Croissance des groupes d'isométries des espaces symétriques

Jean-François Quint

GDR Platon, Institut Henri Poincaré, Paris, Octobre 2009

Chapitre 1

Groupes de Lie semi-simples et sous-groupes discrets

Dans ce cours, nous allons nous intéresser à la compréhension de certaines propriétés asymptotiques des sous-groupes discrets des groupes de Lie semi-simple. Ce premier chapitre a pour but de préciser ce qu'est un groupe de Lie semi-simples, en tâchant d'éviter la théorie générale le plus possible.

1.1 Groupes de Lie semi-simples

Rappelons qu'un groupe de Lie est un groupe G muni d'une structure de variété différentielle pour laquelle l'application $G \times G \to G, (g, h) \mapsto g^{-1}h$ est lisse. Nous utiliserons tous les résultats fondamentaux de la théorie des groupes de Lie, pour lesquels on renvoie à [16].

Définition 1.1.1. Un groupe de Lie connexe G est dit semi-simple si le seul sous-groupe distingué abélien connexe de G est le sous-groupe trivial réduit à l'élément neutre de G.

Cette définition a le mérite de la concision à défaut de celui de la clarté. En effet, les groupes de Lie semi-simples sont des objets extrêmement riches qui possèdent de nombreuses définitions équivalentes. En particulier, les groupes de Lie semi-simple peuvent être décrits très précisément. Tout groupe de Lie semi-simple est, à un revêtement près, le produit d'un nombre fini de groupes de Lie simples (un groupe de Lie connexe G est simple s'il est de de dimension > 1 et si les seuls sous-groupes fermés distingués connexes de G sont le sous-groupe trivial et G lui-même). Les groupes de Lie simples peuvent, quant à eux, être classifiés, à un revêtement près (voir [8]). Sans rentrer dans les détails de cette classification, disons simplement qu'elle comprend de grandes familles comme les groupes $\mathrm{SL}_n(\mathbb{R})$ ou $\mathrm{SL}_n(\mathbb{C})$, $n \geq 2$, la composante connexe des groupes $\mathrm{SO}(p,q)$, $p+q \geq 3$, les groupes $\mathrm{SU}(p,q)$, $p+q \geq 2$, etc. ainsi qu'une liste finie de groupes dits exceptionnels.

Bien que les groupes de Lie semi-simples soient, a priori, des objets de nature différentielle, leur étude est proche de celle de certains objets provenant de la géométriqe algébrique. Si $\mathbb{K}$ est un corps, un groupe algébrique sur $\mathbb{K}$ est un groupe $\mathbf{G}$ muni d'une structure de $\mathbb{K}$-variété algébrique pour laquelle l'application $\mathbf{G} \times \mathbf{G} \to \mathbf{G}$, $(g,h) \mapsto g^{-1}h$ est un morphisme de variétés algébriques (voir [4]). Si $\mathbb{K}$ est $\mathbb{R}$, le groupe $\mathbf{G}(\mathbb{R})$ des points réels de $\mathbf{G}$ possède une structure naturelle de groupe de Lie.

Réciproquement, si G est un groupe de Lie semi-simple, d'algèbre de Lie $\mathfrak{g}$, le groupe des automorphismes de $\mathfrak{g}$ possède une structure naturelle de groupe algébrique. On note $\mathbf{G}$ sa composante connexe au sens de la géométrie algébrique. Alors, la représentation adjointe de G induit un morphisme de groupes de Lie $G \to \mathbf{G}(\mathbb{R})$ dont l'image est la composante connexe (au sens classique) de $\mathbf{G}(\mathbb{R})$. Ce morphisme est un revêtement. Par conséquent, tout groupe de Lie semi-simple est, à un revêtement près, la composante connexe du groupe des points réels d'un groupe algébrique. Ceci explique pourquoi tous les exemples de groupes de Lie que nous avons donné sont de ce type.

Les groupes de Lie semi-simple apparaissent aussi en géométrie. Si M est une variété riemannienne connexe et m un point de M, le théorème de Hopf-Rinov (voir [7]) assure l'existence d'un voisinage symétrique U de 0 dans l'espace tangent en m à M tel que l'application exponentielle en m induise un difféomorphisme de U sur un voisinage V de m. La symétrie géodésique s_m en m est alors l'application $V \to V, \mathrm{Exp_m} X \mapsto \mathrm{Exp_m}(-X)$. On dit que M est symétrique si, pour tout m dans M, la symétrie géodésique s_m se prolonge en une isométrie globale de m (nécessairement unique). Dans ce cas, M peut s'écrire de manière unique $M = M_+ \times M_0 \times M_-$ où M_+, M_0, M_- sont aussi des variétés riemaniennes symétriques telles que M_0 est isométrique à un espace euclidien et M_- (resp. M_+) est à courbure négative (resp. positive) et ne peut pas s'écrire comme le produit d'un espace euclidien avec un autre espace symétrique. Si $M = M_+$, on dit que M est de type compact et, si $M = M_-$, on dit qu'il est de type non compact. Les espaces symétriques de type compact et non compact sont décrits dans [8]. Ceux de type non compact sont toujours contractiles (comme toute variété riemannienne simplement connexe à courbure négative, d'après le théorème de Hadamard, voir [7]).

Le groupe des isométries H d'un espace symétrique M peut être muni d'une structure naturelle de groupe de Lie, pour laquelle l'action de H sur M est une application lisse $H \times M \to M$. Si M est de type non-compact, la composante neutre G de H est semi-simple et son action sur M est transitive. Les stabilisateurs des points de M dans G sont des sous-groupes compacts maximaux de G. Réciproquement, si G est un groupe semi-simple de centre fini, il possède des sous-groupes compacts maximaux et ceux-ci sont tous conjugués. Si K est un tel sous-groupe, les métriques riemanniennes G-invariantes du quotient G/K le munissent d'une structure d'espace symétrique de type non compact.

Exemple 1.1.2. Pour tout $n \geq 2$ (resp. $n \geq 1$), la composante connexe du groupe des isométries de l'espace hyperbolique réel (resp. complexe) de dimension n est la composante connexe du groupe $\mathrm{SO}(1, n)$ (resp. le groupe $\mathrm{SU}(1, n)$).

Pour tout $n \geq 2$, le groupe $\mathrm{SO}(n)$ (resp. $\mathrm{SU}(n)$) est un sous-groupe compact de $\mathrm{SL}_n(\mathbb{R})$ (resp. $\mathrm{SL}_n(\mathbb{C})$). Le quotient $\mathrm{SL}_n(\mathbb{R})/\mathrm{SO}(n)$ (resp. $\mathrm{SL}_n(\mathbb{C})/\mathrm{SU}(n)$) s'identifie à l'ensemble des matrices symétriques (resp. hermitiennes) définies positives de taille n et de déterminant 1.

Signalons enfin une dernière caractérisation des groupes de Lie semi-simples en termes d'actions linéaires. Si Γ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$, pour $n \geq 1$, on dit que Γ agit irréductiblement sur $\mathbb{R}^n$ si pour tout sous-espace vectoriel V de $\mathbb{R}^n$ tel que $\Gamma V \subset V$, on a $V = \{0\}$ ou $V = \mathbb{R}^n$. Rappelons par ailleurs que l'adhérence de Zariski de Γ dans $\mathrm{GL}_n(\mathbb{R})$ est le groupe $\mathbf{G}(\mathbb{R})$ où $\mathbf{G}$ est le plus petit sous-groupe algébrique réel de GL_n tel que $\Gamma \subset \mathbf{G}(\mathbb{R})$. Alors, si Γ agit irréductiblement sur $\mathbb{R}^n$, la composante connexe de son adhérence de Zariski est un groupe de Lie réductif, c'est-à-dire, à un revêtement près, le produit d'un groupe de Lie abélien par un groupe de Lie semi-simple.

1.2 Décompositions des groupes de Lie semi-simples

Nous allons à présent présenter certains résultats de structure des groupes de Lie semi-simples. Ces résultats sont des conséquences de la théorie générale développée dans [8] et [4]. Nous les énonçons et les démontrons ici dans le cas particulier des groupes $\mathrm{SL}_n(\mathbb{R})$ et $\mathrm{SL}_n(\mathbb{C})$, $n \geq 2$. Ils s'étendent sans difficulté aux produits de tels groupes.

On note K le groupe $\mathrm{SO}(n)$ (resp. $\mathrm{SU}(n)$), A le groupe des matrices diagonales de taille n, de déterminant 1 et dont les coefficients sont des réels > 0 et N le groupe des matrices triangulaires supérieures à coefficients réels (resp. complexes) dont toutes les valeurs propres égalent 1. On note A^+ le sous ensemble de A formé des matrices de coefficients diagonaux $a_1, \ldots a_n$ avec $a_1 \geq \ldots \geq a_n$. Enfin, on note M le groupe des matrices diagonales de déterminant 1 dont les coefficients sont réels (resp. complexes) de module 1 et B le groupe des matrices triangulaires supérieures, c'est-à-dire qu'on a $B = MAN$.

