e_i],[H]) = \frac{|f(M_n e_i)|}{||M_n e_i||} \geq C(k)\frac{||M_n^{-1}\cdot f||}{||M_n e_i||} \tag{2.28}$$

Inserting (2.28) in (2.27) gives :

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

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

$$\limsup_{n\to\infty} \left[\mathbb{P}(\frac{||M_n^{-1}\cdot f||}{||M_n x||} \leq a^n)\right]^{\frac{1}{n}} < 1 \tag{2.29}$$

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 2.4.14 by replacing $S_n = X_n \cdots X_1$ with $M_n^{-1} = X_n^{-1}\cdots X_1^{-1}$, V with V^*. If ρ^* denotes the contragredient representation of G on V^*, then for any $a \in]0,1[$,

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

uniformly in x and f. Since $\rho^*(M_n^{-1})$ is just the transpose matrix of M_n, $||M_n x|| \leq ||M_n|| = ||\rho^*(M_n^{-1})||$. Then (2.29) is valid uniformly in x and f.

□

2.4.3 Preliminaries on algebraic groups

Till the end of the paper, k is a local field, $\mathbf{G}$ is a k-algebraic group, $G = \mathbf{G}(k)$ are the k-points of $\mathbf{G}$. **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 $\mathbf{H}$ 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, $\mathbf{G}$ 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 $\mathbf{A}$ be a maximal k-torus of $\mathbf{G}$, $\mathbf{X}(\mathbf{A})$ be the group of k-rational characters of $\mathbf{A}$, Δ be the system of roots of G restricted to $\mathbf{A}$, which consists of the common eigenvalues of $\mathbf{A}$ in the adjoint representation. We fix an order on Δ and denote by Δ^+ the system of positive roots, Π 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

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

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

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

Rational Representations of algebraic groups

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

• every weight χ of ρ different from χ_ρ is of the form : $\chi = \frac{\chi_\rho}{\prod_{\alpha\in\Pi}\alpha^{n_\alpha}}$, where $n_\alpha \in \mathbb{N}$ for every simple root α.

• Every $x \in V_{\chi_\rho}$ is fixed by the subgroup N.

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

Proposition 2.4.20. *[Tit71]For every $\alpha \in \Pi$, let w_α be the fundamental weight associated to α. Then the k-rational irreducible representation (ρ_α, V_α) of G whose highest weight is w_α (called fundamental representation) has a highest weight space of dimension one and satisfies $\Theta_{\rho_\alpha} = \{\alpha\}$.*

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

Proposition 2.4.21. *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 ρ 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 $\rho(A^+) \subset \{diag(a_1, \cdots, a_d); |a_1| \geq |a_i|\ \forall i \neq 1\}$, $\rho(N)$ 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 (ρ, 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 2.4.22. *[[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 $\rho(K)$ acts by isometries on V and $\rho(A)$ is symmetric (resp. Hermitian). The direct sum $V = \oplus_\chi V_\chi$ is good and $a \in A$ induces on each V_χ a homothety of ratio $\chi(a)$. When K is non archimedean, there exists a K-invariant ultrametric norm on V such that the V_χ's are in good direct sum. The action of $a \in A$ on V_χ is by homothety of ratio $\chi(a)$

Such a norm is said to be (ρ, A, K)-good.

Corollary 2.4.23. *Let (ρ, V) be a k-rational representation of G, χ_ρ 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 $x_\rho \in V_{\chi_\rho} \setminus \{0\}$,

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

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

Fubiny-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 δ on the projective space $P(V)$:

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

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

To simplify notations, for $i = 1, \cdots, d$, we denote by λ_i the following rational character of $A : (\lambda_1, \cdots, \lambda_d) \mapsto \lambda_i$. Simple roots are λ_i/λ_{i+1}, $i = 1, \cdots, d-1$. Positive roots are λ_i/λ_j, $1 \leq i < j \leq d$. The fundamental weight associated to $\alpha_i = \lambda_i/\lambda_{i+1}$ is $w_i = \lambda_1 \cdots \lambda_i$ and the representation ρ_{α_i} of Proposition 2.4.20 is just $\bigwedge^i V$. The expression of simple roots in terms of fundamental weights is :

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

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 2.3.2, we can also take the following other choice for A^+ : $A^+ = \{diag(a_1, \cdots, a_d);\ a_i \in]0; +\infty[;\ a_1 \geq \cdots \geq a_d > 0; \prod_{i=1}^d a_i = 1\}$ when $k = \mathbb{R}$ or $\mathbb{C}$ and $A^+ = \{diag(\pi^{n_1}, \cdots, \pi^{n_d});\ n_1 \leq \cdots \leq n_d;\ \sum_{i=1}^d n_i = 0\}$ when k is non archimedean. Let $B = (e_1, \cdots, e_d)$ be the canonical basis on V and $||\cdot||$ the canonical norm on V (see Section 2.4.2), 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.

2.4.4 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 μ be a probability measure on $G = \mathbf{G}(k)$ and ρ a k-rational irreducible representation of **G**. We assume Γ_μ to be Zariski dense. Recall that by [Bor91, Proposition 18.3] G is 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 χ_ρ be the highest weight for V, and r the number of non zero weights of V. We set $\chi_1 = \chi_\rho$, $\chi_2, \cdots, \chi_l$ ($l \in \{2, \cdots, r\}$) the weights adjacent to χ_1, i.e., such that $\chi_i = \chi_1$ or there is $\alpha \in \Theta_\alpha$ such that $\chi_i = \chi_1/\alpha$. We consider a (ρ, A, K)-good norm on V (for the basis of weights) given by Theorem 2.4.22 of the preliminaries.

Fix a Cartan (resp. Iwasawa) decomposition such that the sections $G \to KAK$ and $G \to KAN$ be measurable. For $g \in G$, we denote by $g = k(g)a(g)u(g)$ (resp. $g = \widetilde{k(g)}\widetilde{a(g)}\widetilde{n(g)}$) its Cartan (resp. Iwasawa) decomposition in $G = KA^+K = KAN$. When it comes to the random walk $S_n = X_n \cdots X_1$, we simply write $S_n = K_n A_n U_n$ (resp. $S_n = \widetilde{K_n}\widetilde{A_n}N_n$) for the KAK (resp. KAN) decomposition of S_n in G and set $\rho(A_n) = diag(a_1(n), \cdots, a_d(n))$; $\rho(\widetilde{A_n}) = diag(\widetilde{a_1(n)}, \cdots, \widetilde{a_d(n)})$.

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 2.4.24 (Exponential moment for algebraic groups)**.** *If μ is a probability measure on G, we say that μ has an exponential local moment if $i(\mu)$ (image of μ under i) has an exponential local moment (see Definition 2.2.9).*

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

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 2.4.26 (Comparison between KAK and KAN)**.** *Almost surely there exists a compact subset C of G such that for every $n \in \mathbb{N}^*$, $A_n \widetilde{A_n}^{-1}$ belongs to C. In particular, there exists a compact subset D of $GL(V)$ such that $\rho(A_n)\rho(\widetilde{A_n})^{-1}$ 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 $GL(\mathfrak{g})$ such that $Ad(A_n)Ad(\widetilde{A_n}^{-1})$ belongs to E. This is equivalent to show that almost surely $\frac{\alpha(A_n)}{\alpha(\widetilde{A_n})}$ is in a random compact subset of k for every $\alpha \in \Pi$. Indeed, we decompose α into fundamental weights : $\alpha = \prod_{\beta \in \Pi} w_\beta^{n_\beta}$; $n_\beta \in \mathbb{Z}$. Hence,

$$\frac{\alpha(A_n)}{\alpha(\widetilde{A_n})} = \prod_{\beta \in \Pi} \left(\frac{w_\beta(A_n)}{w_\beta(\widetilde{A_n})} \right)^{n_\beta} \tag{2.30}$$

By Theorem 2.4.22, for each $\beta \in \Pi$, there exists a representation (ρ_β, V_β) of G whose highest weight is w_β and highest weight space is a line, say $k\, x_\beta$. Fix a (ρ_β, A, K)-good norm on V_β. Corollary 2.4.23 applied to the representation ρ_β gives then :

$$||\rho_\beta(S_n)|| = |w_\beta(A_n)| \ ; \ \frac{||\rho_\beta(S_n)x_\beta||}{||x_\beta||} = |w_\beta(\widetilde{A_n})|$$

Then (2.30) becomes then

$$\left|\frac{\alpha(A_n)}{\alpha(\widetilde{A_n})}\right| = \prod_{\beta \in \Pi} \left(\frac{||\rho_\beta(S_n)||}{\frac{||\rho_\beta(S_n)x_\beta||}{||x_\beta||}} \right)^{n_\beta} \tag{2.31}$$

It suffices to control the terms where $n_\beta \geq 0$. Since G is Zariski-connected, ρ_β is in fact strongly irreducible. By Zariski density, $\rho_\beta(\Gamma_\mu)$ also. Hence we can apply Proposition 2.4.9 :

$$\text{a.s.} \qquad Sup_{n\in\mathbb{N}^*} \frac{||\rho_\beta(S_n)||}{\frac{||\rho_\beta(S_n)x_\beta||}{||x_\beta||}} < \infty$$

This is what we want to show. □

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

Proposition 2.4.27 (Comparison between KAK and KAN in expectation)**.** *Assume that μ has an exponential local moment (Definition 2.4.24). 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 $\alpha \in \Pi$:*

$$\mathbb{E}\left(\left|\frac{\alpha(A_n)}{\alpha(\widetilde{A_n})}\right|^\epsilon\right) \leq (1+\epsilon\gamma)^n \quad ; \quad \mathbb{E}\left(\left|\frac{\alpha(\widetilde{A_n})}{\alpha(A_n)}\right|^\epsilon\right) \leq (1+\epsilon\gamma)^n \tag{2.32}$$

Moreover,

$$\mathbb{E}(||\rho(A_n)\rho(\widetilde{A_n}^{-1})||^\epsilon) \leq (1+\epsilon\gamma)^n \tag{2.33}$$

Proof. Let $\epsilon > 0$ and $\alpha \in \Pi$. Let $\beta_1, \cdots, \beta_s$ be an order of the simple roots appearing in identity (2.31). Holder inequality (for s maps) applied to the same identity gives :

$$\mathbb{E}\left(\left|\frac{\alpha(A_n)}{\alpha(\widetilde{A_n})}\right|^\epsilon\right) \leq \prod_{i=1}^{s}\Big[\mathbb{E}\Big[\left(\frac{||\rho_{\beta_i}(S_n)||}{\frac{||\rho_{\beta_i}(S_n)x_{\beta_i}||}{||x_{\beta_i}||}}\right)^{\epsilon s n_{\beta_i}}\Big]\Big]^{\frac{1}{s}}$$

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 $i \in \{1, \cdots, s\}$ and let $\gamma > 0$. By Lemma 2.4.25, the image of μ under ρ_{β_i} has an exponential local moment. Moreover, as explained in the previous proposition, G being Zariski-connected, ρ_{β_i} is strongly irreducible. Consequently, we can apply Proposition 2.4.14 which shows that $\mathbb{E}\Big[\left(\frac{||\rho_{\beta_i}(S_n)||}{\frac{||\rho_{\beta_i}(S_n)x_{\beta_i}||}{||x_{\beta_i}||}}\right)^{\epsilon s n_{\beta_i}}\Big] \leq (1+\gamma\epsilon)^n$. Hence $\mathbb{E}\left(\left|\frac{\alpha(A_n)}{\alpha(\widetilde{A_n})}\right|^\epsilon\right) \leq (1+\gamma\epsilon)^n$. In the same way, we show the inequality on the right hand side of (2.32).
In particular, for every non zero weight χ of (ρ, V) different from χ_ρ, $\mathbb{E}\left([\chi(A_n)/\chi(\widetilde{A_n})]^\epsilon\right) \leq (1+\gamma\epsilon)^n$. Indeed, this follows from the expression $\chi = \chi_1 / \prod_{\alpha\in\Pi} \alpha^{s_\alpha}$ with $s_\alpha \in \mathbb{N}$ and the Holder inequality applied to (2.32). For $\chi = \chi_\rho$, a similar inequality holds because $\chi_\rho(A_n)/\chi_\rho(\widetilde{A_n}) = ||S_n||/||S_n x||$ for some (ρ, A, K)-good norm and every $x \in V_{\chi_\rho}$. This proves (2.33). □

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

Theorem 2.4.28 (Exponential contraction in KAN)**.** *Assume that μ has an exponential local moment and that $\rho(\Gamma_\mu)$ is contracting. Then there exists $\lambda > 0$, such that for every*

$\epsilon > 0$ small enough and all n large enough :

$$\mathbb{E}(|\frac{\widetilde{a_i(n)}}{\widetilde{a_1(n)}}|^{\epsilon}) \leq (1-\lambda\epsilon)^n \quad ; \quad i = 2, \cdots, d$$

We recall that $\widetilde{A_n}$ is the A-component of S_n in the Iwasawa decomposition of S_n in G and that $\widetilde{a_1(n)}, \cdots, \widetilde{a_d(n)}$ are the diagonal components of $\rho(\widetilde{A_n})$ in the basis of weights.

Remark 2.4.29. *When $k = \mathbb{R}$, no contraction assumption is needed. Indeed, by a theorem of Goldsheid-Margulis [GM89], a strongly irreducible semigroup Γ of $GL_d(\mathbb{R})$ is contracting if and only if its Zariski closure is. Hence $\rho(\Gamma_\mu)$ is contracting if and only if $\rho(G)$ is. But G is $\mathbb{R}$-split, hence the highest weight space of ρ is a line, thus ρ is contracting.*

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

Lemma 2.4.30. *[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 μ and s an additive cocycle on $G \times X$. Suppose that ν is a μ-invariant probability measure on X such that :*

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

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

Proof of Theorem 2.4.28. Without loss of generality, one can suppose $\Omega = G^{\mathbb{N}} = \{w = (w_i)_{i\in\mathbb{N}^*}; w_i \in G\}$, $\mathbb{P}$ the probability measure for which the coordinates w_i are independent with law μ and $\mathcal{F}$ the σ-algebra generated by the coordinate maps w_i.
Since ρ is contracting, V_{χ_ρ} 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 $\{\rho\left(a(\eta_n)\right); n \in \mathbb{N}\}$ is also contracting. V_{χ_ρ} is then a one dimensional subspace. Therefore, for some $\alpha \in \Theta_\rho$, $\frac{\widetilde{a_2(n)}}{\widetilde{a_1(n)}} = \frac{1}{\alpha(\widetilde{A_n})}$ and in general for $i \in \{2, \cdots, d\}$, $\frac{\widetilde{a_i(n)}}{\widetilde{a_1(n)}}$ is of the form $1/\prod_{\beta\in\Theta_\rho}\beta^{m_\beta}(\widetilde{A_n})$ with $m_\beta \in \mathbb{N}$ for every $\beta \in \Pi$. By Holder inequality, it suffices to treat the case where $\widetilde{a_i(n)}/\widetilde{a_1(n)} = 1/\alpha(\widetilde{A_n})$ for some $\alpha \in \Theta_\rho$. As in Proposition 2.4.26, we decompose α into fundamental weights : $\alpha = \prod_{i=1}^s w_{\beta_i}^{n_{\beta_i}}$, with $s \in \mathbb{N}^*$, $n_{\beta_i} \in \mathbb{Z}$ for every $i = 1, \cdots, s$. We denote $(\rho_{\beta_i}, V_{\beta_i})$ the fundamental representation associated to w_{β_i}. Using (2.31) of the same proposition, we get for every $i = 1, \cdots, s$ a (ρ_{β_i}, A, K)-good norm on V_i such that :

$$\mathbb{E}\left(|\frac{\widetilde{a_i(n)}}{\widetilde{a_1(n)}}|^{\epsilon}\right) = \mathbb{E}\Big(\Big[\prod_{i=1}^{s}\frac{||\rho_{\beta_i}(S_n)x_{\beta_i}||}{||x_{\beta_i}||}\Big]^{-\epsilon\, n_{\beta_i}}\Big) \leq Sup_{x\in X}\,\mathbb{E}\big[exp(-\epsilon s(S_n,x))\big]$$

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

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

To apply Lemma 2.4.12, we must verify that for some $\tau > 0$,

$$\mathbb{E}\left(exp(\tau sup_{x\in X}\,|s(X_1,x)|)\right) < \infty \tag{2.34}$$

and

$$\lim \frac{1}{n} Sup_{x\in X}\, \mathbb{E}(-s(S_n,x)) < 0 \tag{2.35}$$

By Lemma 2.4.25, there exists $\tau > 0$ such that for every $i = 1, \cdots, s$, $\mathbb{E}\left(||\rho_{\beta_i}(X_1)||^\tau\right) < \infty$. Holder inequality applied recursively ends the proof of (2.34). Now we concentrate on proving (2.35). Since $P(V_{\beta_i})$ is compact for every $i = 1, \cdots, s$, it suffices to show that for all sequences $\{x_{1,n}; n \geq 0\}, \cdots, \{x_{s,n}; n \geq 0\}$ converging to non zero elements of $V_{\beta_1}, \cdots, V_{\beta_s}$:

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

Fix such sequences $\{x_{1,n}; n \geq 0\}, \cdots, \{x_{s,n}; n \geq 0\}$. By Corollary 2.4.10 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 μ-invariant probability measure ν on X, which exists by compactness of X. Again by Corollary 2.4.10,

$$L = \lim_{n\to\infty} \frac{1}{n} s\left(S_n(\omega), x\right) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{s} n_{\beta_i} \log \frac{||\rho_{\beta_i}\left(S_n(\omega)\right) x_i||}{||x_i||} \quad \text{for } \mathbb{P}\otimes\nu \text{ - almost all } (\omega, x)$$

Consider the dynamical system $E = \Omega \times X$, the distribution $\eta = \mathbb{P}\otimes\nu$ on E, the shift $\theta : E \to E$, $((g_0, ...), x) \longmapsto ((g_1, ...), g_0 \cdot x)$. Since ν is μ-invariant, η is θ-invariant. We extend the definition domain of s from $G\times X$ to $G^{\mathbb{N}}\times X$ by setting $s(\omega, x) := s(g_0, x)$ if $\omega = (g_0, ...)$. Since μ 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 η-almost every (ω, x) to a random variable Y whose expectation is $\iint s(g,x)d\mu(g)d\nu(x)$. Since s is a cocycle, $s\left(S_n(\omega), x\right) = \sum_{i=0}^{n} s\circ\theta^i(\omega, x)$. Hence,

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

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 2.4.30 are fulfilled. Since μ has a moment of order one, condition (1) is readily satisfied.
Condition (2) : we must verify that for $\mathbb{P}\otimes\nu$-almost all (ω, x),

$$s\left(S_n(\omega), x\right) = \sum_{i=1}^{s} n_{\beta_i} \log \frac{||\rho_{\beta_i}\left(S_n(\omega)\right) x_i||}{||x_i||} \underset{n\to\infty}{\longrightarrow} +\infty \tag{2.36}$$

By Proposition 2.4.9, the $\mathbb{P}\otimes\nu$-almost everywhere behavior at infinity of $s\left(S_n(\omega), x\right)$ is the same as the $\mathbb{P}$-almost everywhere behavior of :

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

The last equality follows from the expression of α in terms of the fundamental weights and from Corollary 2.4.23. Hence, we reduced the problem to proving that $|\alpha(A_n)| \underset{n\to\infty}{\overset{a.s}{\longrightarrow}}$

$+\infty$ for every $\alpha \in \Theta_\rho$.
$\rho(\Gamma_\mu)$ is strongly irreducible because Γ_μ is Zariski dense in G, ρ is an irreducible representation of G and G is connected. Since by the hypothesis $\rho(\Gamma_\mu)$ is contracting, we can apply Theorem 2.4.5 :
$||\cdot||$ being (ρ, A, K)-good norm, $|a_1(n)| = ||\rho(S_n)||$. Hence a.s. every limit point of $\frac{\rho(S_n)}{a_1(n)}$ is a rank one matrix. In particular, $\frac{a_2(n)}{a_1(n)}, \cdots, \frac{a_d(n)}{a_1(n)}$ 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 χ in terms of χ_ρ, 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 2.4.31 (Exponential contraction in KAK)**.** *With the same hypotheses as in Theorem 2.4.28, there exists $\lambda > 0$ such that for all $\epsilon > 0$:*

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

Proof. Let $i \in \{2, \cdots, d\}$. 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

$$\frac{a_i(n)}{a_1(n)} = \frac{a_i(n)}{\widetilde{a_i(n)}} \times \frac{\widetilde{a_1(n)}}{a_1(n)} \times \frac{\widetilde{a_i(n)}}{\widetilde{a_1(n)}}$$

Fix $\gamma > 0$. By Propositions 2.4.27 and 2.4.28 and Holder inequality, we have for some $\lambda > 0$, every $0 < \epsilon < Min\{\epsilon(\gamma); \frac{1}{3\lambda}\}$ and $n > n(\gamma)$:

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

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 $\gamma = \frac{\sqrt{\lambda}}{2}$ for instance. □

We will see in Section 2.4.5 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 2.3.2). The following corollary will be useful. It is the analog of Theorem 2.4.31 for the KAK decomposition in $SL_d(k)$ (rather than in G).

Corollary 2.4.32 (Ratio in the A-component for the KAK decomposition of $SL_d(k)$)**.** *For $g \in SL_d(k)$, we denote by $g = \widehat{k(g)}\widehat{a(g)}\widehat{u(g)}$ an arbitrary but fixed Cartan decomposition of g in $SL_d(k)$ as described in Section 2.3.2. We write $\widehat{a(g)} = diag\left(\widehat{a_1(g)}, \cdots, \widehat{a_d(g)}\right)$ in the canonical basis of k^d. With this notations and with the same assumptions as in Theorem 2.4.28, we have for some $\lambda > 0$ and every $\epsilon > 0$,*

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

Proof. To simplify notations we omit ρ, so that G is seen as a linear algebraic subgroup of $SL_d(k)$. Let $S_n = K_n A_n U_n$ be the Cartan decomposition of S_n in G (Section 2.4.3) and $S_n = \widehat{K_n}\widehat{A_n}\widehat{U_n}$ its Cartan decomposition in $SL_d(k)$ (Section 2.3.2). Recall that A_n is a diagonal matrix $diag\,(a_1(n), \cdots, a_d(n))$ in the basis of weights while $\widehat{A_n}$ is a diagonal matrix $diag\left(\widehat{a_1(n)}, \cdots, \widehat{a_d(n)}\right)$ in the canonical basis of k^d. We will use the canonical basis and norm of k^d (Section 2.4.2).

Theorem 2.4.31 shows that for some $\lambda > 0$, every $\epsilon > 0$ and all large n,

$$\mathbb{E}\left(|\frac{a_i(n)}{a_1(n)}|^\epsilon\right) \leq (1-\gamma\epsilon)^n \quad ; \quad i = 2, \cdots, d \tag{2.37}$$

Since $K_n, \widehat{K_n}$ belong to compact subgroups in both decompositions, there exist $C_1, C_2 > 0$ such that for every n : $C_2||A_n|| \leq ||\widehat{A_n}|| \leq C_1||A_n||$ and $C_2||\bigwedge^2 A_n|| \leq ||\bigwedge^2 \widehat{A_n}|| \leq C_1||\bigwedge^2 A_n||$.

By the definition of the KAK decomposition in $SL_d(k)$, we have a.s. $||\widehat{A_n}|| = |\widehat{a_1(n)}|$ and $||\bigwedge^2 \widehat{A_n}|| = |\widehat{a_1(n)}\widehat{a_2(n)}|$. 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 ω there exists $i(\omega) \in \{2, \cdots, l\}$ 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

$$\mathbb{E}\left(|\frac{\widehat{a_2(n)}}{\widehat{a_1(n)}}|^\epsilon\right) = \mathbb{E}\Big[\left(\frac{||\bigwedge^2 S_n||}{||S_n||^2}\right)^\epsilon\Big] = \mathbb{E}\Big[\left(\frac{||\bigwedge^2 \widehat{A_n}||}{||\widehat{A_n}||^2}\right)^\epsilon\Big] \leq (C_1C_3^3/C_2^2)^\epsilon \sum_{i=2}^{d} E\left(|\frac{a_i(n)}{a_1(n)}|^\epsilon\right)$$

By (2.37), this is less or equal than $constant \times (1-\gamma\epsilon)^n$. Since $|\widehat{a_2(g)}| \geq |\widehat{a_i(g)}|$ for $i > 2$ and every $g \in SL_d(k)$, the proof is complete. □

Exponential convergence and asymptotic independence in KAK

We recall that the norm on V we are working with is (ρ, A, K)-good (it is the one given by Theorem 2.4.22). 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_χ. Let $(e_1, \cdots, e_d)$ 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_χ such that the norm induced becomes the Max norm. If $(e_1, \cdots, e_d)$ is the corresponding basis of V, then $||x|| = Max\{||x_i||; i = 1, \cdots, d\}$ for every $x = \sum_{i=1} x_i e_i \in V$.