Proposition 1.2.1 (Décomposition de Cartan)**.** *On a $G = KA^+K$. Plus précisément, pour tout g dans G, il existe un unique élément a de A^+ tel que g appartienne à KaK.*

Démonstration. Soit g dans G. Si g^t est la matrice transposée de g, la matrice $g^t g$ est symétrique est définie positive. Elle s'écrit donc s^2, où s est elle même une matrice symétrique définie positive. On a alors $(gs^{-1})^t(gs^{-1}) = 1$, c'est-à-dire $g = ks$, avec k dans K. Mais alors, comme s est diagonalisable en base orthonormée à valeurs propres positives, on peut écrire $s = lal^{-1}$ avec l dans K et a dans A^+. Il vient $g = klsl^{-1}$, d'où l'existence de la décomposition. L'unicité s'obtient de manière analogue.□

Exemple 1.2.2. Munissons $\mathbb{R}^n$ (resp. $\mathbb{C}^n$ du produit scalaire standard qui est K-invariant. Si $n = 2$, pour tout g dans G, on a $g \in K \begin{pmatrix} \|g\| & 0 \\ 0 & \|g\|^{-1} \end{pmatrix} K$. Si $n = 3$, pour tout g dans G, on a $g \in K \begin{pmatrix} \|g\| & 0 & 0 \\ 0 & \|g\|^{-1}\|g^{-1}\| & 0 \\ 0 & 0 & \|g^{-1}\|^{-1} \end{pmatrix} K$.

L'algèbre de Lie $\mathfrak{a}$ de A s'identifie à l'ensemble des éléments $(X_1, \ldots, X_n)$ de $\mathbb{R}^n$ avec $X_1 + \ldots + X_n = 0$. Pour g dans G, on note $\kappa(g) = (\kappa_1(g), \ldots, \kappa_n(g))$ l'unique élément de $\mathfrak{a}$ tel que $g \in K \exp(\kappa(g))K$.

Remarque 1.2.3. L'espace tangent à G/K en K s'identifie de façon K-équivariante à l'espace des matrices symétriques de trace nulle. L'action de K dans cet espace préserve la forme quadratique définie positive $(X, Y) \mapsto \mathrm{tr}(XY)$ et l'on vérifie qu'il s'agit là, à un multiple près, de l'unique forme quadratique préservée par cette action. La métrique riemannienne G-invariante associée sur G/K est donc, à un multiple près, l'unique métrique riemannienne G-invariante sur cet espace. Si g est un élément de G, pour cette métrique, on a $d(gK, K) = \sqrt{\kappa_1(g)^2 + \ldots + \kappa_n(g)^2}$.

Plus généralement, si G est un groupe de Lie simple de centre fini et K un sous-groupe compact maximal de G, G préserve, à un scalaire près, une unique métrique riemannienne sur G/K.

Proposition 1.2.4 (Décomposition d'Iwasawa). *On a $G = KAN$ et l'application produit $K \times A \times N \to G$ est une bijection.*

Démonstration. Il s'agit là d'une traduction immédiate du procédé d'orthogonalisation de Gram-Schmidt.□

Le normalisateur de MA dans G est le groupe des éléments de G qui laissent stable l'ensemble des droites engendrées par la base canonique $(e_1, \ldots, e_n)$ de $\mathbb{R}^n$ (resp. $\mathbb{C}^n$). Son quotient W par MA est donc un groupe fini qui s'identifie naturellement au groupe des permutations de l'ensemble $\{1, \ldots, n\}$.

Proposition 1.2.5 (Décomposition de Bruhat). *On a $G = \bigcup_{w \in W} BwB$. Plus précisément, le groupe G est la réunion distincte des ensembles BwB, où w parcourt W.*

Si $\mathbb{K}$ est un corps et V un $\mathbb{K}$-espace vectoriel, un drapeau de V est une suite strictement croissante $V_0 = \{0\} \subsetneq V_1 \subsetneq \ldots \subsetneq V_r = V$ de sous-espaces vectoriels de V. Si $r = \dim V$, on dit que le drapeau est complet. Si ξ et η sont deux drapeaux complets, on montre aisément qu'il existe une unique permutation w de l'ensemble $\{1, \ldots, n\}$ telle qu'il existe une base $(v_1, \ldots, v_n)$ de V avec $\xi = (\{0\}, \mathbb{K}v_1, \mathbb{K}v_1 \oplus \mathbb{K}v_2, \ldots, V)$ et $\eta = (\{0\}, \mathbb{K}v_{w(1)}, \mathbb{K}v_{w(1)} \oplus \mathbb{K}v_{w(2)}, \ldots, V)$.

On note $\mathcal{B}$ l'espace des drapeaux complets de $\mathbb{R}^n$ (resp. $\mathbb{C}^n$). Si ξ_0 est le drapeau complet $\{0\}, \mathbb{R}e_1, \mathbb{R}e_1 \oplus \mathbb{R}e_2, \ldots, \mathbb{R}^n$ (resp. $\{0\}, \mathbb{C}e_1, \mathbb{C}e_1 \oplus \mathbb{C}e_2, \ldots, \mathbb{C}^n$), l'application $G \to \mathcal{B}, g \mapsto g\xi_0$ identifie $\mathcal{B}$ et G/B.

Démonstration de la proposition 1.2.5. Soit g dans G. D'après la remarque ci-dessus, il existe une permutation w de $\{1, \ldots, n\}$ et une base $(v_1, \ldots, v_n)$ de V avec $\xi_0 = (\{0\}, \mathbb{K}v_1, \mathbb{K}v_1 \oplus \mathbb{K}v_2, \ldots, V)$ et $g\xi_0 = (\{0\}, \mathbb{K}v_{w(1)}, \mathbb{K}v_{w(1)} \oplus \mathbb{K}v_{w(2)}, \ldots, V)$. Soit b un élément de G tel que, pour tout $1 \leq i \leq n$, be_i soit proportionnel à v_i. Alors, on a $b\xi_0 = \xi_0$, donc b appartient à B. De plus, si on note encore w un élément de G tel que, pour tout $1 \leq i \leq n$, we_i soit proportionnel à $e_{w(i)}$, on a $g\xi_0 = bw\xi_0$, donc $g \in bwB$, d'où l'existence de la décomposition. L'unicité se démontre de manière analogue.□

1.3 Sous-groupes Zariski denses

Si G est un groupe de Lie semi-simple, son image par la représentation adjointe, c'est-à-dire son quotient par son centre, peut se voir de manière naturelle comme le groupe des points réels d'un groupe algébrique défini sur $\mathbb{R}$. On dit alors qu'un sous-groupe Γ de G est Zariski dense dans G si l'image de Γ dans ce quotient est Zariski dense, c'est-à-dire n'est pas contenue dans le groupe des points réels d'un sous-groupe algébrique strict. Cela revient à dire que, pour toute représentation linéaire de G dans un espace vectoriel réel V, pour tout sous-espace vectoriel W de V, si $\Gamma W \subset W$, on a $GW \subset W$ (ce fait étant une conséquence du théorème de Chevalley, voir [4]).

Revenons, pour préciser les idées, au cas où G est $\mathrm{SL}_n(\mathbb{R})$ ou $\mathrm{SL}_n(\mathbb{C})$. Nous conservons les notations introduites au paragraphe précédent et nous noterons A^{++} l'ensemble des éléments de A dont les coefficients $a_1, \ldots, a_n$ vérifient $a_1 > \ldots > a_n$, c'est-à-dire que A^{++} est l'intérieur de A^+. Nous dirons qu'un élément g de G est loxodromique s'il est conjugué à un élément de MA^{++}. On démontre aisément qu'un élément est loxodromique si et seulement s'il possède un point fixe attracteur dans $\mathcal{B}$.

Proposition 1.3.1 (Benoist-Labourie, Prasad [11])**.** *Soit Γ un sous-groupe Zariski dense de G. Alors Γ contient un élément loxodromique.*

Exemple 1.3.2. Un sous-groupe de $\mathrm{SL}_2(\mathbb{R})$ est Zariski dense si et seulement s'il est non-élémentaire au sens de la géométrie hyperbolique, ce qui revient à dire qu'il ne fixe ni de produit scalaire sur $\mathbb{R}^2$, ni de droite de $\mathbb{R}^2$, ni de réunion de deux droites dans $\mathbb{R}^2$.

Proposition 1.3.3. *Soient G un groupe de Lie simple et Γ un sous-groupe Zariski dense de G. Alors Γ est discret ou dense.*

Démonstration. Soient $\mathfrak{g}$ l'algèbre de Lie de G et $\mathfrak{h} \subset \mathfrak{g}$ l'algèbre de Lie de l'adhérence de Γ. Alors, pour tout γ dans Γ, on a $\mathrm{Ad}_\gamma \mathfrak{h} \subset \mathfrak{h}$, donc, pour tout g dans G, on a $\mathrm{Ad}_g \mathfrak{h} \subset \mathfrak{h}$. Comme G est simple, on a $\mathfrak{h} = \{0\}$ ou $\mathfrak{h} = \mathfrak{g}$, d'où le résultat. □

1.4 Exemples de sous-groupes discrets Zariski denses

Nous allons à présent donner trois types d'exemples de sous-groupes discrets Zariski dense d'un groupe de Lie semi-simple G.