Let $\rho^* : G \longrightarrow GL(V^*)$ be the contragredient representation of G on V^*, that is $\rho^*(g)(f)(x) = f\,(\rho(g^{-1})x)$ for every $g \in G$, $f \in V^*$, $x \in V$. For $g \in G$ and $f \in V^*$, $g \cdot f$ will simply refer to $\rho^*(g)(f)$. Consider the norm operator on V^*, it is easy to see that it is (ρ^*, 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 : $M_n = X_1 \cdots X_n$, $S_n = X_n \cdots X_1$ where $X_i; i \geq 1$ are independent random variables of law μ. 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 $\rho(A_n) = diag\,(a_1(n), \cdots, a_d(n))$ 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 2.4.33 (Exponential convergence in KAK)**.** *Suppose that μ has an exponential local moment and that $\rho(\Gamma_\mu)$ is contracting. Denote by x_ρ a highest weight vector (e_1 for example), then for all $\epsilon > 0$:*

$$\limsup_{n\to\infty} \left[\mathbb{E}(\delta(k(M_n)[x_\rho], Z_1)^\epsilon)\right]^{\frac{1}{n}} < 1 \;\; ; \;\; \limsup_{n\to\infty} \left[\mathbb{E}(\delta(U_n^{-1}\cdot[x_\rho^*], Z_2)^\epsilon)\right]^{\frac{1}{n}} < 1$$

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

Remark 2.4.34. *From the previous theorem, we deduce by applying the Borel Cantelli lemma that $k(M_n)[x_\rho]$ converges almost surely while $K_n[x_\rho] = k(S_n)[x_\rho]$ converges only in law. This can also be directly derived from Corollary 2.4.7.*

Remark 2.4.35. *When $k = \mathbb{R}$, we give in Chapter 3 another proof of Theorem 2.4.33. See Theorem 3.5.15.*

Proof of Theorem 2.4.33. 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 $S_n^{-1}\cdot[f]$, for every $[f] \in P(V^*)$, obtained by Theorem 2.4.16. Since for every $i = 1, \cdots, d$, $A_n^{-1}\cdot e_i^* = a_i(n)e_i^*$ and $S_n = K_n A_n U_n$, we have for every $f \in V^*$ of norm one, such that $e_1(K_n^{-1}\cdot f) \neq 0$,

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

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

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

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

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

$$\delta(U_n^{-1}\cdot[e_1^*], Z) \leq \frac{1}{|e_1(K_n^{-1}\cdot f)|}\left(\delta(S_n^{-1}\cdot[f], Z) + \sum_{i=2}^{d} O(|\frac{a_i(n)}{a_1(n)}|)\right) \tag{2.38}$$

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 $i = i(n,\omega) \in \{1, \cdots, d\}$, such that $|e_1(K_n^{-1}\cdot e_i^*)| \geq C(k)$. Indeed, in the non archimedean case, $1 = ||K_n\cdot e_1|| = Max\{|K_n\cdot$

$e_1(e_i^*)|; i = 1, \cdots, d\}$. Hence for some random $i = i(n,\omega)$, $|e_1(K_n^{-1}\cdot e_i^*)| = |K_n \cdot e_1(e_i^*)| = 1$ and in the archimedean case, $1 = ||K_n \cdot e_1|| = \sum_{i=1}^d |K_n \cdot e_1(e_i^*)|^2 = \sum_{i=1}^d |e_1(K_n^{-1} \cdot e_i^*)|^2$. Hence one can write for every $\epsilon > 0$:

$$\mathbb{E}(\delta(U_n^{-1} \cdot [e_1^*], Z)^\epsilon) \leq \sum_{i=1}^d \mathbb{E}\left(\delta(U_n^{-1} \cdot [e_1^*], Z)^\epsilon \; ; \; \mathbb{1}_{|e_1(K_n^{-1}\cdot e_i^*)| \geq C(k)}\right) \tag{2.39}$$

In (2.39), for every $i = 1, \cdots, d$, on the event "$|e_1(K_n^{-1}\cdot e_i^*)| \geq C(k)$", we apply (2.38) 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 :

$$\mathbb{E}(\delta(U_n^{-1} \cdot [e_1^*], Z)^\epsilon) \leq \frac{1}{C(k)} \sum_{i=1}^d \mathbb{E}\left(\delta(S_n^{-1} \cdot [e_i^*], Z)^\epsilon\right) + \frac{1}{C(k)} \sum_{i=2}^d \mathbb{E}(|\frac{a_i(n)}{a_1(n)}|^\epsilon) \tag{2.40}$$

Theorem 2.4.31 shows that : $\mathbb{E}(|\frac{a_i(n)}{a_1(n)}|^\epsilon)$ is sub-exponential for $i = 2, \cdots, d$.
Theorem 2.4.16 shows that for every $i = 1, \cdots, d$, $\mathbb{E}\left(\delta(S_n^{-1}.[e_i^*], Z)^\epsilon\right)$ is sub-exponential. In the same way, we show the exponential convergence of $k(M_n)[x_\rho]$. □

We have shown that $U_n^{-1} \cdot [x_\rho^*]$ converges a.s. and $K_n[x_\rho]$ in law. In the following theorem, we show that these two variables become independent at infinity, with exponential "speed". This is Theorem 2.1.5 from the introduction. We recall its statement.

Theorem 2.4.36 (Asymptotic independence in the KAK decomposition)**.** *With the same assumptions as in Theorem 2.4.33, there exist* ***independent random variables*** $Z \in P(V^*)$ *and* $T \in P(V)$ *such that for every* $\epsilon > 0$*, every* ϵ*-holder (real) function* ϕ *on* $P(V^*) \times P(V)$ *and all large* n *:*

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

where

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

Proof. Let $\epsilon > 0$. The analog of Theorem 2.4.33 for $U_n^{-1} \cdot [x_\rho^*]$ does not hold for $K_n[x_\rho]$ 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 :

$$\mathbb{E}\big[\delta\left(K_n[x_\rho] \; , \; k(X_n \cdots X_{\lfloor \frac{n}{2} \rfloor})[x_\rho]\right)^\epsilon\big] \leq \rho(\epsilon)^n \tag{2.41}$$

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

$$\mathbb{E}\big[\delta\left(K_n[x_\rho] \; , \; k(X_n \cdots X_{\lfloor \frac{n}{2} \rfloor})[x_\rho]\right)^\epsilon\big] = \mathbb{E}\big[\delta\left(k(M_n)[x_\rho] \; , \; k(M_{n-\lfloor \frac{n}{2} \rfloor+1})[x_\rho]\right)^\epsilon\big]$$

It suffices now to apply twice the first convergence of Theorem 2.4.33 and the triangle inequality.

Now let ϕ be an ϵ-holder function on $P(V^*) \times P(V)$, $(X'_n)_{n\in\mathbb{N}}$ increments with law μ independent from $(X_n)_{n\in\mathbb{N}}$. We similarly write $M'_n = X'_1 \cdots X'_n$.
Let $Z = \lim U_n^*[x_\rho]$ and $T = \lim k(M'_n)[x_\rho]$ (a.s. limits given by Theorem 2.4.33). **The random variables T and Z are in particular independent**. We write :

$$\mathbb{E}\left(\phi(U_n^{-1}\cdot[x_\rho^*], K_n[x_\rho])\right) - \mathbb{E}\left(\phi(Z,T)\right) = \Delta_1 + \Delta_2 + \Delta_3 + \Delta_4$$

where

$$\Delta_1 = \mathbb{E}\left(\phi(U_n^{-1}\cdot[x_\rho^*], K_n[x_\rho])\right) - \mathbb{E}\left(\phi(U_{\lfloor\frac{n}{2}\rfloor}^{-1}\cdot[x_\rho^*], K_n[x_\rho])\right)$$

$$\Delta_2 = \mathbb{E}\left(\phi(U_{\lfloor\frac{n}{2}\rfloor}^{-1}\cdot[x_\rho^*], K_n[x_\rho])\right) - \mathbb{E}\left(\phi(U_{\lfloor\frac{n}{2}\rfloor}^{-1}\cdot[x_\rho^*], k(X_n\cdots X_{\lfloor\frac{n}{2}\rfloor+1})[x_\rho])\right)$$

$$\Delta_3 = \mathbb{E}\left(\phi(U_{\lfloor\frac{n}{2}\rfloor}^{-1}\cdot[x_\rho^*], k(M'_{n-\lfloor\frac{n}{2}\rfloor})\cdot[x_\rho])\right) - \mathbb{E}\left(\phi(Z, k(M'_{n-\lfloor\frac{n}{2}\rfloor})[x_\rho]\right)$$

$$\Delta_4 = \mathbb{E}\left(\phi(Z, k(M'_{n-\lfloor\frac{n}{2}\rfloor})[x_\rho])\right) - \mathbb{E}\left(\phi(Z,T)\right)$$

In Δ_3, we have replaced $k(X_n\cdots X_{\lfloor\frac{n}{2}\rfloor+1})$ with $k(M'_{n-\lfloor\frac{n}{2}\rfloor})$ because, on the one hand they have the same law and on the other hand, the processes $k(X_n\cdots X_{\lfloor\frac{n}{2}\rfloor+1})$ and $U_{\lfloor\frac{n}{2}\rfloor}$ that appear in the last term of the right hand side of Δ_2 are independent.

• By Theorem 2.4.33, there exist $\rho_1(\epsilon), \rho_2(\epsilon) \in]0,1[$ such that : $|\Delta_1| \preceq ||\phi||_\epsilon\, \rho_1(\epsilon)^n + ||\phi||_\epsilon\, \rho_1(\epsilon)^{\frac{n}{2}}$; $|\Delta_3| \preceq ||\phi||_\epsilon\, \rho_1(\epsilon)^{\frac{n}{2}}$ and $|\Delta_4| \preceq ||\phi||_\epsilon\, \rho_2(\epsilon)^{\frac{n}{2}}$.

• By (2.41), $\Delta_2 \preceq ||\phi||_\epsilon\, \rho_3(\epsilon)^n$.

□

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

Recall that k is a local field, $\mathbf{G}$ a k-algebraic group, G its k-points which we assume to be k-split. We denote by $\mathbf{G}^0$ its Zariski-connected component which we assume to be semi-simple and by G^0 its k-points. Finally, ρ 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 2.4.3 except that **$\mathbf{G}$ 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 2.3.2 regarding the Cartan decomposition in $\mathbf{SL_d}$. We consider the canonical basis $(e_1, \cdots, e_d)$ and canonical norm on $V = k^d$ (see Section 2.4.2). For each $g \in SL_d(k)$, we denote by $g = k(g)a(g)u(g)$ an arbitrary but fixed Cartan decomposition in $SL_d(k)$ and write $a(g) = diag\left(a_1(g), \cdots, a_d(g)\right)$.
We consider a probability measure μ on G such that Γ_μ is Zariski dense in G. As usual, we denote by $S_n = X_n \cdots X_1$ the right random walk.

The aim of this section is to prove that the main results of Section 2.4.4 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 2.4.31 for the KAK decomposition in $SL_d(k)$.

Theorem 2.4.37. *Assume that the representation $\rho|_{G^0}$ is irreducible. Let μ be a probability measure on G having an exponential local moment (see Definition 2.4.24) and such that $\rho(\Gamma_\mu)$ is contracting. Then for every $\epsilon > 0$,*

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

Our next task will be to adapt the proof of Theorem 2.4.33 (exponential convergence in the KAK decomposition) and Theorem 2.4.36 (asymptotic independence in the KAK decomposition) to the Cartan decomposition of $SL_d(k)$. This can be done easily using Theorem 2.4.37. Indeed it will be sufficient to replace x_ρ, highest weight of ρ, 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 $\rho(S_n) = K_n A_n U_n$, we obtain :

Theorem 2.4.38. *With the same assumptions as in Theorem 2.4.37, there exist random variables $Z_1 \in P(V)$ and $Z_2 \in P(V^*)$ such that*

$$\limsup_{n\to\infty} \left[\mathbb{E}(\delta(k(M_n)[e_1], Z_1)^{\epsilon})\right]^{\frac{1}{n}} < 1 \;\; ; \;\; \limsup_{n\to\infty} \left[\mathbb{E}(\delta(U_n^{-1}\cdot[e_1^*], Z_2)^{\epsilon})\right]^{\frac{1}{n}} < 1$$

Theorem 2.4.39. *With the same hypotheses as in Theorem 2.4.37, 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 ϵ-holder (real) function ϕ on $P(V^*) \times P(V)$, every $n > n_0$ we have :*

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

where

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

Before proving Theorem 2.4.37, we give some easy but important facts.

Definition 2.4.40. *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 τ is almost surely finite : let π be the projection $G \to G/G^0$, τ 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 2.4.41. *If μ is a probability measure on G with an exponential local moment (see Definition 2.4.24), then the distribution η of S_τ also has an exponential local moment.*

Proof. We identify G with a closed subgroup of $GL_r(k)$. For every $\alpha > 0$:

$$\mathbb{E}\left(||S_\tau||^\alpha\right) = \sum_{k\in\mathbb{N}^*} \mathbb{E}\left(||S_k||^\alpha \; ; \; \mathbb{1}_{\tau=k}\right) \leq \sum_{k\in\mathbb{N}^*} \sqrt{\mathbb{E}(||S_k||^{2\alpha})}\,\sqrt{\mathbb{P}(\tau=k)} \tag{2.42}$$

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

$$\mathbb{E}(||S_k||^{2\alpha}) \leq (C^{\frac{1}{\alpha_0}})^{\alpha k} \quad ; \quad k \in \mathbb{N}^* \tag{2.43}$$

On the other hand, recall that τ 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 $\mathbb{P}(\tau > k)$ is exponentially decaying. In particular, there exists a constant $\lambda > 0$ such that

$$\mathbb{P}(\tau = k) \leq exp(-\lambda k) \tag{2.44}$$

Combining (2.42), (2.43) and (2.44) gives with $D = C^{\frac{1}{\alpha_0}}$:

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

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

Corollary 2.4.42. *Suppose that μ has an exponential local moment, $\rho|_{G^0}$ is irreducible and $\rho(\Gamma_\mu)$ is contracting. Then for every $\epsilon > 0$,*

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

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

• First we show that Γ_η is Zariski dense in G^0. We claim that $\Gamma_\eta = \Gamma_\mu \cap G^0$. Indeed, recall that Γ_η is the smallest closed semigroup (for the natural topology of $End_d(k)$ induced by that of k) in G^0 containing the support of η. Hence, $M \in \Gamma_\eta$ if and only if for every neighborhood O of M in G^0, $\mathbb{P}(\exists n \in \mathbb{N}^*; S_{\tau(n)} \in O) > 0$. 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, $\mathbb{P}(\exists n \in \mathbb{N}^*; S_n \in O) > 0$ or equivalently $\mathbb{P}(\exists n \in \mathbb{N}^*; S_{\tau(n)} \in O) > 0$. This shows indeed that $\Gamma_\eta = \Gamma_\mu \cap G^0$.

Since Γ_μ is Zariski-dense in G and G^0 is Zariski-open in G, we deduce that Γ_η is Zariski dense in G^0.
• Next, we show that $\rho(\Gamma_\eta)$ is contracting. Indeed, by Lemma 2.2.8, $\rho(\Gamma_\mu)$ 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 2.2.8, contracting.
In consequence, we are in the following situation : G^0 is the group of k-points of a connected algebraic group and η is a probability measure on G^0 such that the semigroup Γ_η is Zariski dense in G^0. Moreover, by Lemma 2.4.41, η has an exponential local moment. Finally $\rho|_{G^0}$ is an irreducible representation of G^0 such that $\rho|_{G^0}(\Gamma_\eta)$ is contracting. An appeal to Corollary 2.4.32 ends the proof. □

Lemma 2.4.43. *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 $\ell\lambda_1$, where λ_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 $n > n(\epsilon)$:

$$\mathbb{P}(|\frac{1}{n}\tau(n) - \ell| > \epsilon) \leq \rho(\epsilon)^n$$

Proof. The stopping time $\tau(n)$ is the sum of the independent, τ-distributed random variables $\{\tau(i+1)-\tau(i); i \geq 1\}$. By the usual strong law of large numbers, a.s. $\lim \frac{\tau(n)}{n} = \ell$, 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 2.4.44 below. To apply the latter, we should check that for some $\xi > 0$, $\mathbb{E}\left(exp(\xi\tau)\right) < \infty$. Indeed, by (2.44), there exists $\xi > 0$ such that for every $y \in \mathbb{R}_+ : \mathbb{P}(\tau > y) \leq exp(-\xi y)$. Hence, for every $t > 0$, write :

$$\begin{aligned}\mathbb{E}\left(exp(t\tau)\right) &= \int_0^\infty \mathbb{P}\left(exp(t\tau) > x\right)\, dx = 1 + \int_1^\infty \mathbb{P}\left(\tau > \frac{\log(x)}{t}\right)\, dx \\ &\leq 1 + \int_1^\infty exp(-\xi\frac{\log(x)}{t})\, dx\end{aligned}$$

The latter is finite as soon as $t < \xi$. □

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

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

Moreover, one can take $\phi(\epsilon) = Sup_{0<t<\xi}\{t\epsilon - \psi(t)\}$ where $\psi(t) = \log\left(\mathbb{E}\left[exp\left(t(X_1 - \mathbb{E}(X_1))\right)\right]\right)$.

Proof of Theorem 2.4.37. 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 ϵ. By definition of the KAK decomposition in $SL_d(k)$, what we want to prove is that for all $\epsilon > 0$ small enough

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

Let $n = \lfloor \frac{N}{\ell} \rfloor$, so that for $N \geq N_1(\epsilon') = \frac{l(l+\epsilon')}{\epsilon'}$, $\quad n(l-\epsilon') \leq N \leq n(l+\epsilon')$. 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 2.4.43, there exists $\rho(\epsilon') \in]0,1[$ such that $\mathbb{P}(A_n) \geq 1 - \rho(\epsilon')^n$. We have then :

$$\mathbb{E}\Big[\left(\frac{||\bigwedge^2 S_N||}{||S_N||^2} \right)^{\epsilon} \Big] \;\leq\; \mathbb{E}\left(\frac{||\bigwedge^2 S_N||^{\epsilon}}{||S_N||^{2\epsilon}} \mathbb{1}_{A_n} \right) + \mathbb{P}(\Omega \backslash A_n) \;\leq\; \underbrace{\mathbb{E}\left(\frac{||\bigwedge^2 S_N||^{\epsilon}}{||S_N||^{2\epsilon}}\, \mathbb{1}_{A_n} \right)}_{(I)} + \rho(\epsilon')^n$$

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

$$(I) \leq \underbrace{\mathbb{E}\left(\frac{||\bigwedge^2 (X_N \cdots X_{\tau(n)+1}\, S_{\tau(n)})||^{\epsilon}}{||X_N \cdots X_{\tau(n)+1} S_{\tau(n)}||^{2\epsilon}}\, \mathbb{1}_{N \geq \tau(n); A_n} \right)}_{(II)} + \underbrace{\mathbb{E}\left(\frac{||\bigwedge^2 (X_{N+1}^{-1} \cdots X_{\tau(n)}^{-1}\, S_{\tau(n)})||^{\epsilon}}{||X_{N+1}^{-1} \cdots X_{\tau(n)}^{-1}\, S_{\tau(n)}||^{2\epsilon}}\; ;\; \mathbb{1}_{N < \tau(n); A_n} \right)}_{(III)}$$

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

$$(II) \leq \mathbb{E}\left((||X_N|| \cdots ||X_{\tau(n)+1}||)^{2d\epsilon}\, \frac{||\bigwedge^2 S_{\tau(n)}||^{\epsilon}}{||S_{\tau(n)}||^{2\epsilon}}\; ;\; \mathbb{1}_{N \geq \tau(n); A_n} \right)$$

$$\begin{aligned}
(II)^2 &\leq \mathbb{E}\left((||X_N|| \cdots ||X_{\tau(n)+1}||)^{4d\epsilon}\; ;\; \mathbb{1}_{N \geq \tau(n);\, A_n} \right) \mathbb{E}\left(\frac{||\bigwedge^2 S_{\tau(n)}||^{2\epsilon}}{||S_{\tau(n)}||^{4\epsilon}} \right) && (2.45)\\
&= \sum_{k=0}^{\infty} \mathbb{E}\left((||X_N|| \cdots ||X_{k+1}||)^{4d\epsilon}\; ;\; \mathbb{1}_{N \geq k;\, A_n}\, \mathbb{1}_{\tau(n)=k} \right) \mathbb{E}\left(\frac{||\bigwedge^2 S_{\tau(n)}||^{2\epsilon}}{||S_{\tau(n)}||^{4\epsilon}} \right)\\
&\leq \sum_{k=n(l-\epsilon')}^{n(l+\epsilon')} \mathbb{E}\left((||X_N|| \cdots ||X_{k+1}||)^{4d\epsilon} \right) \mathbb{E}\left(\frac{||\bigwedge^2 S_{\tau(n)}||^{2\epsilon}}{||S_{\tau(n)}||^{4\epsilon}} \right) && (2.46)\\
&\leq \sum_{k=n(l-\epsilon')}^{n(l+\epsilon')} \Big[\mathbb{E}\left(||X_1||^{4d\epsilon} \right) \Big]^{|N-k|} \mathbb{E}\left(\frac{||\bigwedge^2 S_{\tau(n)}||^{2\epsilon}}{||S_{\tau(n)}||^{4\epsilon}} \right) && (2.47)
\end{aligned}$$

The bound (2.45) is obtained by the Cauchy-Schwartz inequality, (2.46) follows from the fact that on the event A_n, $\tau(n) \in [n(l-\epsilon'); n(l+\epsilon')]$. Finally (2.47) is due to the

sub-multiplicativity of the norm and the independence of $X_N, \cdots, X_{k+1}$.
Since μ has an exponential local moment, for ϵ small enough, $1 \leq \mathbb{E}\left(||X_1||^{4d\epsilon}\right) = C(\epsilon) < \infty$. Moreover, $n(l-\epsilon') < N < n(l+\epsilon')$, hence $\sum_{k=n(l-\epsilon')}^{n(l+\epsilon')} \left[\mathbb{E}\left(||X_1||^{4d\epsilon}\right)\right]^{|N-k|} \leq 2n\epsilon' C(\epsilon)^{2n\epsilon'} \leq C(\epsilon)^{3n\epsilon'}$, for $n \geq n(\epsilon')$ large enough. Hence,

$$(II)^2 \leq C(\epsilon)^{3n\epsilon'} \mathbb{E}\left(\frac{||\bigwedge^2 S_{\tau(n)}||^{2\epsilon}}{||S_{\tau(n)}||^{4\epsilon}}\right)$$

Finally, by Corollary 2.4.42, there exists $\rho(\epsilon) \in]0,1[$ such that for all n large enough :

$$\mathbb{E}\left(\frac{||\bigwedge^2 S_{\tau(n)}||^{2\epsilon}}{||S_{\tau(n)}||^{4\epsilon}}\right) = \mathbb{E}\left(\left|\frac{a_2(\rho(S_{\tau(n)}))}{a_1(\rho(S_{\tau(n)}))}\right|^{2\epsilon}\right) \leq \rho(\epsilon)^n$$

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

2.5 Proof of Theorem 2.2.11

In this section, we complete the proof of Theorem 2.2.11 and Corollary 2.1.2. For simplicity will assume that the subgroups Γ_μ and $\Gamma_{\mu'}$ in the statement of Theorem 2.2.11 are equal.

Now let μ be a probability measure on $SL_d(k)$ such that Γ_μ is a strongly irreducible and contracting closed subgroup. We denote by G the k-Zariski closure of Γ_μ 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 2.4.5 with this G and ρ the natural action of G on $V = k^d$. We use the same notation and conventions as in Section 2.3, regarding attracting points and repelling hyperplanes.

We will show that

$$\limsup_{n\to\infty} \frac{1}{n} \log\ \mathbb{P}\left(\langle S_n, S'_n\rangle \text{do not form a ping-pong pair}\right) < 0. \tag{2.48}$$

Applying lemma 2.3.1, this will end the proof of Theorem 2.2.11. It will follow from the following two propositions.

Proposition 2.5.1. *There exists $\epsilon \in]0,1[$ such that for every $r \in]\epsilon, 1[$:*

$$\limsup_{n\to\infty} \frac{1}{n} \log\ \mathbb{P}\left(S_n, S'_n \textit{are not } (\epsilon^n, r^n)\textit{- very proximal}\right) < 0$$

Proposition 2.5.2. *For every $t \in]0,1[$;*

$$\limsup_{n\to\infty} \frac{1}{n} \log\ \mathbb{P}\left(\delta(v_{S_n{}^{\pm 1}}, H_{S'_n{}^{\pm 1}}) \leq t^n\right)\ < 0$$

Proof of Proposition 2.5.1 : it will follow from Proposition 2.5.3 and Lemma 2.5.4. First, we recall Lemma 2.3.2 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 ϵ-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 $i = 2, \cdots, d$, to be the repelling hyperplane.
We deduce the following proposition :

Proposition 2.5.3. *There exists $\epsilon_0 \in]0,1[$ such that for every $\epsilon \in]\epsilon_0, 1[$,*

$$\limsup_{n\to\infty} \frac{1}{n} \log \mathbb{P}\left(S_n \text{ and } S'_n \text{ are not } \epsilon^n\text{- very contracting}\right) < 0$$

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 2.4.37 shows that there exists $\epsilon_1 \in]0,1[$ such that for all large n we have $\mathbb{E}\left(\left|\frac{a_2(n)}{a_1(n)}\right|\right) \leq \epsilon_1^n$.

By the Markov inequality, for every $\epsilon \in]\epsilon_1, 1[$,

$$\mathbb{P}\left(\left|\frac{a_2(n)}{a_1(n)}\right| \geq \epsilon^n\right) \leq (\frac{\epsilon_1}{\epsilon})^n$$

By Lemma 2.3.2, for every $\epsilon \in]\sqrt{\epsilon_1}, 1[$ we have $\mathbb{P}(S_n \text{ is not } \epsilon^n\text{- contracting}) \leq (\frac{\epsilon_1}{\epsilon^2})^n$.
• For the random walk (S_n^{-1}) : The assumption Γ_μ is a group implies that $\Gamma_{\mu^{-1}} = \Gamma_\mu = \Gamma$ so that the action of $\Gamma_{\mu^{-1}}$ on V is strongly irreducible and contracting. In consequence, we can apply the same reasoning as the previous paragraph by replacing μ with μ^{-1}. This gives $\epsilon_2 \in]0,1[$ such that for every $\epsilon \in]\sqrt{\epsilon_2}, 1[$, $\mathbb{P}(S_n^{-1} \text{ is not } \epsilon^n\text{- contracting})$ is sub-exponential.
Similarly if we denote by ϵ_3, ϵ_4 the quantities relative to S'_n and ${S'_n}^{-1}$, then it suffices to choose $\epsilon_0 = Max\{\sqrt{\epsilon_i}; i = 1, \cdots, 4\}$

□

Recall that for $g \in SL_d(k)$, $v_g = k(g)e_1$ and $H_g = \left[Span\langle u(g)^{-1}e_2, \cdots, u(g)^{-1}e_d\rangle\right]$.

Lemma 2.5.4. *For every $t \in]0,1[$,*

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

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 $H = Kerf$, $f \in V^*$ then for any non zero vector x of V, $\delta([x],[H]) = \frac{|f(x)|}{||f||||x||}$. Since $H_{S_n} = Ker(U_n^{-1} \cdot e_1^*)$, we must show that for every $t \in]0,1[$,

$$\limsup_{n\to\infty} \frac{1}{n} \log \mathbb{P}(||U_n^{-1} \cdot e_1^*(K_n e_1)|| \leq t^n) < 0 \tag{2.49}$$

• For every $\epsilon > 0$, let ψ_ϵ 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 ψ_ϵ is $\frac{1}{\epsilon}$-Lipschitz.
Note also that

$$\mathbb{1}_{[-\epsilon,\epsilon]} \leq \psi_\epsilon \leq \mathbb{1}_{[-2\epsilon,2\epsilon]} \tag{2.50}$$

• Let η be the function on $P(V) \times P(V^*)$ defined by $\eta([x],[f]) = \delta([x], Ker(f)) = \frac{|f(x)|}{||f||||x||}$.
We consider the following metric on $P(V) \times P(V^*) : d(([x],[f]),([y],[g])) = \delta([x],[y]) + \delta([f],[g])$ for every $[x],[y] \in P(V)$ and $[f],[g] \in P(V^*)$.
Let $C(k) = \sqrt{2}$ when k is archimedean and $C(k) = 1$ when k is non archimedean. We claim that η is $C(k)$-Lipschitz. Indeed, let $[x],[y] \in P(V)$, $[f],[g] \in P(V^*)$. By Lemma 2.5.5 below there exist suitable representatives $x, y \in V$, $f, g \in V^*$ in the unit sphere such that $||x-y|| \leq C(k)\delta([x],[y])$ and $||f-g|| \leq C(k)\delta([f],[g])$. But by the triangle inequality, $\left|\eta([x],[f]) - \eta([y],[g])\right| \leq ||f(x) - g(y)|| \leq ||f-g|| + ||x-y|| \leq C(k)\left(\delta([f],[g]) + \delta([x],[y])\right)$.
Define for $\epsilon > 0$, $\phi_\epsilon = \psi_\epsilon \circ \eta$. By the previous remarks, ϕ_ϵ is $\frac{C(k)}{\epsilon}$- Lipschitz.
Theorem 2.4.39 gives a $\rho \in]0,1[$ and independent random variables $Z \in V$ and $T \in V^*$ such that for every Lipschitz function ϕ on $P(V) \times P(V^*)$, and n large enough

$$\left|\mathbb{E}\left(\phi([K_n e_1],[U_n^{-1}.\cdot e_1^*])\right) - \mathbb{E}\left(\phi(Z,T)\right)\right| \leq ||\phi||\,\rho^n \tag{2.51}$$

where $||\phi||$ is the Lipschitz constant of ϕ as it was defined in Theorem 2.4.39.

Now we prove (2.49). For any $t \in]0,1[$

$$\begin{aligned}
\mathbb{P}(||U_n^{-1}\cdot e_1^*(K_n e_1)|| \leq t^n) &\leq \mathbb{E}\left(\phi_{t^n}([K_n e_1],[{U_n}^{-1}\cdot e_1^*])\right) && (2.52)\\
&\leq \mathbb{E}\left(\phi_{t^n}(Z,T)\right) + ||\phi_{t^n}||\,\rho^n && (2.53)\\
&\leq \mathbb{P}\left(\frac{|T(Z)|}{||T||||Z||} \leq 2t^n\right) + C(k)\frac{\rho^n}{t^n} && (2.54)\\
&\leq Sup\{\mathbb{P}\left(\delta(Z,[H]) \leq 2t^n\right);\ H \text{ hyperplane of } V\} + C(k)\frac{\rho^n}{t^n} && (2.55)
\end{aligned}$$

The bound (2.53) follows from (2.51), while (2.52) and (2.54) use (2.50). Finally to get (2.55) we used the independence of Z and T.
By Theorem 2.4.18, (2.55) is sub-exponential and the lemma is proved if $t > \rho$, a fortiori for every $t \in]0,1[$. Γ_μ being a group, the action of $\Gamma_{\mu^{-1}}$ 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. □

Lemma 2.5.5. *Let $C(k) = \sqrt{2}$ when k is archimedean and $C(k) = 1$ when k is not. Then for any $[x],[y] \in P(V)$, 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^*.

Proof. Let x and y be representatives of norm one of $[x]$ and $[y]$. When $k = \mathbb{C}$, denote by $< \cdot, \cdot >$ the canonical scalar product on k^d. 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 : $\delta([x],[y]) = Max\{|x_i y_j - x_j y_i|; i \neq j\}$. The norm being ultrametric, for any i, j, $|x_i y_j - x_j y_i| = |y_j(x_i - y_i) + y_i(y_j - x_j)| \leq ||x - y||$. Hence $\delta([x],[y]) \leq ||x - y||$. For the other inequality, we distinguish two cases :
• Suppose that there is an index m such that x_m and y_m are of norm one (i.e. in Ω_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, $\delta([x],[y]) \geq Max\{|x_i - y_i|;\ i \geq 2\} = ||x - y||$.
• Suppose that there is no index m such that x_m and y_m are of norm one. Let i_0 (resp. j_0) be an index such that x_{i_0} (resp. y_{j_0}) is invertible : such indices exist because x and y are on the unit sphere. $i_0 \neq j_0$ and neither x_{j_0} nor y_{i_0} is of norm one. Hence, $|x_{i_0} y_{j_0} - y_{i_0} x_{j_0}| = 1$ and $\delta([x],[y]) = 1 = ||x - y||$.

□

Proof of Proposition 2.5.2. 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 $(X_1, \cdots, X_n)$ and $(X'_1, \cdots, X'_n)$ are independent, hence

$$\begin{aligned} \mathbb{P}\left(\delta(v_{S_n}, H_{S'^{\pm 1}_n}) \leq t^n\right) &= \mathbb{P}\left(\delta\left(k(M_n)[e_1], H_{S'^{\pm 1}_n}\right) \leq t^n\right) && (2.56) \\ &\leq Sup\{\mathbb{P}\left(\delta\left(k(M_n)[e_1], H\right) \leq t^n\right);\ H \text{ hyperplane of } V\} && (2.57) \end{aligned}$$

By Theorem 2.4.38 and the Markov inequality, there exist $\rho_1, \rho_2 \in]0,1[$, a random variable Z in $P(V)$ such that :

$$\mathbb{P}\left(\delta(k(M_n)[e_1], Z) \geq \rho_1^n\right) \leq \rho_2^n \qquad (2.58)$$

(2.57), (2.58) and the triangle inequality give :

$$\mathbb{P}\left(\delta([v_{S_n}],[H_{S'_n}]) \leq t^n\right) \leq Sup\{\mathbb{P}\left(\delta(Z,[H]) \leq t^n + \rho_1^n\right);\ H \text{ hyperplane of } V\} + \rho_2^n$$

Theorem 2.4.18 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 2.5.3, $\Gamma_{\mu^{-1}}$ acts strongly irreducibly on V and contains a contracting sequence. □

Proof of Corollary 2.1.2. let $l \in \mathbb{N}^*$ and $(M_{n,1})_{n\in\mathbb{N}^*}, \cdots, (M_{n,l})_{n\in\mathbb{N}^*}$ be l independent random walks associated to μ. Propositions 2.5.1 and 2.5.2 give $\epsilon, r, \rho \in]0,1[$, $n_0 \in \mathbb{N}^*$ such that for every $n > n_0$ and $i, j \in \{1, \cdots, l\}$, $\mathbb{P}(A_{n,i,j}) \leq \rho^n$ 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, ϵ^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 ϵ^n-apart from the repelling hyperplane of $M_{n,j}^{\pm 1}$. Hence for every $l \in \mathbb{N}^*$ and $n > n_0$:

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

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

QI embedding of the free group $\langle M_n, M'_n \rangle$

Definition 2.5.6 (QI embedding)**.** *Let Γ be a finitely generated group, d_Γ the word metric for a finite symmetric generating set. A subgroup H is said to be quasi isometrically (QI) embedded in Γ, if there exists a constant C such that for any $h \in H$,*

$$d_H(1, h) \leq C d_\Gamma(1, h)$$

where 1 is the neutral element and d_H is the word metric in H for a certain finite generating set.

End of the proof of Theorem 2.1.1. We will prove the QI embedding part of equation (2.1). Let F be a symmetric generating set of Γ and $H_n = \langle M_n, M'_n \rangle$. The word metric d_Γ in Γ will be considered with respect to F while the word metric d_{H_n} in H_n will be considered with respect to the generating set $\{M_n, M'_n, {M_n}^{-1}, {M'_n}^{-1}\}$. Let (ρ, V) be the representation of Γ given by Theorem 2.2.14, d its dimension and denote $A = Max\{||\rho(s)||, s \in F\}$. By proposition 2.5.3, there exists $\epsilon \in]0, 1[$ such that the ping-pong players $a_n = \rho(M_n)$, $b_n = \rho(M'_n)$ and their inverse act on the complement of their repelling neighborhood by transformations that contract distances by a factor at least ϵ^n. By taking n large enough, we can assume that $\epsilon^n \leq \frac{1}{A}$. Hence if $h = w(a_n, b_n)$ is a reduced word w of length $d_{H_n}(1, h)$ in the free group $\langle M_n, M'_n \rangle$, then $\rho(h)$ will act on some open subset of the projective space $P(V)$ by contracting distances by a factor at least $(\frac{1}{A})^{d_{H_n}(1,h)}$. In particular, $Lip\,(\rho(h)) \geq A^{d_{H_n}(1,h)}$; where $Lip\,(\rho(h))$ is the bi-Lipschitz constant of $\rho(h)$ acting on $P(V)$, $Lip\,(\rho(h)) = Sup\{\left(\frac{\delta(\rho(h)x, \rho(h)y)}{\delta(x,y)}\right)^{\pm 1},\ x, y \in P(V)\}$, δ being the Fubini-Study distance on $P(V)$. On the other hand, for any $g \in SL_d(k)$, $Lip(g) \leq ||g||^{2d}$. Indeed, for every $x, y \in P(V)$, $\frac{\delta(gx,gy)}{\delta(x,y)} \leq ||\bigwedge^2 g||\ ||g^{-1}||^2 \leq ||g||^{2d}$ because $||\bigwedge^2 g|| \leq ||g||^2$ and $||g^{-1}|| \leq ||g||^{d-1}$ for every $g \in SL_d(k)$. Hence, $Lip\,(\rho(h)) \leq A^{2d \times d_\Gamma(1,h)}$. This shows that, $d_{H_n}(1, h) \leq 2d \times d_\Gamma(1, h)$. □

Definition 2.5.7. *Let Γ be a finitely generated group, F a finite symmetric generating set, H a subgroup of Γ, S a finite symmetric generating set of S. We define the compression factor of H by*

$$C(\Gamma, F, H, S) = Inf_{h\in H} \frac{|h|_\Gamma}{|h|_H}$$

where $|h|_\Gamma = d_\Gamma(1, h)$ and $|h|_H = \underset{h=b_{i_1}\cdots b_{i_s}}{Min} (|b_{i_1}|_\Gamma + \cdots + |b_{i_s}|_\Gamma)$ and the minimum is taken over all representations of h in the form $b_{i_1} \cdots b_{i_s}$ with $b_{i_j} \in S$, $1 \leq j \leq s$.

Remark 2.5.8. *We use the same notations as the proof before Definition 2.5.7. In the paper of Gilman, Miasnikov and Osin, the authors showed in [GMO10, Theorem 2.1 (2)] that the compression factor C_n of the subgroup H_n is bounded below by a (non random)*

constant independent of n. Let us prove that the same holds in our case. We suppose in this remark that the support of the probability measure μ is the finite symmetric generating set F of Γ. By the previous proof, we have a.s., for any $h \in H_n$, $(\frac{1}{\epsilon})^{nd_{H_n}(1,h)} \leq Lip\,(\rho(h)) \leq A^{2d|h|_\Gamma}$. But since $\langle M_n, M'_n \rangle$ is free (for n big enough), $|h|_{H_n} \leq Max\{|M_n|_\Gamma, |M'_n|_\Gamma, |{M_n}^{-1}|_\Gamma, |{M'_n}^{-1}|_\Gamma\} \times d_{H_n}(1,h) \leq nd_{H_n}(1,h)$. *We conclude that* $C_n \geq \frac{-\log(\epsilon)}{2d\log(A)}$.

2.6 Open problems and questions

- It would be interesting to give an effective bound of the exponential decay of the probability that two random walks do not generate a free subgroup (Theorem 2.1.1).
- A problem related to the first one : give an effective lower bound of the difference of the top two Lyapunov exponents $\lambda_1 - \lambda_2$ when strong irreducibility and proximality hold.
- Let Γ be a finitely generated linear group which is not virtually solvable. Fix a finite symmetric generating set S. Denote by B_n the ball of radius n for the word metric and μ_n the uniform probability measure on B_n. Is is true that there exist $c \in]0,1[$ such that for all large n :

  $$\mu_n\{(x,y) \in \Gamma^2; \langle x,y \rangle \text{ is free}\} \geq 1 - c^n$$

  In other terms, does Theorem 2.1.1 hold when one replaces the n^{th} convolution power μ^n of μ with the uniform probability measure μ_n ?

Chapitre 3

Transience des sous-variétés algébriques des groupes algébriques et application à la généricité de la Zariski densité

Transience of algebraic varieties in algebraic groups and application to generic Zariski density

Abstract

We study the transience of algebraic varieties in linear groups. In particular, we show that a "non elementary" random walk in $SL_2(\mathbb{R})$ escapes exponentially fast from every proper algebraic subvariety. We also treat the case where the random walk is on the real points of a semi-simple split algebraic group and show such a result for a wide family of random walks. As an application, we prove that generic subgroups (in some sense) of linear groups are Zariski dense.

Keywords: Transience, algebraic varieties, Zariski density, random matrix products, random walks, probability of return.

Sommaire

3.1 Introduction

One of the essential results in probability theory on groups is Kesten's theorem [Kes59] : the probability of return to identity of a random walk on a group Γ decreases exponentially fast if and only if Γ is non amenable. A natural question is to extend this to other subsets : for which subsets does the random walk escape with exponential rate ? Many authors has studied the case where the subset is a subgroup of Γ : see for example [Eym72], [Bek90] and in particular [DlHGCS99, Theorem 51] where it is shown that the probability that a random walk on Γ returns to a subgroup H decreases exponentially fast to zero if and only if the Scheirer graph of Γ/H is non amenable.
In this note we look at random walks on Zariski dense subgroups of algebraic groups (such as $SL_2(\mathbb{R})$) and we look at the escape from proper algebraic subvarieties. Such questions have an interest in their own right since they allow us to study the delicate behavior of the random walk but they have also been recently involved in other domains such as the theory of expander graphs. We are referring here among others to the works of Bourgain and Gamburd [BG08],[BG09], Breuillard and Gamburd [BG10] and Varju [Var]. In [BG10] for instance it is shown that there is an infinite set of primes p of density one, such that the family of all Cayley graphs of $SL_2(\mathbb{Z}/p\mathbb{Z})$ is a family of expanders. A crucial part of the proof is to take a random walk on $SL_2(\mathbb{Z}/p\mathbb{Z})$ and to show that the probability of remaining in a subgroup decreases exponentially fast to zero and uniformly. In [BG09, Corollary 1.1.] the following statement was established : consider a finitely generated subgroup of $SL_d(\mathbb{Z})$ $(d \geq 2)$ which is Zariski dense, the uniform probability measure on a finite symmetric generating set and $(S_n)_{n\in\mathbb{N}}$ the associated random walk, then for every proper algebraic variety $\mathcal{V}$ of $SL_d(\mathbb{C})$, $\mathbb{P}(S_n \in \mathcal{V})$ decreases exponentially fast to zero.
Kowalski [Kow08] and Rivin [Riv08] were interested in similar questions : for example they were able to estimate the probability that a random walk in $SL_d(\mathbb{Z})$ lies in the set of matrices with reducible characteristic polynomial. The techniques used by Kowalski and Rivin are arithmetic sieving ones.

In this article, we develop a more probabilistic approach allowing us to deal with random walks on arbitrary Zariski dense subgroups of semi-simple algebraic groups. In the particular case of $SL_2(\mathbb{R})$, we obtain (see Theorem 3.1.1) that a random walk whose measure generates a non-elementary subgroup escapes with probability tending to one exponentially fast from every algebraic variety. Our method relies on the theory of random matrix products developed in the 60's by Kesten and Furstenberg and in the 70's-80's by the French school : in particular Bougerol, Guivarc'h, Le Page and Raugi.

We also apply our techniques to generic Zariski density. Let Γ_1 and Γ_2 be two Zariski dense subgroups of $SL_d(\mathbb{R})$ $(d \geq 2)$. We prove in Theorem 3.7.4 that one can exhibit a probability measure on each of the subgroups such that two independent random walks will eventually generate a Zariski dense subgroup. We have proved in Chapter 2 that the latter subgroup is also free. This gives consequently a "probabilistic" version of the Tits alternative [Tit72].

All the random variables will be defined on a probability space $(\Omega, \mathcal{F}, \mathbb{P})$, the symbol

$\mathbb{E}$ will refer to the expectation with respect to $\mathbb{P}$ and "a.s." to almost surely. If Γ is a topological group, μ a probability measure on Γ, we define a sequence of independent random variables $\{X_n; n \geq 0\}$ with the same law μ. We denote for every $n \in \mathbb{N}^*$ by $S_n = X_n \cdots X_1$ the n^{th} step of the random walk.
First let us present the result we obtain for $SL_2(\mathbb{R})$. We will say that a probability measure μ on $SL_2(\mathbb{R})$ is non elementary if the group generated by its support is non elementary, i.e. Zariski dense in $SL_2(\mathbb{R})$ or equivalently not virtually solvable.

Theorem 3.1.1. *Let μ be a non elementary probability measure on $SL_2(\mathbb{R})$ having an exponential moment (see Section 3.5.1 for a definition of this notion). Then for every proper algebraic subvariety $\mathcal{V}$ of $SL_2(\mathbb{R})$,*

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

In particular, every proper algebraic subvariety is transient, that is a.s. S_n leaves $\mathcal{V}$ after some time.
More precisely, if P is a non constant polynomial equation in the entries of the 2×2 matrices of $SL_2(\mathbb{R})$, then there exists $\lambda > 0$ such that :

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

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

$$\limsup_{n\to\infty} \left[\mathbb{P}\left(\left|\frac{1}{n} \log |P(S_n)| - \lambda\right| > \epsilon\right)\right]^{\frac{1}{n}} < 1 \tag{3.1}$$

Theorem 3.1.1 is in fact a particular case of a more general statement : Theorem 3.1.2 below. If G is the group of real points of an algebraic group $\mathbf{G}$, m a Cartan projection (see Section 3.4), μ a probability measure on G, then the Kingman subadditive ergodic theorem allows us to define a vector $Liap(\mu)$ (see Definition / Proposition 3.5.8) in the Weyl chamber of G which is the almost sure limit of $\frac{1}{n}m(S_n)$.

Theorem 3.1.2. *Let $\mathbf{G}$ be a semi-simple algebraic group defined and split over $\mathbb{R}$*[1]*, $G = \mathbf{G}(\mathbb{R})$ its group of real points, Γ a Zariski dense subgroup of G, $\mathcal{V}$ a proper algebraic subvariety of $\mathbf{G}$ defined over $\mathbb{R}$, μ a probability on G with an exponential moment (see Section 3.5.1) such that its support generates Γ. Then, there exists a finite union of hyperplanes $H_1, \cdots, H_r$ in the Weyl chamber (see Section 3.4.1) depending only on $\mathcal{V}$ such that if $Liap(\mu) \notin H_1 \cup \cdots \cup H_r$ then,*

$$\limsup_{n\to\infty} \left[\mathbb{P}(S_n \in \mathcal{V})\right]^{\frac{1}{n}} < 1 \tag{3.2}$$

Probability measures, whose support generates Γ, satisfying the condition $Liap(\mu) \notin H_1 \cup \cdots H_r$ exist (See Lemma 3.5.12). A large deviation inequality similar to (3.1) holds as well.

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

Theorem 3.1.2 clearly implies Theorem 3.1.1 : indeed, everything we want to show is that the Lyapunov exponent associated to μ (see Definition 3.5.4) is non zero (positive). This is ensured by Furstenberg's theorem [Fur63].