1.4.1 Réseaux

Rappelons qu'un réseau d'un groupe topologique localement compact G est un sous-groupe discret Γ de G tel quel le quotient G/Γ possède une mesure borélienne finie invariante par G. En particulier, si Γ est un sous-groupe co-compact de G, il est un réseau.

Exemple 1.4.1. Pour tout $n \geq 2$, $\mathrm{SL}_n(\mathbb{Z})$ est un réseau non co-compact de $\mathrm{SL}_n(\mathbb{R})$ et $\mathrm{SL}_n(\mathbb{Z}[i])$ est un réseau non co-compact de $\mathrm{SL}_n(\mathbb{C})$.

Les groupes de Lie semi-simples admettent de nombreux réseaux.

Théorème 1.4.2 (Borel-Harish Chandra [5])**.** *Si G est un groupe de Lie semi-simple, G possède à la fois des réseaux co-compacts et des réseaux non co-compacts.*

Exemple 1.4.3. Pour tout $n \geq 2$, le groupe $\mathrm{SO}(1, n)$ possède un réseau co-compact Γ. D'après le lemme de Selberg (voir [2]), quitte à remplacer Γ par un sous-groupe d'indice fini, Γ est sans torsion. Alors, le quotient $\Gamma\backslash\mathbb{H}^n_{\mathbb{R}}$ de l'espace hyperbolique réel par l'action de Γ est une variété différentielle muni d'une métrique riemanienne localement isométrique à celle de l'espace hyperbolique.

Un groupe de Lie semi-simple peut s'écrire, à revêtement fini près, de manière unique comme le produit de groupes de Lie semi-simples. Nous dirons alors qu'il est sans facteur compact si aucun de ces groupes simples n'est compact.

Théorème 1.4.4 (Borel [17])**.** *Si G est un groupe de Lie semi-simple sans facteur compact, les réseaux de G sont Zariski denses dans G.*

Notons que cette condition est évidemment nécessaire. En effet, si K est un groupe compact, le sous-groupe trivial est un réseau de K ! Plus précisément, si K est un groupe de Lie semi-simple compact, ses sous-groupes Zariski denses sont exactement ses sous-groupes denses au sens usuel.

1.4.2 Déformations de groupes fondamentaux de variétés hyperboliques

Si G est un groupe localement compact et Γ un groupe de type fini l'ensemble $\mathcal{R}(\Gamma, G)$ des homomorphismes de Γ dans G peut être muni d'une topologie localement compacte naturelle. En effet, si S est une partie génératrice de Γ, cet ensemble s'identifie naturellement à

$$\{(g_s)_{s\in S} \in G^S | \forall r \in \mathbb{N} \quad \forall (n_i, s_i)_{1\leq i\leq r} \in (\mathbb{Z}\times\Gamma)^r \\ s_1^{n_1} s_2^{n_2} \dots s_r^{n_r} = e \Rightarrow g_{s_1}^{r_1} g_{s_2}^{r_2} \dots g_{s_r}^{n_r} = e\}$$

et la topologie induite par cette identification sur $\mathcal{R}(\Gamma, G)$ ne dépend pas de S.

Soient G et H des groupes de Lie semi-simples et Γ un réseau de H. Supposons donné un morphisme lisse de noyau fini $\rho : H \to G$. La restriction $\rho_{|\Gamma}$ de ρ à Γ est donc un élément de $\mathcal{R}(\Gamma, G)$ d'image discrète. On peut alors se demander s'il existe des éléments ϱ de $\mathcal{R}(\Gamma, G)$ qui sont d'image discrète et Zariski dense et proches de $\rho_{|\Gamma}$ dans $\mathcal{R}(\Gamma, G)$. L'existence de telles déformations rencontre des obstructions de nature algébrique qui sont décrites par le théorème de Weil (voir [14]). Cependant, il existe des cas où cette constrcution est possible :

Théorème 1.4.5 (Johnson-Millson [10])**.** *Pour tout $n \geq 2$, il existe un réseau co-compact Γ de $\mathrm{SO}(1,n)$ tel que la restriction à Γ de la représentation naturelle de $\mathrm{SO}(1,n)$ dans $\mathrm{SL}_{n+1}(\mathbb{R})$ se déforme en un morphisme d'image discrète et Zariski dense.*

1.4.3 Groupes de Schottky

Nous allons à présent introduire un dernier exemple de sous-groupe discret Zariski dense dont la construction est complètement explicite et permet d'effectuer de nombreux calculs. Pour ce faire, nous allons avoir besoin de compléter nos connaissances sur les éléments loxodromiques.

Si $\mathbb{K}$ est un corps et V un $\mathbb{K}$-espace vectoriel, deux drapeaux complets $\xi = (V_0, V_1, \dots, V_n)$ et $\eta = (W_0, W_1, \dots, W_n)$ de V sont en position générale si, pour tout $0 \leq i \leq n$, on a $V_i \cap W_{n-i} = \{0\}$ (ce qui revient à dire que ces deux sous-espaces engendrent V).

Exemple 1.4.6. Si $\dim V = 2$, les drapeaux complets sont des droites de V. Deux droites sont en position générale si elles sont distinctes. Si $\dim V = 3$, les drapeaux complets sont des couples (V_1, V_2), où V_1 est une droite et V_2 un plan de V. Les couples (V_1, V_2) et (W_1, W_2) sont en position générale si V_1 n'est pas contenu dans W_2 et W_1 n'est pas contenu dans V_2.

Reprenons les notations du paragraphe 1.2 et notons $\xi_0^\vee$ le drapeau $(\{0\}, \mathbb{K}e_n, \mathbb{K}e_n \oplus \mathbb{K}e_{n-1}, \ldots, \mathbb{K}^n)$, qui est en position générale avec ξ_0. Si g est un élément de MA^{++}, l'action de g dans $\mathcal{B}$ admet ξ_0 pour point fixe attracteur. On vérifie aisément que son bassin d'attraction est $\mathcal{B} \setminus \mathcal{Q}_0$, où $\mathcal{Q}_0$ est l'ensemble des drapeaux complets qui ne sont pas en position générale avec $\xi_0^\vee$.

Par conséquent, si g est un élément loxodromique de $G = \mathrm{SL}_n(\mathbb{R})$ ou $\mathrm{SL}_n(\mathbb{C})$, il possède un unique point fixe attracteur ξ_g^+ dans $\mathcal{B}$ et le complémentaire du bassin d'attraction de ce point fixe est l'ensemble $\mathcal{Q}_g^-$ des éléments de $\mathcal{B}$ qui ne sont pas en position générale avec le point fixe attracteur de g^{-1}.

Fixons-nous dorénavant des éléments loxodromiques $g_1, \ldots, g_r$ de G et supposons que pour tout $1 \leq i \neq j \leq r$, on a $\xi_{g_i}^+ \notin \mathcal{Q}_{g_j}^- \cup \mathcal{Q}_{g_j^{-1}}^-$ et $\xi_{g_i^{-1}}^+ \notin \mathcal{Q}_{g_j}^- \cup \mathcal{Q}_{g_j^{-1}}^-$.

Proposition 1.4.7 (Benoist, [3])**.** *Il existe un entier p tel que $g_1^p, \ldots, g_r^p$ engendrent un sous-groupe libre et discret de G.*

La démonstration de cette proposition est une simple application de la méthode du tennis de table de Klein. La condition assurant que $g_1^p, \ldots, g_r^p$ engendrent un sous-groupe libre et discret de G étant ouverte, on peut, quitte à modifier légèrement certains des générateurs, supposer que ce sous-groupe est Zariski dense dans G (voir [15]).

Démonstration. Quitte à remplacer les g_i, $1 \leq i \leq r$, par une puissance, on peut supposer qu'il existe dans $\mathcal{B}$ des ouverts $b_i^+ \ni \xi_{g_i}^+$, $b_i^- \ni \xi_{g_i^{-1}}^+$, $B_i^- \supset \mathcal{Q}_{g_i}^-$ et $B_i^+ \supset \mathcal{Q}_{g_i^{-1}}^-$, avec $b_i^+ \cap B_i^- = \emptyset = b_i^- \cap B_i^+ = \emptyset$, $b_i^+ \subset B_i^+$, $b_i^- \subset B_i^-$ et $g_i(\mathcal{B} \setminus B_i^-) \subset b_i^+$ et $g_i^{-1}(\mathcal{B} \setminus B_i^+) \subset b_i^-$, $1 \leq i \leq r$, tels que, pour tous $1 \leq i \neq j \leq r$, on ait $b_i^+ \cap B_j^- = b_i^+ \cap B_j^+ = b_i^- \cap B_j^- = b_i^- \cap B_j^+ = \emptyset$ et que $\bigcup_{1 \leq i \leq r} B_i^- \cup B_i^+$ ne soit pas dense dans $\mathcal{B}$. Alors, si $\epsilon_1, \ldots, \epsilon_l$ sont des éléments de $\{\pm 1\}$, $t_1, \ldots, t_l$ des entiers non nuls et $h_1, \ldots, h_l$ des éléments de $\{g_1, \ldots, g_r\}$ avec, pour $1 \leq k \leq l-1$, $h_k \neq h_{k+1}$, on a $h_l^{\epsilon_l t_l} \ldots h_1^{\epsilon_1 t_1}(\mathcal{B} \setminus B_1^{-\epsilon_1}) \subset b_l^{\epsilon_l}$. En particulier, si ξ est un point intérieur de $\mathcal{B} \setminus \bigcup_{1 \leq i \leq r} B_i^- \cup B_i^+$, on a $h_l^{\epsilon_l t_l} \ldots h_1^{\epsilon_1 t_1} \xi \in \bigcup_{1 \leq i \leq r} B_i^- \cup B_i^+$. Donc $h_l^{\epsilon_l t_l} \ldots h_1^{\epsilon_1 t_1}$ est non trivial dans G

et il n'appartient pas au voisinage de l'identié constitué de l'ensemble des g dans G tels que $g\xi \notin \bigcup_{1\leq i\leq r} B_i^- \cup B_i^+$. La proposition en découle. $\square$

Exemple 1.4.8. Pour $t > \frac{1}{4}\log(3+2\sqrt{2})$, les matrices

$$\begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix} \text{ et } \begin{pmatrix} \cosh t & \sinh t \\ -\sinh t & \cosh t \end{pmatrix}$$

engendrent un sous-groupe discret, libre et Zariski dense de $\mathrm{SL}_2(\mathbb{R})$.

1.5 Résultats de comptage

Nous allons à présent décrire les résultats connus sur le comptage asymptotique dans les sous-groupes discrets des groupes de Lie semi-simples. Commençons par un résultat général

Théorème 1.5.1 ([12]). *Soit G un groupe de Lie semi-simple de centre fini et K un sous-groupe compact maximal de G. Munissons G/K d'une métrique riemannienne G-invariante. Alors, si Γ est un sous-groupe discret Zariski dense de G, il existe $\delta > 0$ tel que, pour tout x dans G/K, on ait*

$$\frac{1}{a}\log \sharp\{\gamma \in \Gamma | d(x,\gamma x) \leq a\} \xrightarrow[a\to\infty]{} \delta$$

et

$$\sharp\{\gamma \in \Gamma | d(x,\gamma x) \leq a\} \underset{a\to\infty}{=} O\left(a^{r-1}e^{a\tau}\right),$$

où r est le rang réel de G.

Notons que le rang réel de $\mathrm{SL}_n(\mathbb{R})$ est $n-1$.

L'estimation précise de ces quantités est connue dans deux cas. Dans le cas des réseaux, on a le

Théorème 1.5.2 (Eskin-McMullen, [6]). *Soit G un groupe de Lie semi-simple de centre fini et K un sous-groupe compact maximal de G. Munissons G/K d'une métrique riemannienne G-invariante et de la forme volume associée et G de la mesure de Haar λ associée au choix de cette forme volume et de la mesure de Haar de masse totale 1 de K. Alors, si Γ est un réseau de G, pour tout x dans G/K, on a*

$$\sharp\{\gamma \in \Gamma | d(x,\gamma x) \leq a\} \underset{a\to\infty}{\sim} \frac{1}{\lambda(G/\Gamma)}\mathrm{vol}(b(x,a)).$$

Notons que, d'après [9], il existe $C > 0$ avec $\mathrm{vol}(b(x,a)) \underset{a\to\infty}{\sim} Ca^{\frac{r-1}{2}}e^{\delta_G a}$, où r est le rang réel de G et δ_G est un réel > 0.

Dans le cas des groupes de Schottky, on a le

Théorème 1.5.3 ([13]). *Soit G un groupe de Lie semi-simple de centre fini et K un sous-groupe compact maximal de G. Munissons G/K d'une métrique riemannienne G-invariante. Alors, si Γ est un sous-groupe de Schottky de G, il existe $\delta > 0$ tel que, pour tout x dans G/K, on ait*

$$\sharp\{\gamma \in \Gamma | d(x, \gamma x) \leq a\} \underset{a\to\infty}{\sim} Ce^{\delta a}.$$

Dans la suite de ce cours, nous allons donner la démonstration du théorème 1.5.1 dans le cas où G est le groupe $\mathrm{SL}_3(\mathbb{R})$.

Chapitre 2

Produit générique

La démonstration du théorème 1.5.1 repose essentiellement sur la

Proposition 2.0.4. *Soit Γ un sous-groupe discret Zariski dense de G. Il existe une application $\pi : \Gamma \times \Gamma \to \Gamma$ ayant les propriétés suivantes :*

(i) il existe un réel $M \geq 0$ tel que, pour tous g, h dans Γ, on ait :

$$\|\kappa(\pi(g,h)) - \kappa(g) - \kappa(h)\| \leq M.$$

(ii) pour tout réel $R \geq 0$, il existe une partie finie H de Γ telle que, pour g, h, g', h' dans Γ, avec $\|\kappa(g) - \kappa(g')\| \leq R$ et $\|\kappa(h) - \kappa(h')\| \leq R$, on ait :

$$\pi(g,h) = \pi(g',h') \Rightarrow (g' \in gH \text{ et } h' \in Hh).$$

Pour beaucoup de couples g, h, $\pi(g,h)$ est simplement le produit de g et h. Plus généralement $\pi(g,h)$ sera de la forme gfh où f sera choisi dans une partie finie de Γ de façon judicieuse.

2.1 Composante de Cartan du produit générique

Nous supposons donc dorénavant que G est $\mathrm{SL}_3(\mathbb{R})$. Nous notons (e_1^*, e_2^*, e_3^*) la base duale de (e_1, e_2, e_3). Si ρ est la représentation standard de G dans $\mathbb{R}^3$, sa représentation contragradiante ρ^* dans l'espace dual $(\mathbb{R}^3)^*$ de $\mathbb{R}^3$ vérifie, pour tout g dans G, $\rho^*(g) = (g^{-1})^*$. Nous munissons $\mathbb{R}^3$ et son espace dual du produit scalaire usuel. Alors l'espace projectif $\mathbb{P}(\mathbb{R}^3)$ est naturellement muni de la distance telle que, pour toutes droites V et W de $\mathbb{R}^3$, pour tout vecteurs non nuls v de V et w de W, on ait

$$d(V,W) = \frac{\|v \wedge w\|}{\|v\| \, \|w\|}.$$

On munit l'espace projectif du dual de $\mathbb{R}^3$ de la distance analogue.

Pour g dans G, on fixe une fois pour toutes k_g et l_g dans K avec $g = k_g \exp(\kappa(g)) l_g$ et on note $V_g^M = k_g \mathbb{R} e_1$, $V_g^m = l_g^{-1}(\mathbb{R}e_2 \oplus \mathbb{R}e_3)$, $V_g^{*,M} = k_g \mathbb{R} e_3^*$ et $V_g^{*,m} = l_g^{-1}(\mathbb{R}e_1^* \oplus \mathbb{R}e_2^*)$. Notons que, par construction, on a $\kappa(g) = (\log \|\rho(g)\|, \log \|\rho^*(g)\| - \log \|\rho(g)\|, -\log \|\rho^*(g)\|)$. Le lemme suivant nous permettra de calculer la composante de Cartan des produits utilisés pour construire l'application π. On fixe une norme $\|.\|$ sur $\mathfrak{a}$.

Lemme 2.1.1. *Soient $\varepsilon > 0$ et F une partie compacte de G. Il existe $M \geq 0$ tel que, pour tous g, h dans G et f dans F, si $d(fV_h^M, \mathbb{P}(V_g^m)) \geq \varepsilon$ et $d(fV_h^{M,*}, \mathbb{P}(V_g^{*,m})) \geq \varepsilon$, on a*

$$\|\kappa(gfh) - \kappa(g) - \kappa(h)\| \leq M.$$

Démonstration. Soient a dans A^+ et $v \neq 0$ dans $\mathbb{R}^3$ tels qu'on ait $d(\mathbb{R}v, \mathbb{P}(\mathbb{R}e_2 \oplus \mathbb{R}e_3)) \geq \varepsilon$. Posons $v = (v_1, v_2, v_3)$, de sorte que $|v_1| \geq \varepsilon \|v\|$. Il vient

$$\|\rho(a)v\| \geq a_1 |v_1| \geq \varepsilon a_1 \|v\| = \varepsilon \|\rho(a)\| \, \|v\| .$$

Par conséquent, pour tout g dans G, si $v \neq 0$ est tel que $d(\mathbb{R}v, \mathbb{P}(V_g^m)) \geq \varepsilon$, on a $\|\rho(g)v\| \geq \varepsilon \|\rho(g)\| \, \|v\|$.