Remark 3.1.3. *The number λ that appears in Theorem 3.1.1 or 3.1.2, should be seen as a generalization of the classical Lyapunov exponent (see Definition 3.5.4). In fact, it will be the Lyapunov exponent relative to the probability measure $\rho(\mu)$ where ρ is some rational representation of* $\mathbf{G}$.

Remark 3.1.4. *Our method doesn't allow us to estimate $\mathbb{P}(S_n \in \mathcal{V})$ when $Liap(\mu)$ belongs to the finite union of hyperplanes H_i defined by the variety $\mathcal{V}$. Example 2 of Section 3.2 illustrates this.*

Let us justify why we will look at the escape from algebraic subvarieties and not from C^1 submanifolds for instance. Kac and Vinberg proved in [VK67] (see also [Ben04]) that there exist discrete Zariski dense subgroups of $SL_3(\mathbb{R})$ preserving a C^1 (but not algebraic) manifold on the projective plane (in fact, such manifolds are obtained as the boundary of a divisible convex in $P^2(\mathbb{R})$). Let Γ be such a group, $\mathcal{C}$ such a manifold and $\mathcal{V} = \{x \in \mathbb{R}^3 \setminus \{0\}; [x] \in \mathcal{C}\} \cup \{0\}$ where $[x]$ denotes the projection of $x \neq 0$ on $P^2(\mathbb{R})$. Note that $\mathcal{V}$ is differentiable outside 0. Then, for every $x \in \mathcal{V}$, every $n \in \mathbb{N}$, $\mathbb{P}(S_n x \in \mathcal{V}) = 1$. By way of contrast, we show in the following statement that for proper algebraic subvarieties the latter quantity decreases exponentially fast to zero.

Theorem 3.1.5. *Let Γ be a Zariski dense subgroup of $SL_d(\mathbb{R})$ ($d \geq 2$), μ a probability measure with an exponential moment whose support generates Γ. Then for every proper algebraic subvariety $\mathcal{V}$ of $\mathbb{R}^d$, every non zero vector x of $\mathbb{R}^d$ we have :*

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

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

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

Theorem 3.1.6. *Let $\mathbf{G}$ be a semi-simple algebraic group defined over $\mathbb{R}$, G its group of real points assumed without compact factors, Γ a Zariski dense subgroup of G and μ a probability measure with an exponential moment whose support generates Γ. Then for every proper algebraic subgroup $\mathbf{H}$ of $\mathbf{G}$,*

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

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

The bound obtained by Varju is uniform over the subgroups. Unfortunately our bound in Theorem 3.1.6 is not.

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

Theorem 3.1.7. *Let G be the group of real points of a semi-simple algebraic group split over $\mathbb{R}$. Let Γ_1, Γ_2 be two Zariski dense subgroups of G. Then there exist probability measures μ_1 and μ_2 with an exponential moment whose support generate respectively Γ_1 and Γ_2 such that for some $c \in]0,1[$ and all large n,*

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

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

See Section 3.7 for the comparison of these results with Rivin's in [Riva].

Remark 3.1.8. *The fact that $\{w \in \Omega; \langle M_n(w), M_n{}'(w)\rangle$ is Zariski dense$\}$ is measurable will follow from Lemma 3.7.7.*

3.1.1 Outline of the paper

In order to prove Theorem 3.1.2 (or 3.1.5, 3.1.6), one can clearly suppose that $\mathcal{V}$ is a proper hypersurface (i.e. the common zeroes of one polynomial equation). We will do so in all the paper.

In Section 3.2, we provide two examples to explain the general idea of the proofs.

Section 3.3 is purely algebraic. To every proper algebraic hypersurface $\mathcal{V}$ of $\mathbf{G}$ we associate a rational real representation ρ of $\mathbf{G}$ such that $g \in \mathcal{V}$ is equivalent to : the matrix coefficients of $\rho(g)$ satisfy a linear condition "(L)". Thus we have "linearized" our variety. This can be seen as a generalization of the well-known Chevalley theorem (Theorem 3.3.3) concerning the particular case of subgroups.

In Section 3.4 we recall standard facts about semi-simple algebraic groups and their rational representations.

In Section 3.5 we give some additional results to the theory of random matrix products. They will be used in Section 3.6 in order to show that $\rho(S_n)$ may verify (L) only with a probability decreasing exponentially in n.

We consider a random walk on a Zariski dense subgroup Γ of the real points of a semi-simple algebraic group. First we define the Lyapunov vector, which is the normalized Cartan projection of the random walk. We recall in Theorem 3.5.9 that it belongs to the interior of the Weyl chamber. In lemma 3.5.12, we show that for every finite union

of hyperplanes in the Weyl chamber, one can always find a probability measure whose support generates Γ such that the Lyapunov vector does not belong to this union (this is the condition stated in Theorem 3.1.2).

Next, we will be interested in the behavior of the components of the random walk in the Cartan decomposition. In Theorems 3.5.13 and 3.5.15, we give new and shorter proof of the exponential convergence in the KAK decomposition we obtained in Chapter 2. Unlike Chapter 2 when we were working on an arbitrary local field, we will take advantage during the proofs of the fact that our matrices are real valued.

Theorem 3.5.13 shows the exponential decay of the ratio between the first two A-components of the random walk in the KAK decomposition. This is a version in expectation of the fact that the Lyapunov vector belongs to the interior of the Weyl chamber. The proof will follow easily from a large deviations theorem of Le Page in $GL_d(\mathbb{R})$. We note that we proved a similar result in Chapter 2 but with different techniques, the reason is that a large deviation result in an arbitrary local field is not present in the literature.

Theorem 3.5.15 establishes the exponential convergence of the K-parts.

In Section 3.6, we prove our mains results : Theorems 3.1.2, 3.1.5 and 3.1.6. The key is Theorem 3.6.1 which computes the probability that a random walk on a linear algebraic group verifies a linear condition on the matrix coefficients. No irreducibility assumptions are made, a genericity condition on the geometry of the Lyapunov vector is however needed.

Finally in Section 3.7, we apply Theorem 3.6.1 to prove Theorem 3.1.7. We compare our results with Rivin's in [Riva].

Acknowledgments I sincerely thank Emmanuel Breuillard and Yves Guivarc'h for fruitful discussions, remarks and advices. I thank also Igor Rivin for his interest and his comments.

3.2 Examples

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

3.2.1 Example 1

This example illustrates Theorem 3.1.5.
Let Γ be Zariski dense subgroup of $SL_3(\mathbb{R})$ ($SL_3(\mathbb{Z})$ for example). Consider a probability measure μ on $SL_3(\mathbb{R})$ with an exponential moment (see Section 3.5.1) whose support generates Γ. For example, if Γ is finitely generated, choose a probability measure whose

support is a finite symmetric generating set. Let $S_n = X_n \cdots X_1$ be the associated random walk. We write S_n in the canonical basis of $M_{3,3}(\mathbb{R})$:

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

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

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

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

Step 1 : Linearization of the algebraic hypersurface $\mathcal{V}$.

Let E be the vector space of homogenous polynomials on three variables X, Y, Z of degree 2. The group $SL_3(\mathbb{R})$ acts on E by the formula : $g \cdot P(X,Y,Z) = P\left(g^t(X,Y,Z)\right)$ where g^t is the transposed matrix of g when g is expressed in the canonical basis. Let us write down this representation. We will consider the basis $\{X^2, Y^2, Z^2, XY, XZ, XY\}$ of E.

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

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

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

where H is the hyperplane in E defined by $H = \{x = (x_i)_{i=1}^6 \in \mathbb{R}^6; x_1 + x_4 = 0\}$.
We say that we have linearized the hypersurface $\mathcal{V}$. This method generalizes easily and yields Lemma 3.3.2 which holds for arbitrary hypersurfaces.
Note that, for $x = e_1 - e_4$,

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

Random matrix products in $GL_6(\mathbb{R})$

We have now a probability measure $\rho(\mu)$, image of μ under ρ, on $GL_6(\mathbb{R})$ with an exponential moment. The smallest closed group $G_{\rho(\mu)}$ containing the support of $\rho(\mu)$ is a

Zariski dense subgroup of $\rho(SL_3(\mathbb{R}))$. One can verify that ρ is in fact $SL_3(\mathbb{R})$-irreducible. Since $SL_3(\mathbb{R})$ is Zariski connected, we deduce that $G_{\rho(\mu)}$ is a strongly irreducible (Definition 2.2.7) subgroup of $GL_6(\mathbb{R})$. Moreover, the group $\rho(SL_3(\mathbb{R}))$ contains clearly a proximal element, then by Goldsheid-Margulis theorem [GM89] (see Theorem 3.5.3 for the statement), the same applies for $G_{\rho(\mu)}$. We can now apply Theorem 2.4.18 and Theorem 2.4.16 which imply that :

$$\limsup \frac{1}{n} \log \mathbb{P}\left(\rho(S_n)x \in H\right) < 0 \tag{3.3}$$

uniformly on $x \in \mathbb{R}^6 \setminus \{0\}$. This is what we wanted to prove.
Recall that one of the main ingredients of the proof of (3.3) is the separation of the top two Lyapunov exponents of the probability measure $\rho(\mu)$ (see Definition 2.4.2).

Remark 3.2.1. *This method does not give an estimate of the growth of $Q(S_n)$ where Q is the polynomial that defines $\mathcal{V}$. We will see in the next section (Theorem 3.6.1) how such quantities can be estimated.*

3.2.2 Example 2

This example illustrates situations in which we are unable to obtain the exponential decrease of the probability of lying in a subvariety for all probability measures (see the statement of Theorem 3.1.2).
As in Example 1, consider a probability measure on $SL_3(\mathbb{R})$ with an exponential moment whose support generates a Zariski dense subgroup of $SL_3(\mathbb{R})$. Say that we would like to estimate the following probability :

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

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

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

Thus

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

where $x = e_1 \wedge e_2 + e_2$ and $H = \{x \in \mathbb{R}^6; x_1 + 2x_5 = 0\}$. Hence, we have linearized our variety $\mathcal{S}$ as in Example 1. The difference between these two examples is that the representation η is no longer irreducible (η_1 and η_2 are its irreducible sub-representations). Hence we cannot use Theorem 2.4.18 or Theorem 2.4.16.

However, we will see in the proof of Theorem 3.6.1 that we are able to solve the problem if the top Lyapunov exponents of $\eta_1(\mu)$ and $\eta_2(\mu)$ are distinct.
Let us calculate them. If λ_1, λ_2 are top two Lyapunov exponents of μ (see Definition 2.4.2 in Chapter 2), then the top Lyapunov exponent of $\eta_1(\mu)$ is $\lambda_1 + \lambda_2$ and the one corresponding to $\eta_2(\mu)$ is clearly λ_1. So the problem occurs when $\lambda_2 = 0$. This can happen for example when μ is a symmetric probability measure (i.e. the law of X_1 is the same as X_1^{-1}).
However, we can still find a probability measure whose support generates Γ such that $\lambda_2 \neq 0$, see Lemma 3.5.12.

3.3 Linearization of algebraic varieties

Let $\mathbf{G}$ be a semi-simple algebraic group defined on $\mathbb{R}$, G its group of real points.

The goal of this section is to linearize every algebraic hypersurface of $\mathbf{G}$. More precisely, for every proper algebraic hypersurface $\mathcal{V}$ defined over $\mathbb{R}$, we associate a finite dimensional rational real representation (ρ, V) of $\mathbf{G}$, a linear form L of $End(V)$ such that $\mathcal{V} = \{g \in \mathbf{G}; L(\rho(g)) = 0\}$. In fact, we will find a representation (ρ, V) of $\mathbf{G}$, a line D in V, a hyperplane H in V defined over $\mathbb{R}$ such that $\mathcal{V} = \{g \in \mathbf{G}; g \cdot D \subset H\}$ (see Lemma 3.3.2). This has to be seen as a generalization of the well-known Chevalley theorem for subgroups (see Theorem 3.3.3).

Definition 3.3.1 (Matrix coefficients)**.** *If (V, ρ) a finite dimensional representation of G, $\langle \cdot, \cdot \rangle$ a scalar product on V, we call $\langle \rho(g)v, w \rangle$ for $v, w \in V$ a matrix coefficient and we denote by $C(\rho)$ the span of the matrix coefficients of the representation ρ, thus a function $f \in C(\rho)$ can be written $L \circ \rho$ where L is a linear form on the vector space $End(V)$.*

Let $\rho_1, \cdots, \rho_r$ be independent $\mathbb{R}$-rational irreducible representations of $\mathbf{G}$. Any $f_1 \in C(\rho_1), \cdots, f_r \in C(\rho_r)$ are linearly independent provided that the representation ρ_i are pairwise non-isomorphic (see the proof of the Lemma 3.3.2 below). The set of elements of G where such a linear dependance is realized defines clearly an algebraic hypersurface of $\mathbf{G}$. The following lemma says also that each algebraic hypersurface can be realized in this way.

Lemma 3.3.2. *For every algebraic hypersurface $\mathcal{V}$ of $\mathbf{G}$ defined over $\mathbb{R}$, there exist a representation (ρ, V) of $\mathbf{G}$, a line D in V, a hyperplane H of V defined over $\mathbb{R}$ such that $\mathcal{V} = \{g \in \mathbf{G}; g \cdot D \subset H\}$. In particular, there exist a representation (ρ, V) of $\mathbf{G}$ **whose irreducible sub-representations**, say $\rho_1, \cdots, \rho_r$, **occur only once**, $f_1 \in C(\rho_1), \cdots, f_r \in C(\rho_r)$ such that :*

$$\mathcal{V}(\mathbb{R}) = \{g \in G; \sum_{i=1}^{r} f_i(g) = 0\} \tag{3.4}$$

$\mathcal{V}$ is proper if and only if at least one of the f_i's is non zero.
This is equivalent to say that there exists $A \in End(V_1) \oplus \cdots \oplus End(V_r)$ such that :

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

with $\mathcal{V}$ proper if and only if there exists $i = 1, \cdots, r$ such that the restriction of A to V_i is non zero. Here $Tr(M)$ denotes the trace of the endomorphism M.

Proof. Let $\mathbb{R}[\mathbf{G}]$ be the algebra of functions on $\mathbf{G}$, $\mathbf{G}$ acting on $\mathbb{R}[\mathbf{G}]$ by right translations : $g \cdot f(x) = f(xg)\ \forall g, x \in \mathbf{G}$, P the generator of the ideal vanishing on $\mathcal{V}$ (which is of rank one since $\mathcal{V}$ is a hypersurface). Then $g \in \mathcal{V} \Longleftrightarrow g \cdot P(1) = 0$. Consider the sub-representation $V = Vect(g \cdot P, g \in G)$. By [Hum75, Chapter 8, Proposition 8.6], V is a finite dimensional $\mathbb{R}$-rational representation of $\mathbf{G}$. When $\mathcal{V}$ is proper, the subspace $H = \{f \in V; f(1) = 0\}$ is a hyperplane defined over $\mathbb{R}$ so that $g \in \mathcal{V} \Longleftrightarrow g \cdot P \in H$ and the first part of lemma is proved. $\mathbf{G}$ being semi-simple, we decompose (ρ, V) into irreducible sub-representations : $V = \oplus_{i=1}^{r} V_i$. Decomposing P in the $V_i's$ gives easily (3.4) with the only difference that the $V_i's$ are not necessarily pairwise non isomorphic.

Suppose for instance that $V_1 \simeq V_2$. In this case, there exists an invertible matrix M such that $\rho_2(g) = M\rho_1(g)M^{-1}$ for every $g \in \mathbf{G}$. Let $f_i = L_i \circ \rho_i$ where L_i is a suitable linear form on $End(V_i)$ for $i = 1, 2$. Then $f_2 = \widetilde{L_2} \circ \rho_1$ where $\widetilde{L_2}$ is the linear form defined on $End(V_1)$ by $\widetilde{L_2}(h) = L_2(MhM^{-1})$, $h \in End(V_1)$. Consequently, f_2 can be seen in $C(\rho_1)$ so that $f_1 + f_2 \in C(\rho_1)$ and V_2 can be dropped. By updating r if necessary, we obtain (3.4). At least one of the f_i's is non zero, otherwise $\mathcal{V}$ would be $\mathbf{G}$.

• For the converse, we will show that if $\rho_1, \cdots, \rho_r$ are pairwise non isomorphic representations of $\mathbf{G}$, then any $(f_1, \cdots, f_r) \in C(\rho_1) \times \cdots \times C(\rho_r)$ are linearly independent. A simple argument using the Peter-Weyl theorem will immediately give the result for compact groups and a unitary trick will allow us to conclude.
If G were a compact Lie group, the proof would be a consequence of Peter-Weyl theorem for representations of compact groups (see for example [Kna86]) : let $\sum$ be the collection of all irreducible representations of G pairwise non isomorphic, $L^2(G)$ the set of all square integrable functions with respect to the Haar measure on G, then $\{\sqrt{dim(\rho)}\rho_{i,j};\ \rho \in \sum;\ 1 \leq i, j \leq dim(\rho)\}$ forms an orthonormal basis of $L^2(G)$, where $\rho_{i,j}$ denotes the function on G defined by $\rho_{i,j}(g) = \langle \rho(e_i), e_j \rangle$ for a certain basis $\{e_1, \cdots, e_{dim(\rho)}\}$ of the representation. We deduce immediately the linear independence of any $f_1, \cdots, f_r$, where $f_i \in C(\rho_i)$ for each i.
Now we return to the general case. If $\sum_{i=1}^{r} \lambda_i f_i(g) = 0$ for all $g \in G = \mathbf{G}(\mathbb{R})$ then by Zariski density, the same holds for all $g \in \mathbf{G}(\mathbb{C})$. We decompose the ρ_i's into $\mathbf{G}(\mathbb{C})$-irreducible representations. For sake of simplicity, we keep the notation f_i's to denote the new matrix coefficients that follow from this decomposition. The Lie algebra $\mathfrak{g}$ of $\mathbf{G}(\mathbb{C})$ has a compact real form $\mathfrak{g}_0$ (i.e. $\mathfrak{g}_0 \bigotimes_R \mathbb{C} = \mathfrak{g}$). To $\mathfrak{g}_0$ corresponds a subgroup G_0 of $\mathbf{G}(\mathbb{C})$ which is compact and Zariski sense in $\mathbf{G}(\mathbb{C})$. Hence an irreducible real representation of $\mathbf{G}(\mathbb{C})$ is G_0-irreducible. We conclude using the previous paragraph concerning Peter-Weyl theorem for compact groups. □

3.3.1 The particular case of subgroups

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

Theorem 3.3.3 (Chevalley). *[Hum75] Let $\mathbf{H}$ be a proper subgroup of $\mathbf{G}$, then there exist a rational representation (ρ, V) of $\mathbf{G}$, a line D in V such that $\mathbf{H} = \{g \in \mathbf{G}; g \cdot D = D\}$.*

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

Proposition 3.3.4. *[Bor91] Let $\mathbf{H}$ be a proper reductive subgroup of $\mathbf{G}$, then there exists a rational real representation (ρ, V) of $\mathbf{G}$, a non zero vector x of V such that $\mathbf{H} = \{g \in \mathbf{G}; g \cdot x = x\}$.*

The converse is true and is a theorem of Matsushima [Mat60] (see also [Arz08] for a recent proof).

3.4 Preliminaries on algebraic groups

3.4.1 The Cartan decomposition

Let $\mathbf{G}$ be a semi-simple algebraic group defined over $\mathbb{R}$, G its group of real points, $\mathbf{A}$ be a maximal $\mathbb{R}$-split torus of $\mathbf{G}$, $\mathbf{X}(\mathbf{A})$ be the group of $\mathbb{R}$-rational characters of $\mathbf{A}$, Δ be the system of roots of $\mathbf{G}$ restricted to $\mathbf{A}$, Δ^+ the system of positive roots (for a fixed order) and Π the system of simple roots (roots than cannot be obtained as product of two positive roots).
We consider the natural order on $\mathbf{X}(\mathbf{A})$: $\chi_1 > \chi_2$ if and only if there exist non negative integers $\{n_\alpha; \alpha \in \Pi\}$ with at least one non zero n_α such that $\frac{\chi_1}{\chi_2} = \prod_{\alpha \in \Pi} \alpha^{n_\alpha}$.
Finally define $A^\circ = \{a \in A; \chi(a) \in]0; +\infty[\ \forall \chi \in \mathbf{X}(\mathbf{A})\}$ and set

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

Then there exists a compact K of G such that

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

(see [Hel01, Chapter 9, Theorem 1.1])

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

3.4.2 Rational representations of algebraic groups

A reference for this section is [Hum75] and [Tit71]. If (ρ, V) is an $\mathbb{R}$-rational representation of $\mathbf{G}$ then $\chi \in X(\mathbf{A})$ is called a weight of ρ if it is a common eigenvalue of $\mathbf{A}$ under ρ. We denote by V_χ the weight space associated to χ which is $V_\chi = \{x \in V; \rho(a)x = \chi(a)x \ \forall \ a \in \mathbf{A}\}$. The following holds : $V = \oplus_{\chi \in X(\mathbf{A})} V_\chi$. Irreducible representations ρ are characterized by a particular weight χ_ρ called highest weight which has the following property : every weight χ of ρ different from χ_ρ is of the form $\chi = \frac{\chi_\rho}{\prod_{\alpha \in \Pi} \alpha^{n_\alpha}}$, where $n_\alpha \in \mathbb{N}$ for every simple root α. The V_χ's are not necessarily of dimension 1. When $\mathbf{G}$ is $\mathbb{R}$-split, V_{χ_ρ} is one dimensional. Recall that an element $\gamma \in GL_d(\mathbb{R})$ is called proximal if it has a unique eigenvalue of maximal modulus. A representation ρ of a group Γ is said to be proximal if the group $\rho(\Gamma)$ has a proximal element. Thus, we obtain

Lemma 3.4.1. *Every $\mathbb{R}$-rational irreducible representation of an $\mathbb{R}$-split semi-simple algebraic group is proximal*

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

Proposition 3.4.2. *[Tit71] For every $\alpha \in \Pi$, let w_α be the fundamental weight associated to α. Then, there exists an $\mathbb{R}$-rational representation (ρ_α, V_α) of $\mathbf{G}$ whose highest weight is a power of w_α and whose highest weight space V_{w_α} is one-dimensional. Moreover, $\Theta_{\rho_\alpha} = \{\alpha\}$*

We record below a basic fact about root systems ([Bou68]).

Proposition 3.4.3. *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 $\beta \in \Pi$.*

Mostow theorem [Mos73, §2.6] Let $G = KAK$ be the Cartan decomposition of G, (ρ, V) an irreducible rational real representation of $\mathbf{G}$. There exists a scalar product on V for which the elements of $\rho(K)$ are orthogonal and those of $\rho(A)$ are symmetric. In particular, the weight spaces are orthogonal with respect to it. The norm on V induced by this scalar product is qualified by "good".

3.4.3 Standard Parabolic subgroups and their representations

A reference for this section is [BT65, §4].
For every subset $\theta \subset \Pi$, denote $\mathbf{A}_\theta = \{a \in \mathbf{A}; \alpha(a) = 1 \forall \alpha \in \theta\}$ and let $\mathbf{L}_\theta$ be its centralizer in $\mathbf{G}$. Denote by $\mathfrak{g}$ the Lie algebra of $\mathbf{G}$ and for every $\alpha \in \Delta$ denote by $\mathbf{U}_\alpha$ the unique closed unipotent subgroup of $\mathbf{G}$ with Lie algebra : $\mathfrak{u}_\alpha = \mathfrak{g}_\alpha \oplus \mathfrak{g}_{2\alpha}$ where $\mathfrak{g}_{i\alpha} = \{X \in \mathfrak{g}; Ad(a)(X) = \alpha(a)^i X\ \forall a \in \mathbf{A}\}$.
Let $[\theta] \subset \Delta$ be the set of roots which can be written as integral combination of roots of θ. Denote by $\mathbf{U}_\theta$ the unipotent closed subgroup of $\mathbf{G}$ whose Lie algebra is

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

We set

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

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

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

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

The following lemma will be useful to us for the proof of Theorem 3.1.6.