Alors, si f, g, h sont comme dans l'énoncé, on a, d'une part

$$\|\rho(gfh)\| \leq \|\rho(g)\| \, \|\rho(f)\| \, \|\rho(h)\| \leq \max_{f' \in F} \|\rho(f')\| \, \|\rho(g)\| \, \|\rho(h)\|$$

et, d'autre part, si $v \neq 0$ est un vecteur de $h^{-1}V_h^M$, par construction, $\|\rho(h)v\| = \|\rho(h)\| \, \|v\|$, si bien que, d'après la remarque ci-dessus,

$$\begin{aligned} \|\rho(gfh)v\| &\geq \varepsilon \|\rho(g)\| \, \|\rho(fh)v\| \geq \varepsilon \|\rho(g)\| \left\|\rho(f)^{-1}\right\|^{-1} \|\rho(h)v\| \\ &\geq \varepsilon \max_{f' \in F} \left\|\rho(f')^{-1}\right\|^{-1} \|\rho(g)\| \, \|\rho(h)\| \, \|v\| , \end{aligned}$$

si bien que $\|\rho(gfh)\| \geq \varepsilon \max_{f' \in F} \|\rho(f')^{-1}\|^{-1} \|\rho(g)\| \, \|\rho(h)\|$. Le résultat en découle, en raisonnant de manière analogue dans l'espace dual de $\mathbb{R}^3$. $\square$

2.2 Lemme de l'ombre

Nous allons à présent introduire l'outil principal permettant de montrer le point *(ii)* de la proposition 2.0.4, c'est-à-dire un contrôle d'injectivité. Le lemme suivant peut se voir comme une contraposée du lemme de l'ombre de Sullivan dont l'utilisation est fréquente en géométrie hyperbolique et qui assure que l'ombre, vue du point de référence o, d'une boule de rayon $r > 0$ centrée autour de son image go par une isométrie g contient l'image par g du complémentaire d'une certaine boule de rayon $\varepsilon > 0$ dans le bord, muni de la métrique associée à o, où ε ne dépend que de r et peut être rendu arbitrairement petit en augmentant r.

On note $B^\vee$ le groupe des matrices triangulaires inférieures dans $\mathrm{SL}_3(\mathbb{R})$. L'ensemble $B^\vee\xi_0$ est exactement l'ensemble des éléments de $\mathcal{B}$ qui sont en position générale avec $\xi_0^\vee$.

Lemme 2.2.1. *Pour toute partie compacte L de $B^\vee$, il existe une partie compacte M de G telle que, pour tous a dans A^+ et k dans K, si $k\xi_0$ appartient à $aL\xi_0$, on ait $a^{-1}ka \in M$.*

Démonstration. Notons que, pour toute partie relativement compacte M de B (resp. $B^\vee$), l'ensemble $\bigcup_{a\in A^+} a^{-1}Ma$ (resp. $\bigcup_{a\in A^+} aMa^{-1}$) est relativement compact. En particulier, on peut supposer que, pour tout a dans A^+, on a $aLa^{-1} \subset L$.

Soient k dans K et a dans A^+ avec $k\xi_0 \in aL\xi_0$. Ecrivons $k\xi_0 = ap\xi_0$, où p est un élément de L, c'est-à-dire $ap = kq$, avec q dans B. Alors, on a $a^{-1}ka = a^{-1}(apq^{-1})a = p(a^{-1}q)^{-1}$. Or, on a $a^{-1}q = a^{-1}(qa^{-1})a$ et, comme $q = k^{-1}ap$, $qa^{-1} = k^{-1}apa^{-1} \in KL$. Soit L' l'ensemble relativement compact $\bigcup_{b\in A^+} b^{-1}(KL \cap PA)b$. On a $a^{-1}q \in L'$ et, donc, $a^{-1}ka \in L(L')^{-1}$, d'où le résultat. □

Nous allons à présent énoncer le résultat qui nous servira à démontrer le contrôle d'injectivité de la proposition 2.0.4 et qui est une conséquence du lemme 2.2.1. Remarquons que l'espace $\mathcal{B}$ des drapeaux complets de $\mathbb{R}^3$ se plonge de manière naturelle dans $\mathbb{P}(\mathbb{R}^3) \times \mathbb{P}((\mathbb{R}^3)^*)$. Pour tout ξ dans $\mathcal{B}$, notons V_ξ et V_ξ^* les deux droites associées dans $\mathbb{P}(\mathbb{R}^3)$ et $\mathbb{P}((\mathbb{R}^3)^*)$. Pour g dans G et pour $\varepsilon > 0$, notons B_g^ε l'ensemble des ξ dans $\mathcal{B}$ tels que $d(V_\xi, V_g^m) \geq \varepsilon$ et $d(V_\xi^*, V_g^{*,m}) \geq \varepsilon$. Par construction, il existe une partie compacte L de $B^\vee$ telle que, pour tout g dans G, on ait $B_g^\varepsilon = l_g^{-1}L\xi_0$. Pour X, Y dans $\mathfrak{a}$ et $C \geq 0$, on note $X \geq Y$ si et seulement si $X_1 \geq X_2 - C$ et $X_2 \geq X_3 - C$.

Lemme 2.2.2. *Pour tous $C \geq 0$ et $\varepsilon > 0$, il existe une partie compacte M de G telle que, pour tous g, h dans G avec $\kappa(h) \geq_C \kappa(g)$, si $gB_g^\varepsilon \cap hB_h^\varepsilon \neq \emptyset$, on a $g \in k_h \exp(\kappa(g))M$.*

En d'autres termes, la connaissance de la composante de Cartan de G et de l'ensemble gB_g^ε permet de reconstituer g à un compact près.

Démonstration. Notons $A^C = \{a \in A | a_1 \geq e^C a_2 \geq e^{2C} a_3\}$. Soit L une partie compacte de $B^\vee$ telle que, pour tout g dans G, on ait $B_g^\varepsilon \subset l_g^{-1} L\xi_0$ et soit L' l'ensemble relativement compact $\bigcup_{a \in A^C} aLa^{-1}$. D'après le lemme 2.2.1, il existe une partie compacte M de G telle que, pour tous a dans A^+ et k dans K, si $k\xi_0$ appartient à $aL'\xi_0$, on ait $a^{-1}ka \in M$.

Soient alors g et h comme dans l'énoncé. On a $gB_g^\varepsilon \subset k_g \exp(\kappa(g))L\xi_0 \subset k_g \exp(\kappa(g))L'\xi_0$ et, comme $\kappa(h) \geq_C \kappa(g)$, $hB_h^\varepsilon \subset k_h \exp(\kappa(h))L\xi_0 \subset k_h \exp(\kappa(g))L'\xi_0$. En particulier, on a $k_g \exp(\kappa(g))L'\xi_0 \cap k_h \exp(\kappa(g))L'\xi_0 \neq \emptyset$. Soit ξ un élément de cette intersection et soit k dans K tel que $\xi = k\xi_0$. On a $k_g^{-1}k\xi_0 \in \exp(\kappa(g))L'\xi_0$ donc $\exp(-\kappa(g))k_g^{-1}k\exp(\kappa(g)) \in M$ et, de même, $\exp(-\kappa(g))k_h^{-1}k\exp(\kappa(g)) \in M$. Il vient donc

$$g \in k_g \exp(\kappa(g))K \subset k\exp(\kappa(g))M^{-1}K \subset k_h \exp(\kappa(g))MM^{-1}K,$$

d'où le résultat.□

2.3 Produit générique dans G

Nous allons à présent appliquer le lemme 2.2.2 à l'estimation, pour f, g, h dans G, de la décomposition de Cartan de g en fonction de celle de gfh, à condition que soient vérifiées les hypothèses du lemme 2.1.1.

Lemme 2.3.1. *Soient $\varepsilon > 0$ et F une partie compacte de G. Il existe une partie compacte M de G telle que, pour tous g, h dans G et f dans F avec $d(fV_h^M, \mathbb{P}(V_g^m)) \geq \varepsilon$ et $d(fV_h^{*,M}, \mathbb{P}(V_g^{*,m})) \geq \varepsilon$, on ait $g \in k_{gfh}\exp(\kappa(g))M$.*

Ce résultat repose sur le lemme 2.2.2 et sur les estimations suivantes d'algèbre linéaire qui permettront d'en valider les hypothèses.