Lemma 3.4.4. *Let (ρ, V) be a rational irreducible representation of $\mathbf{G}$ and consider $\theta \subset \Pi$. The line generated by every non zero vector x in the highest weight space of V is fixed by $\mathbf{P}_\theta$ if $\beta \notin \Theta_\rho$ for every $\beta \in \theta$. In particular, the line generated by any highest weight vector x_α of the representation (ρ_α, V_α) defined in Proposition 3.4.2 is fixed by the standard parabolic $\mathbf{P}_\theta$ whenever $\alpha \notin \theta$.*

Proof. Let χ_ρ be the highest weight of ρ. We look at the action of the Lie algebra $\mathfrak{g}$ on V. It is clear that $\mathfrak{g}_{-\beta} \cdot v \in V_{\chi_\rho - \beta}$ for every $v \in V_{\chi_\rho}$ and $\beta \in \Pi$. If $\beta \notin \Theta_\rho$, then $\chi_\rho - \beta$ is not a weight of ρ and hence $V_{\chi_\rho - \beta} = 0$. The last part of the lemma is just recalling that the representation ρ_α defined in Proposition 3.4.2 satisfies $\Theta_{\rho_\alpha} = \{\alpha\}$ □

3.5 Random matrix products - convergence in the Cartan decomposition

We will use in this section standard results in the theory of random matrix products. A nice reference is the book of Bougerol and La Croix [BL85].

3.5.1 Preliminaries

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

We consider the basis of weights of V and the "good norm" given by Mostow theorem (Paragraph 3.4.2). It induces a K-invariant norm on $\bigwedge^2 V$ and hence a K-invariant distance $\delta(\cdot,\cdot)$ on the projective space $P(V)$, called Fubini-Study distance, defined by : $\delta([x],[y]) = \frac{||x \wedge y||}{||x||||y||}; [x],[y] \in P(V)$.
We fix an orthonormal basis on each weight space V_χ, and for an element $g \in End(V)$, g^t will be the transpose matrix of g in this basis.

G is isomorphic to a Zariski closed subgroup of $SL_d(\mathbb{R})$ for some $d \in \mathbb{N}^*$ (see [Hum75]). Let i be such an isomorphism. We say way that μ has a moment of order one (resp. an exponential moment) if for some (or equivalently any) norm on $End(\mathbb{R}^d)$, $\int \log ||i(g)|| d\mu(g) < \infty$ (resp. for some $\tau > 0$, $\int ||i(g)||^\tau d\mu(g) < \infty$). Lemma 3.5.1 below shows that is indeed a well defined notion, i.e. the existence of a moment of order one or an exponential moment is independent of the embedding.

Lemma 3.5.1. *Let $G \subset SL(V)$ be the $\mathbb{R}$-points of a semi-simple algebraic group $\mathbf{G}$ and ρ a finite dimensional $\mathbb{R}$-algebraic representation of $\mathbf{G}$. If μ has a moment of order one (resp. an exponential moment) then the image of μ under ρ has also a moment of order one (resp. exponential moment).*

Proof. 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. □

Let us recall some definitions and well-known results.

Definition 3.5.2. *A subgroup Γ of $GL_d(\mathbb{R})$ is called strongly irreducible if and only if the identity component of its Zariski closure does not fix a proper subspace. It is called proximal if it contains a proximal element (see Section 3.4).*

The key result which prevents our results from being generalized to an arbitrary local field is Goldsheid-Margulis theorem we recall here

Theorem 3.5.3. *[GM89] Let $d \geq 2$. A strongly irreducible subgroup of $GL_d(\mathbb{R})$ is proximal if and only if its Zariski closure is.*

3.5.2 Geometry of the Lyapunov vector

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

Definition/Proposition 3.5.4 (Lyapunov exponent)**.** *If μ is a probability measure on $GL_d(\mathbb{R})$, $||\cdot||$ a matricial norm on $End(V)$, $S_n = X_n \cdots X_1$ the corresponding random walk, then the Lyapunov exponent L_μ is $L_\mu = \lim \frac{1}{n}\mathbb{E}(\log ||S_n||)$ which exists by simple application of the subadditive lemma.*
When μ have a moment of order one, the following a.s. limit holds $L_\mu = \lim \frac{1}{n} \log ||S_n||$. It can be proved via the Kingman subadditive ergodic theorem [Kin73].

A useful result will be the following

Proposition 3.5.5. *[BL85, Corollary 4 page 53] Let θ be a probability measure on $GL_d(\mathbb{R})$ with a moment of order one and such that $G_\theta := \overline{\langle Supp(\theta)\rangle}$ is strongly irreducible. Then for every sequence $\{x_n; n \geq 0\}$ of vectors in $\mathbb{R}^d$ converging to some non zero vector $x \in \mathbb{R}^d$, $\frac{1}{n} \log ||S_n x_n|| \xrightarrow[n\to\infty]{a.s.} L_\theta$.*

Remark 3.5.6. *We have checked in Corollary 2.4.10 of Chapter 2 that the almost sure limit of the previous Proposition 3.5.5 holds in an arbitrary local field.*

Remark 3.5.7. *In [BL85], the condition is made on the smallest closed sub-semi-group Γ_θ containing the support of θ. There is no difference taking Γ_θ or G_θ because they have the same Zariski closure. Hence if one is strongly irreducible than the other satisfies the same property. This remark applies also for later applications when proximality is envolved (see for example the statement of Theorem 3.6.5). This is due to Goldsheid-Margulis theorem (Theorem 3.5.3) which is special to the field of real numbers.*

Definition/Proposition 3.5.8 (Lyapunov vector)**.** *Suppose that μ has a moment of order one. Then the Lyapunov vector is the constant vector in the Weyl chamber $\mathfrak{a}^+$ of G (see Section 3.4.1) defined as the following a.s. limit :*

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

where m is the Cartan projection (Section 3.4.1).

Proof. Let $\alpha \in \Pi$. Express α in terms of the fundamental weights (Proposition 3.4.3), $\alpha = \prod_{\beta\in\Pi} w_\beta^{n_\beta}$ where $n_\beta \in \mathbb{Z}$ for every $\beta \in \Pi$. For every $\beta \in \Pi$, consider the rational real irreducible representation (ρ_β, V_β) given by Proposition 3.4.2 and a good norm on V_β (Paragraph 3.4.2). By the definition of ρ_β, there exists an integer l_β such that for every $n \in \mathbb{N}^*$, $||\rho_\beta(S_n)|| = w_\beta^{l_\beta}(A_n)$. Hence,

$$\frac{1}{n}\log\ \alpha(A_n) = \sum_{\beta\in\Pi} \frac{n_\beta}{l_\beta}\ \frac{1}{n}\log\ ||\rho_\beta(S_n)|| \tag{3.5}$$

By Definition/Proposition 3.5.4, $\lim \frac{1}{n}\log\ \alpha(A_n) \overset{a.s.}{=} \sum_{\beta\in\Pi} \frac{n_\beta}{l_\beta} L_{\rho_\beta(\mu)}$. Thus $Liap(\mu)$ is well defined. □

Theorem 3.5.9. *[GR85] Suppose that μ has a moment of order one. Then the Lyapunov vector $Liap(\mu)$ belongs to the interior of the Weyl chamber $\mathfrak{a}^+$, i.e. $\alpha\left(Liap(\mu)\right) > 0$ $\forall \alpha \in \Pi$.*

Remark 3.5.10. *When the local field in not $\mathbb{R}$, the Lyapunov vector does not necessarily belong to the interior of $\mathfrak{a}^+$. The reason is that Goldsheid-Margulis theorem (Theorem 3.5.3) is valid only over the real field.*

For the reader's convenience, we include a proof of Theorem 3.5.9.

Proof. The techniques we use are very similar to the proof of Theorem 2.4.28. Without loss of generality, one can suppose $\Omega = G^{\mathbb{N}} = \{w = (w_i)_{i\in\mathbb{N}^*}; w_i \in G\}$, $\mathbb{P}$ the probability measure for which the coordinates w_i are independent with law μ and $\mathcal{F}$ the σ-algebra generated by the coordinate maps w_i.
We want to show that for every $\alpha \in \Pi$, $l := \lim \frac{1}{n}\log\ \alpha(A_n) > 0$. By equation (3.5), l is the following constant : $l = \sum_{\beta\in\Pi} \frac{n_\beta}{l_\beta} L_{\rho_\beta(\mu)}$. Let $X = \prod_{\beta\in\Pi} P(V_\beta)$, s the application on $G \times X$ defined by :

$$s\left(g, ([x_\beta])_{\beta\in\Pi_\alpha}\right) = \sum_{\beta\in\Pi_\alpha} \frac{n_\beta}{l_\beta}\ \log\ \frac{||\rho_\beta(g)x_\beta||}{||x_\beta||}$$

It is immediate that s is an additive cocycle on $G \times X$ for the natural action of G on X. Since X is compact, one can choose a μ-invariant measure ν on X.
Consider the dynamical system $E = \Omega \times X$, the distribution $\eta = \mathbb{P} \otimes \nu$ on E, the shift $\theta : E \to E$, $((g_0, \cdots), x) \longmapsto ((g_1, \cdots), g_0 \cdot x)$. Since ν is μ-invariant, η is θ-invariant. We extend the definition domain of s from $G \times X$ to $G^{\mathbb{N}} \times X$ by setting $s(\omega, x) := s(g_0, x)$ if $\omega = (g_0, \cdots)$. Since μ has a moment of order one, Lemma 3.5.1 shows that the same holds for the image probability measure $\rho_\beta(\mu)$ for every $\beta \in \Pi$. Hence $s \in L_1(\eta)$. 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 η-almost every (ω, x) to a random variable Y whose expectation is $\iint s(g, x)d\mu(g)d\nu(x)$. Since s is a cocycle, $s\left(S_n(\omega), x\right) = \sum_{i=0}^{n} s \circ \theta^i(\omega, x)$. Hence,

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

But using Proposition 3.5.5, we see that a.s. $Y = l$ so that

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

By lemma 3.5.11 below, l is positive if for η-almost every (ω, x), $s(S_n(w), x) \underset{n\to\infty}{\longrightarrow} +\infty$. Again by Proposition 3.5.5, for η-almost every (w, x), $s(S_n(w), x)$ has the same behavior at infinity as the $\mathbb{P}$-almost everywhere behavior of

$$\sum_{\beta\in\Pi_\alpha} \frac{n_\beta}{l_\beta}\,\frac{1}{n}\log\,||\rho_\beta(S_n)|| = \log\,\alpha(A_n)$$

In consequence, it suffices to show that $\alpha(A_n) \underset{n\to\infty}{\overset{\text{a.s.}}{\longrightarrow}} +\infty$. Indeed, the representation ρ_α is strongly irreducible because G is Zariski connected. By Zariski density of Γ, the same holds for $\rho_\alpha(\Gamma)$. Moreover, by Goldsheid-Margulis Theorem (Theorem 3.5.3) , $\rho_\alpha(\Gamma)$ is also proximal. By [BL85, Theorem 3.1 page 50], a.s. every limit point of $\frac{\rho_\alpha(S_n)}{||\rho_\alpha(S_n)||}$ is a rank one matrix. Hence, if $\rho_\alpha(A_n) = diag\,(a_1(n), \cdots, a_d(n))$, then a.s. $a_2(n)/a_1(n)$ converges a.s. to zero. But $\Theta_{\rho_\alpha} = \{\alpha\}$ so that $\alpha(A_n) = a_1(n)/a_2(n) \underset{n\to\infty}{\longrightarrow} +\infty$. □

Lemma 3.5.11. *[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 μ and s an additive cocycle on $G\times X$. Suppose that ν is a μ-invariant probability measure on X such that :*
(i) $\iint s^+(g,x)d\mu(g)d\nu(x) < \infty$
(ii) For $\mathbb{P}\otimes\nu$-almost every (w,x), $\lim_{n\to\infty} s\,(X_n(w)\cdots X_1(w), x) = +\infty$.
Then s is in $L^1(\mathbb{P}\otimes\nu)$ and $\iint s(g,x)d\mu(g)d\nu(x) > 0$

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

Lemma 3.5.12. *Let Γ be a Zariski dense subgroup of G. Then for every finite union F of hyperplanes in $\mathfrak{a}$ (see Section 3.4.1 for the definition of $\mathfrak{a}$), there exist a probability measure μ on Γ with an exponential moment whose support generates Γ and whose Lyapunov vector $Liap(\mu)$ is not included in F. In consequence, if $(V_1,\rho_1),\cdots,(V_r,\rho_r)$ are pairwise non isomorphic irreducible representations of $\mathbf{G}$, then one can exhibit a probability measure μ whose support generates Γ, a permutation σ of $\{1,\cdots,r\}$ such that $L_{\rho_{\sigma(1)}(\mu)} > \cdots > L_{\rho_{\sigma(r)}(\mu)}$ (See Definition 3.5.4).*

Proof. We recall the definition of the Jordan projection. Every element $g\in G$ has a decomposition : $g = g_e g_h g_u$ with g_e elliptic (i.e. included in a compact subgroup), g_h hyperbolic (i.e. conjugated to an element $a(g)$ in A^+) and g_u unipotent commuting with g_h. The Jordan projection $j : G \longrightarrow \mathfrak{a}^+$ is defined by $\lambda(g) = \log a(g)$.
Y. Benoist proved in [Ben97] that the smallest cone l_Γ in $\mathfrak{a}^+$ containing $j(\Gamma)$ has a non empty interior. Moreover, he showed in [Ben00] that $j(\Gamma)$ fills completely l_Γ in the sense that every open cone in l_Γ contains an infinite elements of $j(\Gamma)$. We deduce that $j(\Gamma)$ cannot be supported on any finite union of hyperplanes in $\mathfrak{a}$.
Let now F be such a finite union of hyperplanes, $g\in\Gamma$ such that $j(g)\notin F$. The spectral radius formula shows that $\frac{1}{n}m(g^n) \underset{n\to\infty}{\longrightarrow} j(g)\notin F$ where m is the Cartan projection (Section 3.4). This is equivalent to say that the Dirac probability measure $\mu = \delta_g$ supported on $\{g\}$ satisfies $Liap(\mu)\notin F$.

Let us perturb μ on Γ, that this define a sequence of probability measure μ_n with an exponential moment whose support generates Γ such that μ_n converge weakly to μ , for example $\mu_n = (1-1/n)\mu + \eta/n$ where η is a probability measure with an exponential moment whose support generates Γ. It is easy to see (see for example [BL85, Corollary 7.3, page 72-73]) that the Lyapunov vector depends continuously on the probability measure so that $Liap(\mu_n)$ converge to $Liap(\mu)$. Hence, for n big enough, μ_n is a probability measure on Γ with $Liap(\mu_n) \notin F$.

Now we prove the last part of the lemma. Let $\rho_1, \cdots, \rho_r$ be r rational real irreducible representations of $\mathbf{G}$ and denote by χ_{ρ_i} the highest weight of ρ_i. Recall that the set Π of simple roots is a basis of the space $X(A)$ of the rational characters of A. Hence for every $i = 1, \cdots r$, there exist real numbers $\{n_{i,\alpha}; \alpha \in \Pi\}$ with at least one non zero number such that :

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

For every $i < j$, denote by $H_{i,j}$ the following hyperplane of $\mathfrak{a}$:

$$H_{i,j} = \{x \in \mathfrak{a}; \sum_{\alpha \in \Pi} n_{i,\alpha} \log \alpha(x) = \sum_{\alpha \in \Pi} n_{j,\alpha} \log \alpha(x)\}$$

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

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

□

3.5.3 Estimates in the A-part

The following theorem gives an estimates in the A-part of the Cartan decomposition of the random walk. It can be proved by the same techniques of Chapter 2 (see Theorem 2.4.31) where the theory of random matrix products is treated over an arbitrary local field. However, since we are working here in $\mathbb{R}$, we will use another route and apply the large deviation theorem of Le Page [LP82] in $GL_d(\mathbb{R})$ we recall below. First, let us state our result :

Theorem 3.5.13. *[Ratio in the A-component] Suppose that μ has an exponential moment then for every $\epsilon > 0$ and every non zero weight χ of ρ distinct from χ_ρ,*

$$\limsup_{n \to \infty} \left[\mathbb{E}[(\frac{\chi(A_n)}{\chi_\rho(A_n)})^\epsilon]\right]^{\frac{1}{n}} < 1 \tag{3.6}$$

Moreover, if ρ_1, ρ_2 are two irreducible rational real representations of $\mathbf{G}$ such that $L_{\rho_1(\mu)} > L_{\rho_2(\mu)}$ (Definition 3.5.4), then for every $\epsilon > 0$:

$$\limsup_{n \to \infty} \left[\mathbb{E}[(\frac{\chi_{\rho_2}(A_n)}{\chi_{\rho_1}(A_n)})^\epsilon]\right]^{\frac{1}{n}} < 1 \tag{3.7}$$

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

Theorem 3.5.14. *[LP82][Large deviations in $GL_d(\mathbb{R})$]*

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

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

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

Proof of Theorem 3.5.13. For every $\beta \in \Pi$, a similar large deviation inequality as in Theorem 3.5.14 holds for the quantity $\frac{1}{n}\log||\rho_\beta(S_n)||$ because ρ_β is strongly irreducible and $\rho_\beta(\mu)$ has an exponential moment by Lemma 3.5.1. Hence by equation (3.5) a large deviation inequality holds for $\frac{1}{n}\log\alpha(A_n)$ for every $\alpha \in \Theta$. Since $\chi_\rho/\chi = \prod_{\alpha\in\Pi}\alpha^{n_\alpha}$ for non-negative integers $\{n_\alpha; \alpha \in \Pi\}$, we get for $\lambda = -\sum_{\alpha\in\Pi} n_\alpha$ $\lim_{n\to\infty}\frac{1}{n}\log\ \alpha(A_n)$ and for every $\epsilon > 0$,

$$\limsup_{n\to\infty} \left[\mathbb{P}\left(\left|\frac{1}{n}\log\ \frac{\chi(A_n)}{\chi_\rho(A_n)} - \lambda\right| > \epsilon\right)\right]^{\frac{1}{n}} < 1 \tag{3.8}$$

By Theorem 3.5.9, $\lambda < 0$. Hence, by relation (3.8), there exists $\rho_1, \rho_2 \in]0,1[$ such that for all large n : $\mathbb{P}\left(\frac{\chi(A_n)}{\chi_\rho(A_n)} \geq \rho_1^n\right) \leq \rho_2^n$. Since $\chi(a) \leq \chi_\rho(a)$ for every $a \in A^+$, we get for every $\epsilon > 0$, $\mathbb{E}\left[\left(\frac{\chi(A_n)}{\chi_\rho(A_n)}\right)^\epsilon\right] \leq \rho_1^{\epsilon n} + \rho_2^n$. This shows (3.6).
By the same large deviation techniques, one can show (3.7). □

3.5.4 Estimates in the K-parts

Recall that we fix a measurable section of the Cartan decomposition $G \to KAK$ and the corresponding decomposition of the random walk S_n is denoted by $S_n = K_n A_n U_n$. Our next task is to prove the following theorem which gives the convergence in the K-parts of the Cartan decomposition of the random walk.
This result was proved in Chapter 2 (Theorem 2.4.33). We give here another proof special to archimedean fields.

Theorem 3.5.15. *[Exponential convergence of the K-components] Suppose that μ has an exponential moment and ρ is proximal. Let v_ρ be a highest weight vector. Then there exists a random variable Z on the projective space $P(V)$ such that for every $\epsilon > 0$:*

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

Here, for $M \in GL(V)$, we have denoted by M^t the transpose matrix of M with respect to the basis of weights. We recall that δ is the Fubini-Study distance (see the beginning of Section 3.5.1). A similar estimate holds if we replace U_n with $k(X_1 \cdots X_n)$ where $k(g)$ is the K-component of $g \in G$ for the fixed KAK decomposition in G.

Proof. Our proof is inspired by Goldsheid and Margulis proof of Oseledets theorem [LP82]. We recall that by Mostow theorem, there exists a scalar product $\langle\cdot\rangle$ on V such

that the weight spaces are orthogonal and K acts by isometries and that we choose an orthonormal basis in each weight space so that $\rho(K)\rho(K)^t$ is the trivial group.
For every $n \in \mathbb{N}^*$, every non zero weight χ, we denote by $Q_\chi(n)$ the orthogonal projection on the space $U_n^{-1}\cdot V_\chi = \rho(U_n)^t V_\chi$. In particular $Q_{\chi_\rho}(n)$ is the projection on the line $\mathbb{R}U_n^{-1}\cdot v_\rho$, where v_ρ is a highest weight vector (it is one-dimensional because ρ is proximal). We will show that for every $\epsilon > 0$ small enough :

$$\limsup_{n\to\infty} \left[\mathbb{E}(||Q_{\chi_\rho}(n) - Q_{\chi_\rho}(n+1)||^\epsilon)\right]^{\frac{1}{n}} < 1 \tag{3.9}$$

This ends the proof because if x and y are two non zero vectors of V and Q_x and Q_y are the orthogonal projections on the lines $\mathbb{R}x$ and $\mathbb{R}y$, then $||Q_x - Q_y|| \geq \frac{1}{2}\delta([x],[y])$, so that (3.9) would imply by the Markov property that $\{U_n^{-1}\cdot[v_\rho];\ n \geq 0\}$ is a.s. a Cauchy series in the projective space $P(V)$. Hence it converges to some variable Z. By Fatou lemma and the triangular inequality, we get for some $t = t(\epsilon) \in]0,1[$ and all large n : $\mathbb{E}\left(\delta(Z, U_n^{-1}\cdot[v_\rho])^\epsilon\right) \leq \liminf_{m\to\infty} \mathbb{E}\left(\delta(U_m^{-1}\cdot[v_\rho], U_n^{-1}\cdot[v_\rho])^\epsilon\right) \leq t^n$.
Now we prove (3.9). For every $n \in \mathbb{N}^*$, $\sum_\chi Q_\chi$ is the identity operator, where the sum is over all the non zero weights of (ρ, V). Moreover, two orthogonal projections commute, hence : $||Q_{\chi_\rho}(n) - Q_{\chi_\rho}(n+1)|| \leq \sum_{\chi\neq\chi_\rho} ||Q_{\chi_\rho}(n+1)Q_\chi(n)|| + ||Q_{\chi_\rho}(n)Q_\chi(n+1)||$.
Fix a weight $\chi \neq \chi_\rho$. First we show that $\mathbb{E}(||Q_{\chi_\rho}(n+1)Q_\chi(n)||^\epsilon)$ is sub-exponential for every $\epsilon > 0$ small enough. This is equivalent to prove that there exists $\eta \in]0,1[$ such that for all large n :

$$\mathbb{E}\left(\left[\sup_{x\in U_n^{-1}\cdot V_\chi; ||x||=1} |Q_{\chi_\rho}(n+1)(x)|\right]^\epsilon\right) \leq \eta^n$$

Let $x \in U_n^{-1}\cdot V_\chi$ of norm one and $y_n = Q_{\chi_\rho}(n+1)(x)$, i.e. the orthogonal projection of x on the line $U_{n+1}^{-1}\cdot V_{\chi_\rho}$. Now we evaluate $||S_{n+1}\cdot x||$ in two different ways. On the one hand,

$$||S_{n+1}\cdot x|| = ||X_{n+1}S_n\cdot x|| \leq ||\rho(X_{n+1})||\ ||S_n\cdot x|| = ||\rho(X_{n+1})||\ \chi(A_n) \tag{3.10}$$

On the other hand, $\langle S_{n+1}\cdot(x-y_n), S_{n+1}\cdot y_n\rangle = \langle (x-y_n), S_{n+1}^t S_{n+1}\cdot y_n\rangle = 0$ because $x - y_n \perp U_{n+1}^{-1}\cdot V_{\chi_\rho}$ and if $y_n = U_{n+1}^{-1}\cdot z_n$ for some $z_n \in V_{\chi_\rho}$, then $S_{n+1}^t S_{n+1}\cdot y_n = U_{n+1}^{-1}A_{n+1}^2 U_{n+1}U_{n+1}^{-1}\cdot z_n = {\chi_\rho}^2(A_{n+1})y_n \in U_{n+1}^{-1}\cdot V_{\chi_\rho}$. Hence

$$||S_{n+1}\cdot x|| = \sqrt{||S_{n+1}\cdot y_n||^2 + ||S_{n+1}\cdot(x-y_n)||^2} \geq ||S_{n+1}\cdot y_n|| = \chi_\rho(A_{n+1})\ ||y_n|| \tag{3.11}$$

Combining (3.10) and (3.11) gives :

$$\sup_{x\in U_n^{-1}\cdot V_\chi; ||x||=1} ||Q_{\chi_\rho}(n+1)(x)|| = ||y_n|| \leq ||\rho(X_{n+1})||\ \frac{\chi(A_n)}{\chi_\rho(A_{n+1})}$$

But for every $p \in \mathbb{N}^*$, $||\rho(S_p)|| = \chi(A_p)$ (because the norm on V is K-invariant). Hence,

$$\sup_{x\in U_n^{-1}\cdot V_\chi; ||x||=1} ||Q_{\chi_\rho}(n+1)(x)|| = ||y_n|| \leq ||\rho(X_{n+1})||\cdot||\rho(X_{n+1}^{-1})||\ \frac{\chi(A_n)}{\chi_\rho(A_n)} \leq ||\rho(X_{n+1})||^d\ \frac{\chi(A_n)}{\chi_\rho(A_n)} \tag{3.12}$$

Last inequality is due to the relation $||g^{-1}|| \leq ||g||^{d-1}$ true for every $g \in SL_d(k)$. By Lemma 3.5.1, the probability measure $\rho(\mu)$ has an exponential moment so that

there exists $C \geq 1$ such that for all $\epsilon > 0$ small enough $\mathbb{E}(||\rho(X_{n+1})||^{\epsilon}) < C$. By Theorem 3.5.13, for every $\epsilon > 0$ small enough, some $\eta(\epsilon) \in]0,1[$ and all n large enough : $\mathbb{E}\Big[\Big(\frac{\chi(A_n)}{\chi_\rho(A_n)}\Big)^{\epsilon}\Big] \leq \eta(\epsilon)^n$. It suffices to apply Cauchy-Schwartz inequality to (3.12) to obtain the sub-exponential behavior of $\mathbb{E}\left(||Q_{\chi_\rho}(n)Q_\chi(n+1)||^{\epsilon}\right)$.

To bound $\mathbb{E}(||Q_{\chi_\rho}(n)Q_\chi(n+1)||^{\epsilon})$ we apply the same reasoning as above : we fix $x \in V_\chi(n+1)$ of norm one and denote by y_n its projection on $U_n^{-1} \cdot V_{\chi_\rho}$. Then, we evaluate $||S_n \cdot x||$ in two ways :

$$||S_n \cdot x|| = ||X_{n+1}^{-1} S_{n+1} \cdot x|| \leq ||\rho(X_{n+1}^{-1})||\ \chi(A_{n+1})$$

$$||S_n \cdot x|| = \sqrt{||S_n \cdot (x - y_n)||^2 + ||S_n \cdot y_n||^2} \geq ||S_n \cdot y_n|| = ||y_n|| \chi_\rho(A_n)$$

The end of the proof is the same as above. For the law of Z, see the following remark. □

Remark 3.5.16. *[Identification of the limit] By the Markov inequality and the Borel-Cantelli lemma, Theorem 3.5.15 shows that $U_n^{-1}[v_\rho]$ converges towards some random variable Z. In fact, the law of Z is the unique $\rho(\mu)^t$-invariant probability measure on $P(V)$ (see for example [BL85, Proposition 3.2 page 50]).*

Finally, we quote two useful results from Chapter 2.

Theorem 3.5.17 (Asymptotic independence of the K-components)**.** *With the same assumptions as in Theorem 3.5.15, there exist* ***independent random variables*** *Z and T with respective laws the unique $\rho(\mu)^t$ (resp. $\rho(\mu)$)- invariant probability measure on $P(V)$ such that for every $\epsilon > 0$, every ϵ-holder (real) function ϕ on $P(V) \times P(V)$ and all large n we have :*

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

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

Remark 3.5.18. *This is Theorem 2.4.36 from Chapter 2 with the only difference that the Zariski closure of Γ_μ was assumed split over $\mathbb{R}$. Here, this condition can be dropped for the following reasons. In Chapter 2 we were working with a semi-simple algebraic group $\mathbf{G}$ defined over a local field k. The condition k-split was imposed in order to have the Cartan decomposition for the k-points G of $\mathbf{G}$ in the form : $G = KAK$ (which is not the case in general, see Chapter 4). However, when $k = \mathbb{R}$, the Cartan decomposition can be taken $G = KAK$ in both cases, split and not split.*

Theorem 3.5.19 (Exponential convergence in direction)**.** *With the same notations and assumptions as in Theorem 3.5.15, for every $t \in]0,1[$, there exists $\rho(t) \in]0,1[$ such that for all large n :*

$$\underset{H \text{ hyperplane in } \mathbb{R}^d}{Sup} \ \underset{[x] \in P(V)}{Sup} \ \mathbb{P}\Big(\delta\left(S_n \cdot [x], H\right) \leq t^n\Big) < \rho(t)^n \tag{3.13}$$

Remark 3.5.20. *This is obtained by combining Theorems 2.4.16 and 2.4.18 of Chapter 2.*

3.6 Proof of the main theorems

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

Theorem 3.6.1. *Let* $\mathbf{G}$ *be a semi-simple algebraic group defined over* $\mathbb{R}$, G *its group of real points, let* (ρ, V) *be a rational real representation of* $\mathbf{G}$ *such that its irreducible sub-representations* $(\rho_1, V_1), \cdots, (\rho_r, V_r)$ *are pairwise non isomorphic and let finally* $A \in End(V_1) \oplus \cdots \oplus End(V_r)$ *such that its projection on* $End(V_1)$ *is non zero. Consider a probability measure* μ *on* G *with an exponential moment and such that* $G_\mu := \overline{\langle Supp(\mu) \rangle}$ *is Zariski dense in* G. *Denote by* $\{S_n; n \geq 0\}$ *the corresponding random walk. Assume that :*

1. ρ_1 *is proximal.*
2. $L_{\rho_1(\mu)} > L_{\rho_i(\mu)}$, $i = 2, \cdots, r$ *(see Definition 3.5.4).*

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

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

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

Assumption 1 in Theorem 3.6.1 is fulfilled whenever $\mathbf{G}$ is $\mathbb{R}$-split (see Lemma 3.4.1). We provide two sufficient conditions for assumption 2 to hold : a probabilistic one and a determinist (algebraic) one.

Remark 3.6.2 (A probabilistic sufficient conditions for assumption 2)**.** *Lemma 3.5.12 proves that assumption 2 is fulfilled whenever the Lyapunov vector* $Liap(\mu)$ *does not belong to a finite union of hyperplanes in the Weyl chamber* $\mathfrak{a}^+$.

Remark 3.6.3 (An algebraic sufficient conditions for assumption 2)**.** *Let* χ_i *be the highest weight of* V_i, $i = 1, \cdots, r$. *A necessary condition for* 2 *to hold is that* $\chi_1/\chi_i = \prod_{\alpha \in \Pi} \alpha^{n_\alpha}$ *for some non negative integers* $\{n_\alpha; \alpha \in \Pi\}$ *with at least one non zero* n_α. *This is easily checked using the fact that the Lyapunov vector is in the interior of the weyl chamber (Theorem 3.5.9).*
See the applications of this remark in the proof of Theorem 3.1.5

Proof. Without loss of generality, we can assume $r = 2$. Let $d = dim(V)$, $p = dim(V_1)$, $B_1 = (v_1, \cdots, v_p)$ (resp. $B_2 = (v_{p+1}, \cdots, v_d)$) a basis of V_1 (resp. V_2) consisting of weight vectors. We impose v_1 to be a highest weight. This gives a basis $B = (B_1, B_2)$ of V. The scalar products on V_1 and V_2 given by Theorem 3.4.2 induce naturally a scalar product on V for which V_1 and V_2 are orthogonal. In the basis B, $\rho(A_n) = diag(\rho_1(A_n), \rho_2(A_n)) = diag(a_1(n), \cdots, a_d(n))$ with $a_1(n) = \chi_{\rho_1}(A_n)$ and $a_{p+1}(n) = \chi_{\rho_2}(A_n)$ (notations of Section 3.4). Let W_{ρ_i} be the set of non zero weights of (V_i, ρ_i), $i = 1, 2$. A simple computation gives :

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

where $S_n = K_nA_nU_n$ is the Cartan decomposition of S_n (see Section 3.4.1). Since ρ_1 is proximal, $a_2(n) = \chi(A_n)$ for some weight $\chi \in W_{\rho_1}$ distinct from χ_ρ. Then,

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

Le Page large deviations theorem (Theorem 3.5.14) shows that for every $\epsilon > 0$ and some $\rho \in]0,1[$:

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

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

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

Indeed, for $\chi \neq \chi_{\rho_1} \in W_{\rho_1}$, this follows from Theorem 3.5.13 and the fact that ρ_1 is proximal. For $\chi \in W_{\rho_2}$, this follows also from Theorem 3.5.13 and assumption 2.

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

Proposition 3.6.4. *Let* $\mathbf{G}$ *be a semi-simple algebraic group defined over* $\mathbb{R}$, G *its group of real points,* Γ *a Zariski dense subgroup of* G, (ρ, V) *an irreducible rational real representation of* $\mathbf{G}$, μ *a probability measure with an exponential moment and whose support generates* Γ. *If* ρ *is proximal, then for any non zero endomorphism* $A \in End(V)$ *:*

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

where v_ρ *is a highest weight vector.*

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

Theorem 3.6.5. *[Gui90] Let* μ *be a probability measure on* $GL_d(\mathbb{R})$ *having an exponential moment and such that* G_μ *is strongly irreducible and proximal. Denote by* ν *the unique* μ*-invariant probability measure on the projective space* $P(\mathbb{R}^d)$ *. Then there exists* $\alpha > 0$ *(small enough) such that :*

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

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

$$Sup\{\mathbb{P}(|\langle Z, \frac{x}{||x||}\rangle| \leq \epsilon); \;\; x \in \mathbb{R}^d \setminus \{0\}\} \leq C\epsilon^\alpha$$

Proof of Proposition 3.6.4. This proof is very similar to the proof of Lemma 2.5.4 of Chapter 2.

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

$$\mathbb{1}_{[-a,a]} \leq \psi_a \leq \mathbb{1}_{[-2a,2a]} \tag{3.14}$$

Define for $a > 0$, $\phi_a = \psi_a \circ \eta$. By the previous remarks, ϕ_a is lipshitz with lipshitz constant : $||\phi_a|| \leq \frac{Max\{1,||A||\}}{a}$.
By Theorem 3.5.17 there exist independent random variables Z and T in $P(V)$ such that for any $t \in]0,1[$, we have :

$$\begin{aligned}
\mathbb{P}(|\langle K_n \cdot v_\rho, AU_n^{-1} \cdot v_\rho\rangle| \leq t^n) &\leq \mathbb{E}\left(\phi_{t^n}([K_n \cdot v_\rho],[{U_n}^{-1} \cdot v_\rho])\right) &(3.15)\\
&\leq \mathbb{E}\left(\phi_{t^n}(Z,T)\right) + ||\phi_{t^n}||\rho^n &(3.16)\\
&\leq \mathbb{P}(|\langle Z, AT\rangle| \leq 2t^n) + Max\{1,||A||\}\frac{\rho^n}{t^n} &(3.17)
\end{aligned}$$

In the last line, we confused between Z and T in $P(V)$ and some representative in the unit sphere. The bounds (3.15) and (3.17) follow from (3.14).
To prove our proposition, we can clearly suppose $t \in]\rho, 1[$. It suffices then to show that $\mathbb{P}(|\langle Z, AT\rangle| \leq 2t^n)$ is sub-exponential. The law of T is the unique $\rho(\mu)^t$-invariant probability measure ν on $P(V)$ (Theorem 3.5.17). Moreover, a general lemma of Furstenberg (see for example [BL85, Proposition 2.3 page 49]) shows that ν is proper. Hence, a.s. $AT \neq 0$. Moreover, we claim that following the stronger statement holds : there exist $C, \alpha > 0$ such that for every $t' \in]0,1[$ and $n \in \mathbb{N}^*$:

$$\mathbb{P}(||AT|| \leq t'^n) \leq Ct'^{n\alpha} \tag{3.18}$$

Indeed, A being a non zero endomorphism, there exist a non zero vector of norm one, v_0 such that $A^t v_0 \neq 0$. Then by Theorem 3.6.5,

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

Hence for every $t' \in]t, 1[$,

$$\begin{aligned}
\mathbb{P}(|\langle Z, AT\rangle| \leq 2t^n) &= \mathbb{P}(|\langle Z, \frac{AT}{||AT||}\rangle| \leq 2\frac{t^n}{||AT||})\\
&\leq \mathbb{P}\left(|\langle Z, \frac{AT}{||AT||}\rangle| \leq 2(t/t')^n\right) + \frac{C}{||A^t v_0||^\alpha} t'^{n\alpha}\\
&\leq Sup\{\mathbb{P}\left(\delta(Z,[H]) \leq 2(t/t')^n\right);\ H \text{ hyperplane of } V\} + Ct'^{n\alpha}
\end{aligned}$$

The last line is by independence of Z and T. Theorem 3.6.5 shows that it decreases exponentially fast to zero. □

As an application, we give the

Proof of Theorem 3.1.2. Lemma 3.3.2 allows us to be in the situation of Theorem 3.6.1, i.e., we have a representation (ρ, V) whose irreducible sub-representations $\rho_1, \cdots, \rho_r$ are pairwise non isomorphic, a endomorphism $A \in End(V_1) \oplus \cdots \oplus End(V_r)$ whose restriction to each $End(V_i)$ non zero such that $\mathcal{V} = \{g \in G; Tr(gA) = 0\}$. Lemma 3.5.12 allows us to distinguish a representation, say ρ_1, whose Lyapunov exponent is the biggest. Lemma 3.4.1 shows that this representation is proximal. It suffices to apply Theorem 3.6.1. □

Proof of Theorem 3.1.5. For every $k \in \mathbb{N}$, let $Sym^k(\mathbb{R}^d)$ be the vector space of homogenous polynomials on d variables of degree k. The group $SL_d(\mathbb{R})$ acts on $Sym^k(\mathbb{R}^d)$ by the formula : $g.P(X_1, \cdots, X_d) = P(g^{-1}(X_1, \cdots, X_d))$ for every $g \in SL_d(\mathbb{R})$, $P \in Sym^k(\mathbb{R}^d)$. A known fact (see for example [FH91]) is that the action of $SL_d(\mathbb{R})$ on $Sym^k(\mathbb{R}^d)$ is irreducible for every $k \in \mathbb{N}$.
Consider now a proper algebraic hypersurface $\widetilde{\mathcal{V}}$ of $\mathbb{R}^d$ defined over $\mathbb{R}$, a non zero vector x of $\mathbb{R}^d$ and denote $\mathcal{V} = \{g \in SL_d(\mathbb{R}); gx \in \widetilde{\mathcal{V}}\}$. Let now P be the polynomial that defines $\widetilde{\mathcal{V}}$, k its degree. The polynomial P can be seen as a vector in $V = \oplus_{i=0}^k Sym^i(\mathbb{R}^d)$. Let ρ_i be the action of $SL_d(\mathbb{R})$ on $Sym^i(\mathbb{R}^d)$. If P_i denotes projection of P on $Sym^i(\mathbb{R}^d)$, then "$gx \in \mathcal{V} \Leftrightarrow P(gx) = 0 \Leftrightarrow \sum_{i=0}^k f_i(g^{-1}) = 0$" where $f_i(g) = \rho_i(g)(P_i)(x) \in C(\rho_i)$ (see Definition 3.3.1). Moreover, the highest weight of $Sym^i(\mathbb{R}^d)$ is strictly bigger (for the natural order on $X(\mathbf{A})$ defined in Section 3.4.1) than the one of $Sym^{i-1}(\mathbb{R}^d)$, the ratio being the highest weight of the natural representation of $SL_d(\mathbb{R})$ on $\mathbb{R}^d$. We can then apply Remark 3.6.3 and Theorem 3.6.1 to the probability measure μ^{-1}. □

An application of the results of Section 3.5 independent from Theorem 3.6.1 is the

Proof of Theorem 3.1.6. If the identity component $\mathbf{H}^0$ of $\mathbf{H}$ is reductive, then by Proposition 3.3.4, there exists a rational representation (ρ, V) of $\mathbf{G}$ such that the reductive group $\mathbf{H}^0$ fixes a non zero vector x of V. By decomposing ρ into irreducible sub-representations, one can assume (ρ, V) to be irreducible. If $h_1, \cdots, h_r$ denote the cosets of the finite group H/H^0, then we can write

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

Since G has no compact factors, $\rho(G)$ is non compact. In particular, $\rho(G_\mu)$ is not contained in a compact subgroup of $SL(V)$ because compact subgroups of $SL(V)$ are algebraic and $\rho(G_\mu)$ is Zariski dense in $\rho(G)$. Hence we can apply Furstenberg theorem ([Fur63]) which shows that $L_{\rho(\mu)} > 0$ (see Definition 3.5.4). Applying Le Page large deviations theorem (Theorem 3.5.14) shows that for every $i = 1, \cdots, r$, $\mathbb{P}\left(||S_n \cdot (h_i^{-1} \cdot x)|| \leq exp(nL_{\rho(\mu)}/2)\right)$ decreases exponentially fast to zero.

If $\mathbf{H}^0$ is not reductive, then it contains a unipotent Zariski connected $\mathbb{R}$-subgroup $\mathbf{U}$ which is normal in $\mathbf{H}^0$. Hence $\mathbf{H}^0 \subset N(\mathbf{U})$, where $N(\mathbf{U})$ is the normalizer of $\mathbf{U}$ in $\mathbf{G}$. By [BT71, Corollary 3.9], there is an $\mathbb{R}$-parabolic subgroup $\mathbf{P}$ of $\mathbf{G}$ such that $N(\mathbf{U}) \subset \mathbf{P}$. By [BT65, Proposition 5.14], $\mathbf{P}$ is conjugated to one of the standard parabolic subgroups $\mathbf{P}_\theta$, $\theta \subset \Pi$ described in Section 3.4.3. Hence, by Lemma 3.4.4, $\mathbf{P}_\theta$ fixes the line generated by the highest weight x_α of (ρ_α, V_α) for every $\alpha \notin \theta$. Fix such α. Hence,

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

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

$$\mathbb{P}(S_n \in H) \leq \sum_{i=1}^{r} \mathbb{P}(\rho_\alpha(S_n)[h_i^{-1} x_\alpha] = [x_\alpha]) \tag{3.19}$$

The representation ρ_α is G-irreducible hence by connectedness, strongly irreducible. Moreover, it is proximal because $\Theta_{\rho_\alpha} = \{\alpha\}$, its highest weight space is a line and G has no compact factors. By Golsheid-Margulis theorem (Theorem 3.5.3), $\rho_\alpha(\Gamma)$ is proximal. Hence we can apply Theorem 3.5.19 which proves the exponential decay of the probability 3.19. □

3.7 Application to generic Zariski density and to free subgroups of linear groups

3.7.1 Statement of the results and commentaries

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

Question 3.7.1. *Let Γ be a Zariski dense subgroup of G. Is it true that two "random" elements in Γ generate a Zariski dense subgroup of G.*

A motivation for this question is the following

Question 3.7.2. *By the Tits alternative [Tit72], any Zariski dense subgroup Γ of G contains a Zariski dense free subgroup on two generators. A natural question is to see if this property is generic. In Theorem 2.1.1 of Chapter 2, we proved that two "random" elements in Γ generate a free subgroup. The question that arises immediately is to see if the latter subgroup is Zariski dense.*

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

Theorem 3.7.3. *[Riva, Corollary 2.11] Let $\mathbf{G} = \mathbf{SL_d}$ and $\Gamma = SL_d(\mathbb{Z})$ for some $d \geq 3$. Consider the uniform probability measure on a finite symmetric generating set and denote by $\{S_n, n \geq 0\}$ the associated random walk. Then, for any $g \in \Gamma$, there exists a constant $c(g) \in]0,1[$ such that*

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

Moreover, $c(g)$ is effective.

Passing from the "1.5 random subgroup" in Theorem 3.7.3 to the subgroup generated by two random elements is delicate since the constant $c(g)$ depends among others things on the norm of g.

Using our Theorem 3.1.2, we will prove the following

Theorem 3.7.4. *Let G be the group of real points of a semi-simple algebraic group defined and split over $\mathbb{R}$. Let Γ_1, Γ_2 be two Zariski dense subgroups of G. Then there exists probability measures μ_1 and μ_2 respectively on Γ_1 and Γ_2 with an exponential moment such that for some $c \in]0,1[$ and all large n,*

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

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

When $\mathbf{G} = \mathbf{SL_2}$, a stronger statement holds. It will follow immediately from the Theorem 2.1.1 of Chapter 2.

Theorem 3.7.5. *Let Γ_1, Γ_2 be two Zariski dense subgroups of $SL_2(\mathbb{R})$. Then for any probability measures μ_1 and μ_2 with an exponential moment whose support generates respectively Γ_1 and Γ_2, there exists $c \in]0,1[$ such that*

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

Remark 3.7.6. *Let us compare Theorem 3.7.4 with Rivin's Theorem 3.7.3. The advantage of our method is that it allows us to consider two elements at random and not a "1.5 random subgroup", which is crucial to solve Question 3.7.2. Furthermore, we do not necessarily consider arithmetic groups, neither finitely generated groups : any Zariski dense subgroup Γ works. In addition to that, the statement shows that Zariski density is generic for a pair of random elements taken in two groups Γ_1 and Γ_2 not necessarily equal.*
However, the big inconvenient is that our constants are not effective unlike Rivin's. Our result can be applied to prove the "1.5 random subgroup" but is less interesting than Rivin results since we don't know if the uniform probability measure on a finite symmetric generating of $SL_d(\mathbb{Z})$ works.
For $d = 2$, Theorem 3.7.5 is more satisfying ; there is no restrictions neither on μ_1 nor μ_2.

3.7.2 Proofs

Proof of Theorem 3.7.5. A subgroup of $SL_2(\mathbb{R})$ is Zariski dense if and only it is not virtually solvable. In particular, a free subgroup of $SL_2(\mathbb{R})$ is always Zariski dense. But in Theorem 2.2.11, we proved that with the same assumptions as in Theorem 3.7.5, $\mathbb{P}(\langle S_{1,n}, S_{2,n}\rangle$ is not free) decreases exponentially fast.

□

Proof of Theorem 3.7.4. The key point is the following

Lemma 3.7.7. *[Bre08, Lemma 6.8] Let k be a field of characteristic zero, $\mathbf{G}$ be a semi-simple group defined over k, $G = \mathbf{G}(k)$. Then there exists a proper algebraic variety $\mathcal{W}$ of $\mathbf{G} \times \mathbf{G}$ defined over k such that any pair of elements $x, y \in G$ generate a Zariski dense subgroup unless $(x, y) \in \mathcal{W}(k)$.*

By Lemma 3.3.2, there exist a rational real representation (ρ, V) of $\mathbf{G} \times \mathbf{G}$, an endomorphism $A \in End(V_1) \oplus \cdots \oplus End(V_r)$ such that

$$\mathcal{W} = \{(g,h) \in \mathbf{G} \times \mathbf{G};\ Tr\,(\rho(g,h)A) = 0\} \tag{3.20}$$

Let $\rho_1, \cdots, \rho_r$ the irreducible sub-representations of ρ. Since $\Gamma_1 \times \Gamma_2$ is Zariski dense in $\mathbf{G} \times \mathbf{G}$, the proof of Lemma 3.5.12 shows that there exist two probability measures μ_1 and μ_2 respectively on Γ_1 and Γ_2, a permutation σ of $\{1, \cdots, r\}$ such that $L_{\rho_{\sigma(i)}(\mu_1 \otimes \mu_2)} > L_{\rho_{\sigma(i+1)}(\mu_1 \otimes \mu_2)}$ for $i = 1, \cdots, r$. Let T_n be the random walk $(S_{1,n}, S_{2,n})$ on $\Gamma_1 \times \Gamma_2$ (i.e. the one corresponding to the probability measure $\mu_1 \otimes \mu_2$.) By Lemma 3.7.7 and identity (3.20),

$$\mathbb{P}(\langle S_{n,1}, S_{n,2}\rangle \text{ is not Zariski dense in } G) \leq \mathbb{P}\Big(Tr\,(\rho(T_n)A) = 0\Big) \tag{3.21}$$

Theorem 3.6.1 shows that the latter quantity decreases exponentially fast to zero. □

3.8 Open problems and questions

- It is interesting to see if the probabilistic methods we used can generalize Theorem 3.1.2. More precisely, if μ is a probability measure with an exponential moment and whose support generates a Zariski dense subgroup of the real points of a semi-simple algebraic group $\mathbf{G}$, is it true that for every proper algebraic subvariety $\mathcal{V}$ of $\mathbf{G}$,
$$\limsup \big[\mathbb{P}(S_n \in \mathcal{V})\big]^{\frac{1}{n}} < 1$$
where S_n the random walk associated to μ.
- The same question for Theorem 3.7.4 (i.e. replace there exists by for all, and do not assume the semi-simple algebraic group $\mathbf{G}$ $\mathbb{R}$-split.)