Lemme 2.3.2. *Pour tous g dans G et $\varepsilon > 0$, la restriction de g à l'ensemble $\{X \in \mathbb{P}(\mathbb{R}^3) | d(X, \mathbb{P}(V_g^m)) \geq \varepsilon\}$ est $\frac{1}{\varepsilon^2}$-lipschitzienne.*

Démonstration. Par décomposition de Cartan, il suffit de démontrer ce résultat pour $g = a$ appartenant à A^+. Alors, pour v et w dans $\mathbb{R}^3 \setminus \{0\}$ avec $d(\mathbb{R}v, \mathbb{P}\left(V_g^m\right)) \geq \varepsilon$ et $d(\mathbb{R}w, \mathbb{P}\left(V_g^m\right)) \geq \varepsilon$, on a, d'une part $\|av\| \geq a_1 |v_1| \geq \varepsilon a_1 \|v\|$ et, de même, $\|aw\| \geq \varepsilon a_1 \|w\|$, et, d'autre part, $\|a(v \wedge w)\| \leq \|a\|^2 \|v \wedge w\| = a_1^2 \|v \wedge w\|$, si bien que

$$d(a\mathbb{R}v, a\mathbb{R}w) = \frac{\|a(v \wedge w)\|}{\|av\| \|aw\|} \leq \frac{1}{\varepsilon^2} d(\mathbb{R}v, \mathbb{R}w),$$

ce qu'il fallait démontrer. $\square$

Lemme 2.3.3. *Soient $\varepsilon, \eta > 0$. Il existe $\varpi > 0$ tel que, pour tout g dans G, pour tout hyperplan W de $\mathbb{R}^3$ avec $d(V_g^M, \mathbb{P}(W)) \geq \varepsilon$, on ait*

$$g^{-1} b(\mathbb{P}(W), \varpi) \subset b(\mathbb{P}\left(g^{-1}W\right), \eta).$$

Démonstration. On vérifie aisément que, pour $v \neq 0$ dans $\mathbb{R}^3$ et $\varphi \neq 0$ dans $(\mathbb{R}^3)^*$, on a $d(\mathbb{R}v, \mathbb{P}(\ker \varphi)) = \frac{|\varphi(v)|}{\|\varphi\| \|v\|}$. Par ailleurs, pour g dans G, on a $V_{g^*}^{*,m} = (V_g^M)^\perp$, si bien que si $v \neq 0$ est dans $\mathbb{R}^3$ et $\varphi \neq 0$ est dans $(\mathbb{R}^3)^*$ avec $d(\mathbb{R}v, \mathbb{P}(\ker \varphi)) \leq \frac{\varepsilon}{2}$ et $d(V_g^M, \mathbb{P}(\ker \varphi)) \geq \varepsilon)$, on a aussi $d(\mathbb{R}\varphi, \mathbb{P}\left(v^\perp\right)) \leq \frac{\varepsilon}{2}$ et $d(\mathbb{R}\varphi, V_{g^*}^{*,m}) \geq \varepsilon$. D'après le lemme 2.3.2, appliqué dans $(\mathbb{R}^3)^*$, il vient $d(g^*\mathbb{R}\varphi, g^*\mathbb{P}\left(v^\perp\right)) \leq \frac{4}{\varepsilon^2} d(\mathbb{R}\varphi, \mathbb{P}\left(v^\perp\right))$. En d'autres termes, pour tout $0 < \eta \leq \frac{\varepsilon}{2}$, on a $g^{-1} b(\mathbb{P}(\ker \varphi), \eta) \subset b(\mathbb{P}(g^{-1} \ker \varphi), \frac{4}{\varepsilon^2}\eta)$. Le résultat en découle. $\square$

Démonstration du lemme 2.3.1. D'après le lemme 2.1.1, il existe $C \geq 0$ tel que, pour tous g, f, h comme dans l'énoncé, on a $\kappa(gfh) \geq_C \kappa(g)$ si bien que, pour appliquer le lemme 2.2.2, il suffit de garantir que, pour un certain $\varpi > 0$, on a $gB_g^\varpi \cap gfhB_{gfh}^\varpi \neq \emptyset$, c'est-à-dire $h^{-1}f^{-1}B_g^\varpi \cap B_{gfh}^\varpi \neq \emptyset$.

Choisissons $\theta > 0$ suffisament petit pour que, pour tous hyperplans W_1, W_2 dans $\mathbb{R}^3$ et W_1^*, W_2^* dans $(\mathbb{R}^3)^*$, il existe un drapeau complet (V, V^*) dans $\mathcal{B}$ avec $d(V, \mathbb{P}(W_1) \cup \mathbb{P}(W_2)) \geq \theta$ et $d(V^*, \mathbb{P}(W_1^*) \cup \mathbb{P}(W_2^*)) \geq \theta$. Soit $\eta > 0$ tel que, pour tous f dans F et X, Y dans $\mathbb{P}(\mathbb{R}^3)$ (resp. $\mathbb{P}((\mathbb{R}^3)^*)$) avec $d(X,Y) \leq \eta$, on ait $d(f^{-1}X, f^{-1}Y) \leq \varepsilon$. D'après le lemme 2.3.3, il existe $\omega > 0$ tel que, pour tout h dans G et pour tout plan W de $\mathbb{R}^3$ (resp.W^* de $(\mathbb{R}^3)^*$) tel que $d(V_h^M, \mathbb{P}(W)) \geq \theta$) (resp. $d(V_h^{*,M}, \mathbb{P}(W^*)) \geq \theta$)), on ait $h^{-1} b(\mathbb{P}(W), \omega) \subset b(\mathbb{P}(h^{-1}W), \theta)$ (resp. $h^{-1} b(\mathbb{P}(W^*), \omega) \subset b(\mathbb{P}(h^{-1}W^*), \theta)$). Enfin, il existe $0 < \varpi \leq \theta$ tel que, pour tous f dans F et X, Y dans $\mathbb{P}(\mathbb{R}^3)$ (resp. $\mathbb{P}((\mathbb{R}^3)^*)$) avec $d(X,Y) \leq \varpi$, on ait $d(f^{-1}X, f^{-1}Y) \leq \omega$. Alors, pour tous f dans F et g, h dans G avec $d(fV_h^M, \mathbb{P}(V_g^m)) \geq \varepsilon$ et $d(fV_h^{*,M}, \mathbb{P}(V_g^{*,m})) \geq \varepsilon$, on a $h^{-1}f^{-1}b(\mathbb{P}(V_g^m), \varpi) \subset b(\mathbb{P}(h^{-1}f^{-1}V_g^m), \theta)$ et $h^{-1}f^{-1}b(\mathbb{P}(V_g^{*,m}), \varpi) \subset b(\mathbb{P}(h^{-1}f^{-1}V_g^{*,m}), \theta)$. Par conséquent, par définition de θ, il existe un drapeau $\xi = (V, V^*)$ dans $\mathcal{B}$ tel que $d(V, V_{gfh}^m) \geq \theta \geq \varpi$ et $d(V^*, V_{gfh}^{*,m}) \geq \theta \geq \varpi$, c'est-à-dire que ξ appartient à B_{gfh}^{ϖ}, ainsi que $d(hfV, V_g^m) \geq \varpi$ et $d(hfV^*, V_g^{*,m}) \geq \varpi$, c'est-à-dire que $hf\xi$ appartient à B_g^{ϖ}. Il vient bien $h^{-1}f^{-1}B_g^{\varpi} \cap B_{gfh}^{\varpi} \neq \emptyset$ et le lemme découle alors directement du lemme 2.2.2. $\square$

2.4 Le lemme de finitude d'Abels-Margulis-Soifer

Il nous reste, pour construire l'application π de la proposition 2.0.4, à construire, dans tout sous-groupe Zariski dense Γ de G, une partie F telle que, pour tous g, h dans Γ, il existe f dans F tel que f, g, h vérifient les hypothèses des lemmes 2.1.1 et 2.3.1. C'est l'objet du lemme suivant.

Lemme 2.4.1 (Abels-Margulis-Soifer [1]). *Soit Γ un sous-groupe Zariski dense de G. Il existe $\varepsilon > 0$ et une partie finie F de Γ ayant la propriété suivante : pour toutes droites V dans $\mathbb{R}^3$ et V^* et $(\mathbb{R}^3)^*$, pour tous hyperplans W dans $\mathbb{R}^3$ et W^* et $(\mathbb{R}^3)^*$, il existe f dans F tel que $d(fV, \mathbb{P}(W)) \geq \varepsilon$ et $d(fV^*, \mathbb{P}(W^*)) \geq \varepsilon$.*

Démonstration. D'après la proposition 1.3.1, Γ contient un élément loxodromique g. Alors, l'action de g dans $\mathbb{P}(\mathbb{R}^3)$ est proximale : si V^+ désigne la droite propre associée à sa plus grande valeur propre en module, V^+ est un point fixe attracteur pour l'action de g sur $\mathbb{P}(\mathbb{R}^3)$ et son bassin d'attraction est $\mathbb{P}(\mathbb{R}^3) \setminus \mathbb{P}(W^-)$, où W^- est le plan engendré par les deux autres droites propres de g. De même, on note $V^{*,+}$ la droite propre associée à la plus grande valeur propre de $\rho^*(g)$ dans l'espace dual de $\mathbb{R}^3$, et $W^{*,-}$ son unique supplémentaire g-stable.