Chapitre 4

Produits de matrices aléatoires sur les groupes réductifs

4.1 Introduction

Let k be a local field of characteristic zero, $d \geq 2$, μ a probability measure on $GL_d(k)$, Γ_μ the smallest closed sub-semigroup containing the support of μ and consider the associated random walk. In this chapter, we show under natural assumptions on Γ_μ, the exponential convergence of the K-parts of the random walk in the Cartan decomposition and their asymptotic independence. In Chapter I, we have proved the same results (Theorems 2.4.38 and 2.4.39) with the following additional assumption : the Zariski closure of Γ_μ is a semi-simple algebraic group defined and split over k. Our aim in this section is to remove this condition and to replace it by the more natural one : Γ_μ is strongly irreducible. This implies that the identity component of the Zariski closure $\mathbf{G}$ of Γ_μ is a reductive algebraic group [1].
The proofs are very similar in spirit, the differences that occur are mostly technical. For example, the Cartan decomposition of $G = \mathbf{G}(k)$, the group of k-points of $\mathbf{G}$, reads $G = KZK$ where $Z = \mathbf{Z}(k)$ and $\mathbf{Z}$ is the centralizer of $\mathbf{A}$ in $\mathbf{G}$ and no longer $G = KAK$, as in the k-split case.

We recall that $\{X_n; n \geq 1\}$ is a sequence of independent random variables with law μ and we denote for every $n \in \mathbb{N}^*$, $S_n = X_n \cdots X_1$ and $M_n = X_1 \cdots X_n$. Our main goal in this chapter is to prove the following two statements :

Theorem 4.1.1 (Exponential convergence in the Cartan decomposition)**.** *Let k be a local field of characteristic zero, $d \geq 2$, μ a probability measure on $GL_d(k)$ having an exponential moment (Definition 4.2.1) and such that Γ_μ is strongly irreducible and*

1. A reductive algebraic k-group is an algebraic group defined over k which does not contain a Zariski connected normal unipotent algebraic k-subgroup. For every algebraic k-group $\mathbf{E}$ we donte by E its k-points. Let us prove that $\Gamma_\mu \subset GL(V)$ is strongly irreducible implies that $\mathbf{G} = \overline{\Gamma_\mu}^0$ is reductive. Indeed, if it is not the case, then $\mathbf{G}^0$ contains a non trivial connected unipotent algebraic subgroup $\mathbf{N}$. Notice that its k-points N is non trivial, because in characteristic zero N is Zariski dense in $\mathbf{N}$ (see [Bor91, Corollary 18.3]). The subgroup N being unipotent, it fixes a non zero vector $x \in V$. Since N is normal, it induces the identity on the vector space $V' = Span\{g \cdot x, g \in G^0\}$. By irreducibility of G^0, $V' = V$. This contradicts the fact that N is non trivial.

contracting (see Definition 2.2.7). Denote by $(e_1, \cdots, e_d)$ *the canonical basis of* k^d. *Let* $S_n = K_n A_n U_n$ *be a Cartan decomposition of* S_n *in* $GL_d(k)$ *(See Section 1.3.2). Then,* $U_n^t[e_1]$ *converges almost surely toward a variable* Z *in the projective space* $P(k^d)$ *with law the unique* μ^t*-invariant probability measure on* $P(k^d)$ *(see Theorem 2.4.5) with an exponential speed, that is for every* $\epsilon > 0$ *:*

$$\limsup_{n\to\infty} \frac{1}{n} \log \mathbb{E}\left(\delta(U_n^t[e_1], Z)^\epsilon\right) < 0$$

where δ *is the Fubini-Study distance on the projective space :* $\delta([x],[y]) = \frac{||x\wedge y||}{||x||||y||}$, $[x],[y] \in P(k^d)$. *Recall that, for* $g \in GL_d(k)$, g^t *is the transposed matrix of* g *when expressed in the canonical basis and* μ^t *is the law of* X_1^t.

Theorem 4.1.2 (Asymptotic independence in the Cartan decomposition)**.** *With the same assumptions as in Theorem 4.1.1, there exist independent random variables* Z *and* T *with law the unique the unique* μ^t *(resp.* μ*)-invariant probability measure on* $P(k^d)$ *such that for every* $\epsilon > 0$, *every* ϵ*-Holder function on* $P(k^d) \times P(k^d)$,

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

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

The proof will rely on a careful study of random walks on reductive algebraic groups and their decomposition in the Cartan decomposition.
The analog of these results for the Iwasawa decomposition are known over the real field. They were proved by Yves Guivarc'h in [Gui90].

In Section 4.2 we recall main results obtained in Chapter I concerning random matrix products theory and we indicate that they hold in a slightly more general context.

In Section 4.3 we recall important facts about reductive algebraic groups.

In Section 4.4, we consider a reductive algebraic group $\mathbf{G}$ defined over a local field k, G its group of k-points and a random walk on a Zariski dense subgroup of G. We study carefully the components of the Cartan decomposition of the random walk and we prove Theorems 4.1.1 and 4.1.2 above.

4.2 Notation and summary of prior results from Section 2.4

In this section, we recall some results we obtained in Chapitre 2 when working with random walks on subgroups of $SL_d(k)$ (k being a local field). We claim that their generalization to subgroups of $GL_d(k)$ is straightforward. We will refrain from including all the details of the proofs, and will content ourselves with precise statements of the

results.

Let k be a local field, $d \geq 2$, μ a probability measure on $GL_d(k)$, Γ_μ the smallest close sub-semi-group of $GL_d(k)$ containing the support of μ.

Definition 4.2.1. *We say that μ has a moment of order one (resp. an exponential moment) if $\int l(g)d\mu(g) < \infty$ (resp. $\int exp\,(\tau l(g))\,d\mu(g) < \infty$ for some $\tau > 0$), where $l(g) = \log^+(||g||) \vee \log^+(||g^{-1}||)$ and $x^+ = Sup(x, 0)$ for every $x \in \mathbb{R}$.*

4.2.1 Norm estimates

Proposition 4.2.2. *(Proposition 2.4.9) If Γ_μ is strongly irreducible, then for any sequence $\{x_n; n \geq 0\}$ in k^d converging to a non zero vector :*

$$a.s \qquad inf_{n\in\mathbb{N}^*} \frac{||S_n.x_n||}{||S_n||} > 0 \tag{4.1}$$

A version in expectation is the following proposition :

Proposition 4.2.3. *(Proposition 2.4.14)[Weak large deviations] Suppose that μ has an exponential moment and that Γ_μ 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 $n > n(\gamma)$:*

$$Sup_{x\in k^d;\, ||x||=1} \mathbb{E}\big[(\frac{||S_n||}{||S_n x||})^\epsilon\big] \leq (1+\epsilon\gamma)^n \tag{4.2}$$

In particular, for every $\epsilon > 0$,

$$\limsup_{n\to\infty} \Big[Sup_{x\in k^d;\, ||x||=1} \mathbb{P}\left(\frac{||S_n||}{||S_n x||} \geq exp(n\epsilon)\right)\Big]^{\frac{1}{n}} < 0 \tag{4.3}$$

4.2.2 Convergence in direction

Theorem 4.2.4. *(Theorem 2.4.16)[Exponential convergence in direction] Assume that Γ_μ is strongly irreducible and proximal, then there exists a random variable Z on the projective space $P(k^d)$ with law the unique μ-invariant probability measure on $P(k^d)$ such that for some $\lambda > 0$ and every $\epsilon > 0$:*

$$Sup_{[x]\in P(k^d)} \mathbb{E}\left(\delta(M_n[x], Z)^\epsilon\right) \leq (1-\lambda\epsilon)^n$$

where δ is the Fubini-Study distance on $P(k^d)$. In particular, for every $[x] \in P(k^d)$, $M_n[x]$ converges almost surely towards Z.

The key lemma used to prove Proposition 4.2.3 and Theorem 4.2.4 is the following result, which generalizes a lemma of Le Page :

Lemma 4.2.5. *(Lemma 2.4.12)[Cocycle lemma] Let G be a topological semigroup acting on a topological space X, s a cocycle on $G \times X$, i.e. s is continuous and $s(gh,x) = s(g,h\cdot x)+s(h,x)$ for every $g,h \in G$ and $x \in X$, μ a probability measure on G satisfying for $r(g) = sup_{x\in X}|s(g,x)|$: there exists $\tau > 0$ such that*

$$\mathbb{E}\left(exp(\tau r(X_1))\right) < \infty \tag{4.4}$$

- *If*

$$\lim_{n\to\infty} \frac{1}{n} Sup_{x\in X}\, \mathbb{E}(s(S_n,x)) < 0,$$

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

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

- *If*

$$\lim_{n\to\infty} \frac{1}{n} Sup_{x\in X}\, \mathbb{E}(s(S_n,x)) = 0,$$

then for all $\gamma > 0$, there exist $\epsilon(\gamma) > 0$, $n(\gamma) \in \mathbb{N}^*$ such that for every $0 < \epsilon < \epsilon(\gamma)$ and $n > n(\gamma)$,

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

4.3 Reductive algebraic groups defined over local fields

In this section, we recall some well-known facts about reductive groups over local fields and their linear representations.

Let k be a local field : either $\mathbb{R}$ or $\mathbb{C}$ or a finite extension of $\mathbb{Q}_p$ for a prime p or a field of Laurent series over a finite field.
If $k = \mathbb{R}$ or $\mathbb{C}$, we consider the standard absolute value and set $q = e$, the base of the natural logarithm, and $v(x) = -\log|x|$ for every $x \in k$.
When k is non archimedean, we denote by Ω_k its discrete valuation ring, π a generator of its unique maximal ideal, q the degree of its residual field, $v(.)$ a discrete valuation and consider the following ultrametric norm : $|.| = q^{-v(.)}$.

Let $\mathbf{G}$ be a a connected reductive algebraic k-group, G its group of k-points. We fix a maximal k-split torus $\mathbf{A}$ and denote by $\mathbf{Z}$ its centralizer in $\mathbf{G}$ and Z its group of k-points. For every algebraic k-group $\mathbf{H}$, we denote by $X(\mathbf{H})$ the group of k-rational characters of $\mathbf{H}$. By definition, the k-rank of $\mathbf{G}$ is the rank of the free abelian group $X(\mathbf{A})$. The homomorphism of restriction identifies $X(\mathbf{Z})$ with a finite index subgroup of $X(\mathbf{A})$. We denote by E^* the $\mathbb{R}$-vector space $\mathbb{R}\otimes_{\mathbb{Z}} X(\mathbf{A})$ and E its dual. For every $\chi \in X(\mathbf{A})$, we denote by χ^w the linear form induced on E. For every $z \in Z$, there exists a unique vector $\nu(z) \in E$ such that for every $\chi \in X(\mathbf{Z})$,

$$\chi^w\left(\nu(z)\right) = -v\left(\chi(z)\right)$$

Let Δ be the system of roots of G restricted to $\mathbf{A}$, which consists of the common eigenvalues of $\mathbf{A}$ in the adjoint representation. We fix an order on Δ and denote by Δ^+ the system of positive roots, Π the system of simple roots. We set $E^+ = \{x \in E; \alpha^w(x) \geq 0 \ \forall \alpha \in \Pi\}$ the Weyl chamber and its interior $E^{++} = \{x \in E; \alpha^w(x) > 0 \ \forall \alpha \in \Pi\}$. We set

$$Z^+ = \nu^{-1}(E^+)$$

Reference for the above : Bruhat and Tits [BT72], [BT84]. See also nice exposition in Quint [Qui02a], [Qui02b].

4.3.1 Decompositions in reductive algebraic groups

With these notation, there exists a maximal compact K of G such that

$$G = KZ^+K \quad \text{Cartan decomposition}$$

Let $\mathfrak{g}$ 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 $\mathbf{N}$ be the unique connected subgroup of $\mathbf{G}$ whose Lie algebra is $\oplus_{\alpha \in \Delta^+} \mathfrak{g}_\alpha$; it is a maximal unipotent connected subgroup. Then the following decomposition, called Iwasawa decomposition, holds :

$$G = KZN \quad \text{Iwasawa decomposition}$$

4.3.2 Representations of reductive algebraic groups

From now on, abusing notation, we will not differentiate between χ and χ^w.

A weight χ of a linear k-representation (ρ, V) is a k-rational character of $\mathbf{A}$ which is a common eigenvalue of the elements of $\mathbf{A}$ under ρ. The corresponding weight space V_χ is defined by : $V_\chi = \{x \in V; \rho(a)x = \chi(a)x \ \forall a \in A\}$. An irreducible k-rational representation (ρ, V) of $\mathbf{G}$ is characterized by a highest weight χ_ρ such that every weight $\chi \neq \chi_\rho$ can be written : $\chi = \chi_\rho - \sum_{\alpha \in \Pi} n_\alpha \alpha$ where n_α is a non negative integer. We set

$$\Theta_\rho = \{\alpha \in \Pi; \ \chi_\rho - \alpha \text{ is a weight of } (\rho, V)\}$$

Let (ρ, V) be an irreducible k-rational representation of $\mathbf{G}$. We have $V = \oplus_\chi V_\chi$ where the sum is over all weights of V. According to [Qui02a, Theorem 6.1], there exists a norm $||.||$ on V which is preserved by $\rho(K)$, and such that, for every $z \in \rho(z)$ is a similitude on each V_χ with ratio $q^{\chi(\nu(z))}$, i.e. $\frac{||\rho(z)x||}{||x||} = q^{\chi(\nu(z))}$ for every $z \in Z$ and $x \in V_\chi$. Moreover the direct sum V_χ is good (see Section 2.4.3). Such a norm on V is called a "good norm". As a consequence, we obtain :

Lemma 4.3.1. *For every $g \in G$, we set $g = k(g)z(g)u(g)$ its Cartan decomposition and $g = \widetilde{k(g)}\widetilde{z(g)}n(g)$ its Iwasawa decomposition. Let (ρ, V) be an irreducible k-rational representation of $\mathbf{G}$ and denote by χ_ρ its highest weight. Then there exists a norm on V such that*

$$||\rho(g)|| = q^{\chi_\rho(\nu(z(g)))}$$

and

$$\frac{||\rho(g)x||}{||x||} = q^{\chi_\rho\left(\widetilde{\nu(z(g))}\right)} \quad ; \quad x \in V_{\chi_\rho}$$

4.3.3 A useful lemma

We will need to express every k-rational character χ of $\mathbf{A}$ in terms of highest weights of irreducible linear representations of $\mathbf{G}$. The following lemma will be useful to us.

Lemma 4.3.2. *The $\mathbb{Z}$-module generated by the highest weights of irreducible representations of $\mathbf{G}$ is of finite index in $X(\mathbf{A})$. In particular, there exists $\chi_1, \cdots, \chi_r$ highest weights of irreducible k-rational representations $\rho_1, \cdots, \rho_r$ such that every $\chi \in X(\mathbf{A})$ can be written :*

$$\chi = \sum_{i=1}^{r} n_i \chi_i \quad ; n_i \in \mathbb{Q}$$

Proof. Let $\mathbf{Z}(\mathbf{G})$ be the center of $\mathbf{G}$, $\mathbf{D}(\mathbf{G})$ its derived group. Denote $X_{\mathbf{Z}(\mathbf{G})} = \{\chi \in X(\mathbf{A}); \chi(a) = 1 \ \forall a \in \mathbf{Z}(\mathbf{G})\}$ and $X_{\mathbf{D}(\mathbf{G})} = \{\chi \in X(\mathbf{A}); \chi(a) = 1 \ \forall a \in \mathbf{D}(\mathbf{G}) \cap \mathbf{A}\}$. First, notice that $X_{\mathbf{Z}(\mathbf{G})}$ is isomorphic to $X(\mathbf{A}_1)$ and $X_{\mathbf{D}(\mathbf{G})}$ is isomorphic to $X(\mathbf{A}_2)$ where A_1 is the maximal k-split torus of the semi-simple algebraic group $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ and A_2 is the maximal k-split torus of the k-torus $\mathbf{G}/\mathbf{D}(\mathbf{G})$. Since $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ is semi-simple, there exists a $\mathbb{Q}$-basis (even a $\mathbb{Z}$-basis) of $X(\mathbf{A_1})$ consisting of highest weights of $\mathbf{G}/\mathbf{Z}(\mathbf{G})$ (consider the fundamental weights, see Proposition 2.4.21), hence of $\mathbf{G}$. Moreover, every weight of $X(\mathbf{A}_2)$ comes from a highest weight of a one-dimensional representation of $\mathbf{G}$, which factors through $\mathbf{D}(\mathbf{G})$. Hence the $\mathbb{Z}$-module generated by the highest weights of irreducible representations of $\mathbf{G}$ contains the $\mathbb{Z}$-module $X_{\mathbf{Z}(\mathbf{G})} + X_{\mathbf{D}(\mathbf{G})}$ which is of index in $X(\mathbf{A})$ because it is the sum of two $\mathbb{Z}$-submodules of the $\mathbb{Z}$-module $X(\mathbf{A})$ whose intersection is finite and such that the sum of their ranks equals the rank of $X(\mathbf{A})$ (see [BT65, Proposition 4.27]). □

4.4 Random walks on reductive algebraic groups

In this section, k is a local field, $\mathbf{G}$ is a connected reductive algebraic group defined over k, G its group of k-points, μ a probability measure on G such that Γ_μ (the smallest closed semi-group containing the support of μ) is Zariski dense. Consider an irreducible k-rational representation (ρ, V) of $\mathbf{G}$. We use the notation of Section 4.3. Notice that since G is Zariski dense in $\mathbf{G}$ (see [Bor91, Corollary 18.3]), then ρ is G-irreducible. Fix a measurable section $G \to KZ^+K$ (resp. $G \to KZN$)) of the Cartan decomposition (resp. Iwasawa decomposition) of G. The Cartan decomposition of S_n will be denoted by $S_n = K_n Z_n U_n$ and its Iwasawa decomposition by $S_n = \widetilde{K_n}\widetilde{Z_n}N_n$.

4.4.1 The Lyapunov vector

In this section, we define the Lyapunov vector $Liap(\mu)$. It is an element of the Weyl chamber E^+ and is the limiting process of the well normalized Cartan projection of the random walk S_n.

Theorem 4.4.1 (Lyapunov vector)**.** *There exists a constant vector $Liap(\mu)$ in the Weyl chamber E^+ such that the following limit exists*

$$\lim_{n\to+\infty} \frac{1}{n}\nu(Z_n) = Liap(\mu)$$

Moreover, when $k = \mathbb{R}$, $Liap(\mu) \in E^{++}$, i.e. a.s. $\lim \frac{1}{n}\alpha\left(\nu(Z_n)\right) > 0$ for every $\alpha \in \Pi$.

Proof. For the existence of $Liap(\mu)$, it suffices to show that a.s. for every $\chi \in X(A)$, $\frac{1}{n}\chi\left(\nu(Z_n)\right)$ has a non random limit as n goes to infinity. Indeed, by Lemma 4.3.2, we can write $\chi = \sum_{i=1}^{r} n_i\chi_i$ where $n_i \in \mathbb{Q}$ and χ_i is a highest weight. Hence, without loss of generality we can assume that χ is a highest weight of an irreducible representation (ρ, V) of $\mathbf{G}$. By Lemma 4.3.1,

$$\frac{\chi\left(\nu(Z_n)\right)}{n} = \frac{\log_q ||\rho(S_n)||}{n}$$

The last expression has a limit as n goes to infinity by Kingman's ergodic subadditive theorem [Kin73]. Notice that when $\chi \in X_{\mathbf{D}(\mathbf{G})}$ (see the proof of Lemma 4.3.2), the existence of this limit follows from the law of large numbers.
The proof that $Liap(\mu) \in E^{++}$ whenever $k = \mathbb{R}$ is one of the main results of [GR85] and we have checked it in Theorem 3.5.9 of Chapter 3. □

4.4.2 Limit theorems in the Z-component of the Cartan and Iwasawa decompositions.

Let i be an algebraic embedding of $\mathbf{G}$ inside $\mathbf{GL}_r$ defined over k.

Definition 4.4.2 (Exponential moment for algebraic groups)**.** *If μ is a probability measure on G, we say that μ has an exponential moment if $i(\mu)$ (image of μ under i) has an exponential moment (see Definition 4.2.1).*

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 4.4.3. *Let $G \subset GL(V)$ be the k-points of a k-algebraic group $\mathbf{G}$ and ρ a finite dimensional k-algebraic representation of $\mathbf{G}$. If μ has an exponential moment then the image of μ under ρ has also an exponential 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. Hence, one can easily verify that there exists $C, D > 0$ such that $||\rho(g^{\pm 1})|| \leq ||g^{\pm 1}||^C + D$ for every $g \in G$. This suffices to show the lemma. □

Proposition 4.4.4 (Comparison betwen Cartan and Iwasawa decomposition)**.** *Assume that μ has an exponential moment. Then there exists random compact subsets E and F of G such that a.s. for n big enough, $Z_n\widetilde{Z_n}^{-1} \in E$, $\widetilde{Z_n}{Z_n}^{-1} \in F$.*

Proof. Since $\mathbf{G}$ can be embedded in some $\mathbf{GL_d}$, it is equivalent to prove that for every k-rational representation (ρ, V) of $\mathbf{G}$, $\rho(Z_n)\widetilde{\rho(Z_n)}^{-1}$ and $\widetilde{\rho(Z_n)}\rho(Z_n)^{-1}$ belong a.s. to some random subset of G. Let (ρ, V) be such a representation. By decomposing it into irreducible sub-representations (this is possible because we are in characteristic zero), we can assume that ρ is irreducible. The vector space V is the direct sum of the weight spaces V_χ. Moreover, this direct sum is good and for every $z \in Z$, $\rho(z)$ induces on each V_χ a similitude of ratio $q^{\chi(\nu(z))}$ (notice that Z fixes every weight space V_χ). Hence, for every non zero weight χ of V, every $x \in V_\chi$:

$$\frac{||\rho(Z_n)\rho(\widetilde{Z_n}^{-1})x||}{||x||} = q^{\chi(\nu(Z_n))-\chi\left(\nu(\widetilde{Z_n})\right)}$$

By Lemma 4.3.2, $\chi = \sum_{i=1} n_i\chi_i$ where $n_i \in \mathbb{Q}$ and χ_i is a highest weight of an irreducible k-rational representation (ρ_i, V_i). Hence,

$$\frac{||\rho(Z_n)\rho(\widetilde{Z_n}^{-1})x||}{||x||} = \prod_{i=1}^{r} q^{n_i\left[\chi_i(\nu(Z_n))-\chi_i\left(\nu(\widetilde{Z_n})\right)\right]}$$

By Lemma 4.3.1 we have :

$$\frac{||\rho(Z_n)\rho(\widetilde{Z_n}^{-1})x||}{||x||} = \prod_{i=1}^{r} \left(\frac{||\rho_i(S_n)||}{||\rho_i(S_n)x_i||}\right)^{n_i}$$

where x_i is a highest weight vector of ρ_i of norm one. Since G is Zariski connected, every representation ρ_i is strongly irreducible. Then, the last expression is a.s. bounded by Proposition 4.2.2. □

Proposition 4.4.5 (Comparison between Cartan and Iwasawa in expectation)**.** *Assume that μ has an exponential moment (Definition 4.4.2). Let $\chi \in X(\mathbf{A})$ and set $\eta = \pm 1$. Then, for every $\gamma > 0$, there exist $\epsilon(\gamma) > 0$ and $n(\gamma) \in \mathbb{N}^*$ such that for $0 < \epsilon < \epsilon(\gamma)$, $n > n(\gamma)$,*

$$\mathbb{E}\left[q^{\eta\epsilon\chi\left(\nu(Z_n)-\nu(\widetilde{Z_n})\right)}\right] \leq (1+\epsilon\gamma)^n \tag{4.5}$$

Proof. Let $\epsilon > 0$ and $\chi \in X(\mathbf{A})$. Express χ in terms of highest weights : $\chi = \sum_{i=1}^{s} n_i\chi_i$ where $s \in \mathbb{N}^*$ and for every $i = 1, ..., s$, $n_i \in \mathbb{Q}$ and χ_i is a highest weight of an irreducible k-rational representation (ρ_i, V_i). Then, by Lemma 4.3.1, we have a.s. : $||\rho_i(S_n)|| = q^{n_i\chi_i(\nu(Z_n))}$ and $\frac{||\rho_i(S_n)x_i||}{||x_i||} = q^{n_i\chi_i\left(\nu(\widetilde{Z_n})\right)}$ where x_i is a highest weight vector of ρ_i. In consequence,

$$\mathbb{E}\left[q^{\epsilon\chi\left(\nu(Z_n)-\nu(\widetilde{Z_n})\right)}\right] = \mathbb{E}\left[\prod_{i=1}^{s}\left(\frac{||\rho_i(S_n)||}{\frac{||\rho_i(S_n)x_i||}{||x_i||}}\right)^{\epsilon n_i}\right]$$

By the Holder inequality,

$$\mathbb{E}\Big[q^{\epsilon\chi\left(\nu(Z_n)-\nu(\widetilde{Z_n})\right)}\Big] \leq \prod_{i=1}^{s}\Big[\mathbb{E}\Big[\left(\frac{||\rho_i(S_n)||}{\frac{||\rho_i(S_n)x_i||}{||x_i||}}\right)^{\epsilon s n_i}\Big]\Big]^{\frac{1}{s}}$$

Terms with $n_i \leq 0$ are less or equal to one. Hence, it suffices to control the terms where $n_i > 0$. Fix such $i \in \{1, ..., s\}$. By Lemma 4.4.3, the image of μ under ρ_i has an exponential moment. Moreover, as explained in the proof of the previous proposition, G being Zariski-connected, ρ_i is strongly irreducible. Consequently, we can apply Proposition 4.2.3 which shows what we want. □

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

Theorem 4.4.6 (Exponential contraction in KAN)**.** *Assume that μ is a probability on G with an exponential moment. Then for every simple root α such that $\alpha \in \Theta_\rho$ (see Section 4.3.2) for some irreducible k-rational representation ρ of $\mathbf{G}$ such that $\rho(\Gamma_\mu)$ is contracting, the following holds : there exists $\lambda > 0$, such that for every $\epsilon > 0$ small enough and all n large enough :*

$$\mathbb{E}\Big[q^{-\epsilon\alpha\left(\nu(\widetilde{Z_n})\right)}\Big] \leq (1-\lambda\epsilon)^n \tag{4.6}$$

Remark 4.4.7. *When $k = \mathbb{R}$, inequality (4.6) is true for every $\alpha \in \Pi$. Indeed, by Proposition 3.4.2, for every $\alpha \in \Pi$, there exists an irreducible k-rational representation ρ_α of $\mathbf{G}$ whose highest weight is a line and such that $\Theta_{\rho_\alpha} = \{\alpha\}$. By Zariski density of Γ_μ and Goldsheid-Margulis theorem (see Theorem 3.5.3), $\rho_\alpha(\Gamma_\mu)$ is contracting.*

Proof. Let $\alpha \in \Theta_\rho$ and decompose α into highest weights : $\alpha = \sum_{i=1}^{s} n_i\chi_i$, with $n_i \in \mathbb{Q}$ for every $i = 1, ..., s$ and χ_i a highest weight of some irreducible k-rational representation (ρ_i, V_i) as we may according to Lemma 4.3.2. By Lemma 4.3.1, for every $i = 1, ..., s$, there exists a (ρ_i, A, K)-good norm on V_i such that :

$$\chi_i\left(\nu(\widetilde{Z_n})\right) = \log_q \frac{||\rho_i(\widetilde{Z_n})x_i||}{||x_i||}$$

where x_i is a highest weight vector of ρ_i. Hence,

$$\mathbb{E}\Big(q^{-\epsilon\alpha\left(\nu(\widetilde{Z_n})\right)}\Big) \leq Sup_{x\in X}\ \mathbb{E}\left(q^{-\epsilon s(S_n,x)}\right)$$

where $X = \prod_{i=1}^{s} P(V_i)$ and s is the cocycle defined on $G \times X$ by :

$$s\left(g, ([x_1], ..., [x_s])\right) = \sum_{i=1}^{s} n_i \log_q \frac{||\rho_i(g).x_i||}{||x_i||}$$

We are now in the same setting as in the proof of Theorem 2.4.28. Applying verbatim the proof of Theorem 2.4.28, we see that it is enough to show that :

$$\alpha\left(\nu(Z_n)\right) \xrightarrow[n\to\infty]{\text{a.s.}} +\infty \quad \forall\alpha \in \Theta_\rho$$

Consider the canonical Cartan decomposition of $\rho(S_n)$ in $GL_d(k)$ (See Section 1.3.2 or 2.3.2). Let $a_1(n), \cdots, a_d(n)$ be the diagonal components. Since by the hypothesis $\rho(\Gamma_\mu)$ is contracting, we have by Theorem 2.4.5 that a.s. every limit point of $\frac{\rho(S_n)}{a_1(n)}$ is a rank one matrix. In particular, $\frac{a_2(n)}{a_1(n)}, ..., \frac{a_d(n)}{a_1(n)}$ converge a.s. to zero. Hence, $\frac{||\bigwedge^2 \rho(Z_n)||}{||\rho(Z_n)||^2}$ tends a.s. to zero as n goes to infinity. But the set of highest weights of the irreducible sub-representations of $\bigwedge^2 V$ is exactly $\{2\chi_\rho - \beta; \beta \in \Theta_\rho\}$. Since $||\rho(Z_n)|| = q^{\chi_\rho(\nu(Z_n))}$, $||\bigwedge^2 \rho(Z_n)|| = Max\{q^{(2\chi_\rho - \beta)(\nu(Z_n))}; \beta \in \Pi\}$, we have

$$Max\{q^{-\beta(\nu(Z_n))}; \beta \in \Theta_\rho\} \xrightarrow[n\to\infty]{\text{a.s.}} 0$$

In particular, $\alpha\left(\nu(Z_n)\right) \xrightarrow[n\to\infty]{\text{a.s.}} \infty$. □

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

Theorem 4.4.8 (Exponential contraction in KAK)**.** *With the same hypotheses as in Theorem 4.4.6, there exists $\lambda > 0$ such that for all $\epsilon > 0$:*

$$\mathbb{E}\left[q^{-\epsilon\alpha(\nu(Z_n))}\right] \leq (1-\lambda\epsilon)^n \quad ; \quad \alpha \in \Theta_\rho$$

Proof. We write

$$q^{-\epsilon\alpha(\nu(Z_n))} = q^{-\epsilon\alpha\left(\nu(\widetilde{Z_n})\right)} \times q^{\epsilon\left[\alpha\left(\nu(\widetilde{Z_n})\right) - \alpha(\nu(Z_n))\right]}$$

Fix $\gamma > 0$. By Proposition 4.4.5, Theorem 4.4.6 and Cauchy-Schwartz inequality, there exists $\lambda > 0$, $\epsilon(\gamma) > 0$, such that for every $0 < \epsilon < \epsilon(\gamma)$ and all large n :

$$\mathbb{E}\left[q^{-\epsilon\alpha(\nu(Z_n))}\right] \leq (1-2\lambda\epsilon)^{\frac{1}{2}} \times (1+2\gamma\epsilon)^{\frac{1}{2}}$$

It suffices to choose γ (in terms of λ) small enough. □

Corollary 4.4.9 (Ratio in the A-component for the KAK decomposition of $GL_d(k)$)**.** *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 $GL_d(k)$ as described in Section 1.3.2 or 2.3.2 . We write $a(g) = diag\left(a_1(g), ..., a_d(g)\right)$ in the canonical basis of k^d. With this notation and with the same assumptions as in Theorem 4.4.6, we have for some $\lambda > 0$ and every $\epsilon > 0$ small enough,*

$$\limsup_{n\to\infty} \left[\mathbb{E}\left(\left|\frac{a_i\left(\rho(S_n)\right)}{a_1\left(\rho(S_n)\right)}\right|^\epsilon\right)\right]^{\frac{1}{n}} \leq 1 - \gamma\epsilon \qquad \forall i = 2, ..., d$$

Proof. We write the Cartan decomposition of $\rho(S_n)$ in both decompositions : the one associated to the algebraic group G and the canonical one in $GL_d(k)$: $\rho(S_n) = \rho(K_n)\rho(Z_n)\rho(U_n) = k(S_n)a(S_n)u(S_n)$.

We use the canonical norm on k^d. We have $|a_i(\rho(S_n))| \leq |a_2(\rho(S_n))|$ for $i = 3, ..., d$, $|a_1(n)a_2(n)| = ||\bigwedge^2 S_n||$ and that $\rho(K_n), \rho(U_n), k(S_n), u(S_n)$ belong to compact groups of $GL_d(k)$. Hence there exists a constant $C > 0$ such that :

$$\mathbb{E}\left(\left|\frac{a_i(\rho(S_n))}{a_1(\rho(S_n))}\right|^{\epsilon}\right) \leq \mathbb{E}\left(\frac{||\bigwedge^2 a(S_n)||^{\epsilon}}{||a(S_n)||^{2\epsilon}}\right) \leq C\mathbb{E}\left(\frac{||\bigwedge^2 \rho(Z_n)||^{\epsilon}}{||\rho(Z_n)||^{2\epsilon}}\right) \tag{4.7}$$

The representation $\bigwedge^2 V$ may not be G-irreducible. However, the only possible highest weights of its irreducible sub-representations [2] are the $\{2\chi_\rho - \alpha;\ \alpha \in \Theta_\rho\}$. Combining this fact, the fact that Z_n acts by similitude on the weight spaces of V and $\bigwedge^2 V$, and inequality (4.7) gives :

$$\mathbb{E}\left(\left|\frac{a_i(\rho(S_n))}{a_1(\rho(S_n))}\right|^{\epsilon}\right) \ll \sum_{\alpha \in \Theta_\rho} \mathbb{E}\left[q^{-\epsilon\alpha(\nu(Z_n))}\right]$$

By Theorem 4.4.8, this decreases exponentially fast to zero for every $\epsilon > 0$ small enough.

□

Proof of Theorems 4.1.1 and 4.1.2. We follow verbatim the proof of Theorems 2.4.38 and 2.4.39 given in Chapter 2 using Corollary 4.4.9 instead of Corollary 2.4.32. □

2. We are in characteristic zero, hence the action of $\mathbf{G}$ on $\bigwedge^2 V$ is completely reducible

Bibliographie

[AAG99] I. Anshel, M. Anshel, and D. Goldfeld. An algebraic method for public-key cryptography. *Math. Res. Lett.*, 6(3-4) :287–291, 1999.

[AO96] G. N. Arzhantseva and A. Yu. Ol′shanskiĭ. Generality of the class of groups in which subgroups with a lesser number of generators are free. *Mat. Zametki*, 59(4) :489–496, 638, 1996.

[Aoua] R. Aoun. Random subgroups of linear groups are free. *To appear in Duke Mathematical Journal. Arxiv : 1005.3445.*

[Aoub] R. Aoun. Transience of algebraic groups and application to generic zariski density. *In preparation.*

[Arz97] G. N. Arzhantseva. On groups in which subgroups with a fixed number of generators are free. *Fundam. Prikl. Mat.*, 3(3) :675–683, 1997.

[Arz98] G. N. Arzhantseva. Generic properties of finitely presented groups and Howson's theorem. *Comm. Algebra*, 26(11) :3783–3792, 1998.

[Arz08] I. Arzhantsev. Invariant ideals and Matsushima's criterion. *Comm. Algebra*, 36(12) :4368–4374, 2008.

[Bab89] L. Babai. The probability of generating the symmetric group. *J. Combin. Theory Ser. A*, 52(1) :148–153, 1989.

[BAG01] A. Broise-Alamichel and Y. Guivarc'h. Exposants caractéristiques de l'algorithme de Jacobi-Perron et de la transformation associée. *Ann. Inst. Fourier (Grenoble)*, 51(3) :565–686, 2001.

[Bek90] M. Bekka. Amenable unitary representations of locally compact groups. *Invent. Math.*, 100(2) :383–401, 1990.

[Ben97] Y. Benoist. Propriétés asymptotiques des groupes linéaires. *Geom. Funct. Anal.*, 7(1) :1–47, 1997.

[Ben00] Y. Benoist. Propriétés asymptotiques des groupes linéaires. II. In *Analysis on homogeneous spaces and representation theory of Lie groups, Okayama–Kyoto (1997)*, volume 26 of *Adv. Stud. Pure Math.*, pages 33–48. Math. Soc. Japan, Tokyo, 2000.

[Ben04] Y. Benoist. Convexes divisibles. I. In *Algebraic groups and arithmetic*, pages 339–374. Tata Inst. Fund. Res., Mumbai, 2004.

[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.

[BG08] J. Bourgain and A. Gamburd. Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$. *Ann. of Math. (2)*, 167(2) :625–642, 2008.

[BG09] J. Bourgain and A. Gamburd. Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$ II - with an appendix by J. bourgain. *J. Eur. Math. Soc. (JEMS)*, 5 :1057–1103, 2009.

[BG10] E. Breuillard and A. Gamburd. Strong uniform expansion in $\mathrm{SL}(2,p)$. *To appear in GAFA*, 2010.

[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.

[Bor91] A. Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[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.

[Bou86] P. Bougerol. Oscillation des produits de matrices aléatoires dont l'exposant de Lyapounov est nul. In *Lyapunov exponents (Bremen, 1984)*, volume 1186 of *Lecture Notes in Math.*, pages 27–36. Springer, Berlin, 1986.

[Bou87] P. Bougerol. Tightness of products of random matrices and stability of linear stochastic systems. *Ann. Probab.*, 15(1) :40–74, 1987.

[BQ09] Y. Benoist and J.-F. Quint. Mesures stationnaires et fermés invariants des espaces homogènes. *C. R. Math. Acad. Sci. Paris*, 347(1-2) :9–13, 2009.

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

[Bre08] E. Breuillard. A strong tits alternative. *preprint*, 2008.

[BT65] A. Borel and J. Tits. Groupes réductifs. *Inst. Hautes Études Sci. Publ. Math.*, (27) :55–150, 1965.

[BT71] A. Borel and J. Tits. Éléments unipotents et sous-groupes paraboliques de groupes réductifs. I. *Invent. Math.*, 12 :95–104, 1971.

[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.

[CD97] M. Cowling and B. Dorofaeff. Random subgroups of Lie groups. *Rend. Sem. Mat. Fis. Milano*, 67 :95–101 (2000), 1997.

[Cha95] C. Champetier. Propriétés statistiques des groupes de présentation finie. *Adv. Math.*, 116(2) :197–262, 1995.

[Coh79] J. E. Cohen. Ergodic theorems in demography. *Bull. Amer. Math. Soc. (N.S.)*, 1(2) :275–295, 1979.

[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.

[DD] B. Deroin and R. Dujardin. Random walks, kleinian groups, and bifurcation currents. *Arxiv : 1011.1365.*

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

[Dia88] P. Diaconis. *Group representations in probability and statistics.* Institute of Mathematical Statistics Lecture Notes—Monograph Series, 11. Institute of Mathematical Statistics, Hayward, CA, 1988.

[Dix69] J. Dixon. The probability of generating the symmetric group. *Math. Z.*, 110 :199–205, 1969.

[DlHGCS99] P. De la Harpe, R. Grigorchuk, and T. Chekerini-Silberstein. Amenability and paradoxical decompositions for pseudogroups and discrete metric spaces. *Tr. Mat. Inst. Steklova*, 224(Algebra. Topol. Differ. Uravn. i ikh Prilozh.) :68–111, 1999.

[dSGLP04] B. de Saporta, Y. Guivarc'h, and E. Le Page. On the multidimensional stochastic equation $Y_{n+1} = A_n Y_n + B_n$. *C. R. Math. Acad. Sci. Paris*, 339(7) :499–502, 2004.

[ET65] P. Erdős and P. Turán. On some problems of a statistical group-theory. I. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 4 :175–186 (1965), 1965.

[ET67a] P. Erdős and P. Turán. On some problems of a statistical group-theory. II. *Acta math. Acad. Sci. Hungar.*, 18 :151–163, 1967.

[ET67b] P. Erdős and P. Turán. On some problems of a statistical group-theory. III. *Acta Math. Acad. Sci. Hungar.*, 18 :309–320, 1967.

[ET68] P. Erdős and P. Turán. On some problems of a statistical group-theory. IV. *Acta Math. Acad. Sci. Hungar*, 19 :413–435, 1968.

[ET70] P. Erdős and P. Turán. On some problems of a statistical group theory. VI. *J. Indian Math. Soc.*, 34(3-4) :175–192 (1971), 1970.

[ET71] P. Erdős and P. Turán. On some problems of a statistical group theory. V. *Period. Math. Hungar.*, 1(1) :5–13, 1971.

[Eym72] P. Eymard. *Moyennes invariantes et représentations unitaires.* Lecture Notes in Mathematics, Vol. 300. Springer-Verlag, Berlin, 1972.

[FH91] W. Fulton and J. Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[FK60] H. Furstenberg and H. Kesten. Products of random matrices. *Ann. Math. Statist.*, 31 :457–469, 1960.

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

[GG96] I. Ya. Goldsheid and Y. Guivarc'h. Zariski closure and the dimension of the Gaussian law of the product of random matrices. I. *Probab. Theory Related Fields*, 105(1) :109–142, 1996.

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

[GMO10] I. Gilman, A. Miasnikov, and D. Osin. Exponentially generic subsets of groups. *preprint available at http ://arxiv.org/abs/1007.0552*, 2010.

[Gol91] I. Ya. Gol′dsheĭd. Lyapunov exponents and asymptotic behaviour of the product of random matrices. In *Lyapunov exponents (Oberwolfach, 1990)*, volume 1486 of *Lecture Notes in Math.*, pages 23–37. Springer, Berlin, 1991.

[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.

[GR86] Y. Guivarc'h and A. Raugi. Products of random matrices : convergence theorems. In *Random matrices and their applications (Brunswick, Maine, 1984)*, volume 50 of *Contemp. Math.*, pages 31–54. Amer. Math. Soc., Providence, RI, 1986.

[Gro93] M. Gromov. Asymptotic invariants of infinite groups. In *Geometric group theory, Vol. 2 (Sussex, 1991)*, volume 182 of *London Math. Soc. Lecture Note Ser.*, pages 1–295. Cambridge Univ. Press, Cambridge, 1993.

[Gro03] M. Gromov. Random walk in random groups. *Geom. Funct. Anal.*, 13(1) :73–146, 2003.

[Gui80] Y. Guivarc'h. Sur la loi des grands nombres et le rayon spectral d'une marche aléatoire. In *Conference on Random Walks (Kleebach, 1979) (French)*, volume 74 of *Astérisque*, pages 47–98, 3. Soc. Math. France, Paris, 1980.

[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.

[Gui06] Y. Guivarc'h. Heavy tail properties of stationary solutions of multidimensional stochastic recursions. In *Dynamics & stochastics*, volume 48 of *IMS Lecture Notes Monogr. Ser.*, pages 85–99. Inst. Math. Statist., Beachwood, OH, 2006.

[Gui08] Y. Guivarc'h. On the spectrum of a large subgroup of a semisimple group. *J. Mod. Dyn.*, 2(1) :15–42, 2008.

[Hel01] S. Helgason. *Differential geometry, Lie groups, and symmetric spaces*, volume 34 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2001. Corrected reprint of the 1978 original.

[Hum75] J.E. Humphreys. *Linear algebraic groups*. Springer-Verlag, New York, 1975. Graduate Texts in Mathematics, No. 21.

[Kes59] H. Kesten. Symmetric random walks on groups. *Trans. Amer. Math. Soc.*, 92 :336–354, 1959.

[Kes73] Harry Kesten. Random difference equations and renewal theory for products of random matrices. *Acta Math.*, 131 :207–248, 1973.

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

[KMSS03] I. Kapovich, A. Miasnikov, P. Schupp, and V. Shpilrain. Generic-case complexity, decision problems in group theory, and random walks. *J. Algebra*, 264(2) :665–694, 2003.

[Kna86] A. Knapp. *Representation theory of semisimple groups*. Princeton University Press, 1986.

[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.

[Lia04] M. Liao. *Lévy processes in Lie groups*, volume 162 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2004.

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

[LP83] É. Le Page. Théorèmes de renouvellement pour les produits de matrices aléatoires. Équations aux différences aléatoires. In *Séminaires de probabilités Rennes 1983*, Publ. Sém. Math., page 116. Univ. Rennes I, Rennes, 1983.

[LP89] É. Le Page. Régularité du plus grand exposant caractéristique des produits de matrices aléatoires indépendantes et applications. *Ann. Inst. H. Poincaré Probab. Statist.*, 25(2) :109–142, 1989.

[LS96] M. Liebeck and A. Shalev. Classical groups, probabilistic methods, and the $(2, 3)$-generation problem. *Ann. of Math. (2)*, 144(1) :77–125, 1996.

[Lyo00] Russell Lyons. Singularity of some random continued fractions. *J. Theoret. Probab.*, 13(2) :535–545, 2000.

[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.

[Mat60] Y. Matsushima. Espaces homogènes de Stein des groupes de Lie complexes. *Nagoya Math. J*, 16 :205–218, 1960.

[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. Soĭfer. Maximal subgroups of infinite index in finitely generated linear groups. *J. Algebra*, 69(1) :1–23, 1981.

[MU07] A. Myasnikov and A. Ushakov. Length based attack and braid groups : cryptanalysis of Anshel-Anshel-Goldfeld key exchange protocol. In *Public key cryptography—PKC 2007*, volume 4450 of *Lecture Notes in Comput. Sci.*, pages 76–88. Springer, Berlin, 2007.

[MU08] A.. Miasnikov and A. Ushakov. Random subgroups and analysis of the length-based and quotient attacks. *J. Math. Cryptol.*, 2(1) :29–61, 2008.

[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.

[Rau97] A. Raugi. Théorème ergodique multiplicatif. Produits de matrices aléatoires indépendantes. In *Fascicule de probabilités*, volume 1996/1997 of *Publ. Inst. Rech. Math. Rennes*, page 43. Univ. Rennes I, Rennes, 1997.

[Riva] I. Rivin. Zariski density and genericity. *International Mathematics Research Notices Advance Access.*

[Rivb] Y. Rivin. Zariski density and genericity. *International Mathematics Research Notices Advance.*

[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.

[Riv10] I. Rivin. Zariski density and genericity. *Int. Math. Res. Not. IMRN*, (19) :3649–3657, 2010.

[SC04] L. Saloff-Coste. Random walks on finite groups. In *Probability on discrete structures*, volume 110 of *Encyclopaedia Math. Sci.*, pages 263–346. Springer, Berlin, 2004.

[Sha99] A. Shalev. Probabilistic group theory. In *Groups St. Andrews 1997 in Bath, II*, volume 261 of *London Math. Soc. Lecture Note Ser.*, pages 648–678. Cambridge Univ. Press, Cambridge, 1999.

[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.

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

[VK67] È. B. Vinberg and V. G. Kac. Quasi-homogeneous cones. *Mat. Zametki*, 1 :347–354, 1967.

[ZL] A. Zuk and A. Lubotzky. *On property (τ).* To appear. Available at http ://www.ma.huji.ac.il/ alexlub/.

[Żuk03] A. Żuk. Property (T) and Kazhdan constants for discrete groups. *Geom. Funct. Anal.*, 13(3) :643–670, 2003.