Soit l un entier ≥ 1 et $V_1, \ldots, V_l$ des droites distinctes de $\mathbb{R}^3$, $V_1^*, \ldots, V_l^*$ des droites distinctes de l'espace dual de $\mathbb{R}^3$, $W_1, \ldots, W_l$ des plans distincts de $\mathbb{R}^3$ et $W_1^*, \ldots, W_l^*$ des plans distincts de l'espace dual de $\mathbb{R}^3$. Il existe des droites V dans $\mathbb{R}^3$ et V^* dans l'espace dual de $\mathbb{R}^3$, ainsi que des plans W dans $\mathbb{R}^3$ et W^* dans l'espace dual de $\mathbb{R}^3$ tels que, pour tout $1 \leq i \neq j \leq l$, V (resp.

V^*) n'appartienne pas au plan engendré par V_i et V_j (resp. V_i^* et V_j^*) et W (resp. W^*) ne contienne pas l'intersection de W_i et de W_j (resp. de W_i^* et de W_j^*). Comme Γ est Zariski dense dans G qui est Zariski connexe, il existe h dans Γ tel que hV^+ (resp. $hV^{*,+}$) n'appartienne pas au plan engendré par V_i et V_j (resp. V_i^* et V_j^*) et hW^- (resp. $hW^{-,*}$) ne contienne pas l'intersection de W_i et de W_j (resp. de W_i^* et de W_j^*). Ainsi, par récurrence, il existe une suite $(h_i)_{i\geq 1}$ d'éléments de Γ, tels que, pour tous $i, j, k \geq 1$ distincts, les droites h_iV^+, h_jV^+ et h_kV^+ (resp. $h_iV^{+,*}$, $h_jV^{+,*}$ et $h_kV^{+,*}$) engendrent $\mathbb{R}^3$ (resp. l'espace dual de $\mathbb{R}^3$) et l'intersection des plans h_iW^-, h_jW^- et h_kW^- (resp. $h_iW^{-,*}$, $h_jW^{-,*}$ et $h_kW^{-,*}$) est triviale. On pose, pour tout $i \geq 1$, $V_i = h_iV^+$, $V_i^* = h_iV^{*,+}$, $W_i = h_iW^-$, $W_i^* = h_iW^{*,-}$ et $g_i = h_igh_i^{-1}$.

Par construction, si V et V^* sont des droites de $\mathbb{R}^3$ et de l'espace dual de $\mathbb{R}^3$ et si W et W^* sont des plans de $\mathbb{R}^3$ et de l'espace dual de $\mathbb{R}^3$, il existe $1 \leq i \leq 9$ tel qu'on ait

$$\begin{array}{ll} V \not\subset W_i & V^* \not\subset W_i^* \\ V_i \not\subset W & V_i^* \not\subset W^* \end{array}$$

et, donc, il existe $\varepsilon > 0$ tel que pour tous V, V^*, W, W^* comme ci-dessus, on puisse trouver $1 \leq i \leq 9$ avec

$$\begin{array}{ll} d(V, \mathbb{P}(W_i) \geq 2\varepsilon & d(V^*, \mathbb{P}(W_i^*)) \geq 2\varepsilon \\ d(V_i, \mathbb{P}(W)) \geq 2\varepsilon & d(V_i^*, \mathbb{P}(W^*)) \geq 2\varepsilon. \end{array}$$

Il existe un entier k tel que, pour tout $1 \leq i \leq 9$, on ait $g_i^k\{X \in \mathbb{P}(V) \,|\, d(X, \mathbb{P}(W_i)) \geq \varepsilon\} \subset b(V_i, \varepsilon)$. Par conséquent, si V, V^*, W, W^* sont comme ci-dessus, il existe un entier $1 \leq i \leq 9$ avec

$$\begin{array}{ll} d(g^kV, V_i) \leq \varepsilon & d(g^kV^*, V_i^*) \leq \varepsilon \\ d(V_i, \mathbb{P}(W)) \geq 2\varepsilon & d(V_i^*, \mathbb{P}(W^*)) \geq 2\varepsilon. \end{array}$$

Le résultat en découle, en posant $F = \{g_i^k | 1 \leq i \leq 9\}$. $\square$

2.5 Produit générique dans Γ

Nous pouvons à présent conclure la

Démonstration de la proposition 2.0.4. Soient $\varepsilon > 0$ et F comme dans le lemme 2.4.1. Pour tous g et h dans Γ, choisissons $f_{g,h}$ dans F avec

$d(f_{g,h}V_h^M, \mathbb{P}\left(V_g^m\right)) \geq \varepsilon$ et $d(f_{g,h}V_h^{*,M}, \mathbb{P}\left(V_g^{*,m}\right)) \geq \varepsilon$. Posons $\pi(g,h) = gf_{g,h}h$. D'après le lemme 2.1.1, il existe $C \geq 0$ tel que, pour tous g, h dans Γ, on ait $\|\kappa(\pi(g,h)) - \kappa(g) - \kappa(h)\| \leq C$ tandis que, d'après le lemme 2.3.1, il existe une partie compacte M de G telle que, pour tout g, h dans Γ, on a $g \in k_{\pi(g,h)} \exp(\kappa(g))M$. En particulier, si g' et h' sont des éléments de Γ tels que $\pi(g', h') = \pi(g, h)$, on a $g' \in gM^{-1} \exp(\kappa(g') - \kappa(g))M$ et donc, comme $h' = (g' f_{g',h'}^{-1})^{-1} g f_{g,h} h$, $h' \in F^{-1}M^{-1} \exp(\kappa(g') - \kappa(g))MFh$. Le résultat en découle.$\square$

Chapitre 3

Mesures à croissance concave

Nous allons à présent détailler le lien abstrait qui existe entre la proposition 2.0.4 et le théorème 1.5.1.

Soit E un espace vectoriel réel de dimension finie, muni d'une norme N. Une mesure de Radon ν sur E sera dite à croissance concave s'il existe des réels $\alpha, \beta, \gamma > 0$ tels que, pour tous x, y dans E,

$$\nu\left(b^N(x+y,\alpha)\right) \geq \gamma\nu\left(b^N(x,\beta)\right)\nu\left(b^N(y,\beta)\right).$$

La proposition 2.0.4 assure que, si Γ est un sous-groupe discret Zariski dense de G, l'image par κ de la mesure de comptage de Γ est une mesure à croissance concave sur $\mathfrak{a}$.

3.1 Exposants de convergence et formules de Hadamard

Pour tout réel t, on pose $\mathcal{L}_\nu^N(t) = \int_E e^{-tN(x)}\mathrm{d}\nu(x)$ et

$$\begin{aligned}\tau_\nu^N &= \inf\left\{t \in \mathbb{R} \,\middle|\, \mathcal{L}_\nu^N(t) < \infty\right\} \\ &= \sup\left\{t \in \mathbb{R} \,\middle|\, \mathcal{L}_\nu^N(t) = \infty\right\} \in \mathbb{R} \cup \{+\infty, -\infty\},\end{aligned}$$

qu'on appelle l'exposant de convergence de ν par rapport à N. Pour tous réels $a \leq b$, on note $C^N(a,b) = \{x \in E \,|a \leq N(x) \leq b\}$. Donnons quelques formules de Hadamard pour le calcul de τ_ν^N :

Lemme 3.1.1. *Pour tous $a > 0$ et $b, c \geq 0$ avec $b + c \geq a$, on a :*

$$\tau_\nu^N = \frac{1}{a} \limsup_{n\to\infty} \frac{\log\left(\nu\left(C^N(na-b, na+c)\right)\right)}{n}.$$

Si $\tau_\nu^N > 0$, on a :

$$\tau_\nu^N = \limsup_{a\to\infty} \frac{\log\left(\nu\left(b^N(0,a)\right)\right)}{a}.$$

Démonstration. Soient $a > 0$ et $b, c \geq 0$ avec $b + c \geq a$. Il existe un entier $n_0 > 0$ tel que, pour tout x dans E,

$$0 < \mathrm{card}\left\{n \in \mathbb{N} | x \in C^N(na-b, na+c)\right\} \leq n_0.$$

Il vient, pour tout t dans $\mathbb{R}$,

$$\begin{aligned}\frac{1}{n_0} e^{-|t|\max(b,c)} \sum_{n=0}^{\infty} \nu\left(\left(C^N(na-b, na+c)\right) e^{-tna} \leq \int_E e^{-tN(x)} \mathrm{d}\nu(x)\right. \\ \leq e^{|t|\max(b,c)} \sum_{n=0}^{\infty} \nu\left(\left(C^N(na-b, na+c)\right) e^{-tna},\right.\end{aligned}$$

d'où la première formule.

Par ailleurs, on a :

$$\begin{aligned}\tau_\nu^N = \limsup_{n\to\infty} \frac{\log\left(\nu\left(C^N(n-1,n)\right)\right)}{n} &\leq \limsup_{n\to\infty} \frac{\log\left(\nu\left(b^N(0,n)\right)\right)}{n} \\ &\leq \limsup_{a\to\infty} \frac{\log\left(\nu\left(b^N(0,a)\right)\right)}{a}.\end{aligned}$$

Supposons $\tau_\nu^N > 0$. Soient t et s avec

$$0 < t < s < \limsup_{a\to\infty} \frac{\log\left(\nu\left(b^N(0,a)\right)\right)}{a}.$$

Pour tout réel $a \geq 0$, il existe $b \geq a$ tel que, pour tout $c \geq b$, on ait :

$$e^{sc} - e^{tc} \geq \nu\left(b^N(0,a)\right)$$

et, donc, il existe $c \geq b$ tel que l'on ait :

$$\nu\left(C^N(a,c)\right) \geq \nu\left(b^N(0,c)\right) - \nu\left(b^N(0,a)\right) \geq e^{sc} - \nu\left(b^N(0,a)\right) \geq e^{tc}.$$

On peut donc construire une suite $(a_n)_{n\in\mathbb{N}}$ de réels ≥ 0 avec, pour tout n dans $\mathbb{N}$,

$$a_{n+1} \geq a_n + 1 \text{ et } \nu\left(C^N(a_n+1, a_{n+1})\right) \geq e^{ta_{n+1}}.$$

Il vient alors :

$$\int_E e^{-tN(x)} \mathrm{d}\nu(x) \geq \sum_{n=0}^{\infty} \nu\left(C^N(a_n+1, a_{n+1})\right) e^{-ta_{n+1}} = \infty,$$

donc $t \leq \tau_\nu^N$, d'où la seconde formule. □

3.2 Contrôle de la divergence

Nous dirons qu'une mesure de Radon à croissance concave ν sur E est à croissance strictement divergente si $\tau_\nu^N > 0$ (ce qui est indépendant de la norme N choisie). Pour les mesures à croissance concave, on peut améliorer le lemme 3.1.1 :

Proposition 3.2.1. *Si ν est à croissance concave strictement divergente, pour toute norme N sur E, on a :*

$$\frac{\log\left(\nu\left(b^N(0,a)\right)\right)}{a} \xrightarrow[a\to\infty]{} \tau_\nu^N \text{ et } \nu\left(b^N(0,a)\right) \underset{a\to\infty}{=} O\left(a^{r-1}e^{a\tau_\nu^N}\right).$$

Commençons par itérer la formule de définition :

Lemme 3.2.2. *Supposons ν à croissance concave. Soit N une norme sur E et soient α, β, γ tels que, pour tous x, y dans E,*

$$\nu\left(b^N(x+y,\alpha)\right) \geq \gamma\nu\left(b^N(x,\beta)\right)\nu\left(b^N(y,\beta)\right).$$

Alors il existe des réels $\theta > 0$ et $\eta > 0$ tels que, pour tout entier $k \geq 2$ et pour tous $x_1, \ldots, x_k$ dans E, on ait :

$$\nu\left(b^N(x_1+\ldots+x_k, (k-1)\alpha+(k-2)\beta)\right) \\ \geq \theta\eta^k\nu\left(b^N(x_1,\beta)\right)\ldots\nu\left(b^N(x_k,\beta)\right).$$

La démonstration fait appel au lemme suivant dont la démonstration est immédiate.

Lemme 3.2.3. *Soient N une norme sur E et $\beta > 0$. Il existe un réel $M > 0$ telle que, pour tout x dans E et pour tout $a > 0$, il existe un entier $p \leq M\,(1+a)^r$ et des points $x_1, \ldots, x_p$ de E avec $b^N(x,a) \subset \bigcup_{i=1}^p b^N(x_i,\beta)$.*

Démonstration du lemme 3.2.2. Soit N une norme sur E. Donnons-nous α, β, γ comme ci-dessus et M comme dans le lemme 3.2.3.

Posons $r = \dim E$ et $\eta = \frac{1}{M(\alpha+\beta+1)^r}$ et montrons par récurrence sur $k \geq 2$ que, si l est le plus petit entier tel que $2^l \geq k$, alors, pour tous $x_1, \ldots, x_k$ dans E, on a :

$$\begin{aligned}
&\nu\left(b^N(x_1+\ldots+x_k,(k-1)\alpha+(k-2)\beta)\right) \\
&\qquad\geq \frac{\gamma^{k-1}\eta^{k-2}}{\left(2^{2(l-1)+4(l-2)+8(l-3)+\ldots+2^{l-1}}\right)^r}\nu\left(b^N(x_1,\beta)\right)\ldots\nu\left(b^N(x_k,\beta)\right).
\end{aligned}$$

Pour $k=2$, il s'agit juste de la définition de la croissance concave ; pour $k=3$, c'est un raisonnement analogue à celui fait ci-après.

Soit donc $k \geq 4$ et supposons la formule vraie pour tous les entiers $< k$. Soient l le plus petit entier tel que $2^l \geq k$ et $x_1, \ldots, x_k$ dans E. Si k est pair, on pose $h = \frac{k}{2}$; s'il est impair, on pose $h = \frac{k-1}{2}$. Dans les deux cas, on a

$$2^{l-1} \geq h > 2^{l-2} \text{ et } 2^{l-1} \geq k-h > 2^{l-2}.$$

D'après le lemme 3.2.3, il existe un point y_1 dans $b^N(x_1+\ldots+x_h,(h-1)(\alpha+\beta))$ tel que l'on ait :

$$\begin{aligned}
&\nu\left(b^N(x_1+\ldots+x_h,(h-1)\alpha+(h-2)\beta)\right) \\
&\qquad\leq M\,(1+(h-1)\alpha+(h-2)\beta)^r\,\nu\left(b^N(y_1,\beta)\right) \leq \frac{2^{r(l-1)}}{\eta}\nu\left(b^N(y_1,\beta)\right).
\end{aligned}$$

De même, il existe un point y_2 dans $b^N(x_{h+1}+\ldots+x_k,(k-h-1)(\alpha+\beta))$ tel que l'on ait :

$$\begin{aligned}
&\nu\left(b^N(x_{h+1}+\ldots+x_k,(k-h-1)\alpha+(k-h-2)\beta)\right) \\
&\leq M\,(1+(k-h-1)\alpha+(k-h-2)\beta)^r\,\nu\left(b^N(y_2,\beta)\right) \leq \frac{2^{r(l-1)}}{\eta}\nu\left(b^N(y_2,\beta)\right).
\end{aligned}$$

On a alors :

$$\begin{aligned}\nu(b^N(y_1+y_2,\alpha)) &\geq \gamma\nu(b^N(y_1,\beta))\nu(b^N(y_2,\beta))\\ &\geq \frac{\gamma\eta^2}{2^{2r(l-1)}}\nu\left(b^N(x_1+\ldots+x_h,(h-1)\alpha+(k-2)\beta)\right)\\ &\quad \nu\left(b^N(x_{h+1}+\ldots+x_k,(k-h-1)\alpha+(k-h-2)\beta)\right).\end{aligned}$$

Or, on a, par récurrence,

$$\begin{aligned}&\nu\left(b^N(x_1+\ldots+x_h,(h-1)\alpha+(h-2)\beta)\right)\\ &\qquad\geq \frac{\gamma^{h-1}\eta^{h-2}}{(2^{2(l-2)+4(l-3)+\ldots+2^{l-2}})^r}\nu\left(b^N(x_1,\beta)\right)\ldots\nu\left(b^N(x_h,\beta)\right).\end{aligned}$$

et

$$\begin{aligned}&\nu\left(b^N(x_{h+1}+\ldots+x_k,(k-h-1)\alpha+(k-h-2)\beta)\right)\\ &\qquad\geq \frac{\gamma^{k-h-1}\eta^{k-h-2}}{(2^{2(l-2)+4(l-3)+\ldots+2^{l-2}})^r}\nu\left(b^N(x_{k+1},\beta)\right)\ldots\nu\left(b^N(x_k,\beta)\right).\end{aligned}$$

Il vient :

$$\begin{aligned}&\nu\left(b^N(y_1+y_2,\alpha)\right)\\ &\qquad\geq \frac{\gamma^{k-1}\eta^{k-2}}{(2^{2(l-1)+4(l-2)+8(l-3)+\ldots+2^{l-1}})^r}\nu\left(b^N(x_1,\beta)\right)\ldots\nu\left(b^N(x_k,\beta)\right),\end{aligned}$$

d'où le résultat, puisque l'on a :

$$b^N(y_1+y_2,\alpha)\subset b^N(x_1+\ldots+x_k,(k-1)\alpha+(k-2)\beta).$$

Par récurrence, la formule est vraie pour tout $k\geq 2$. Or, pour tout $k\geq 2$, si $2^{l-1}<k\leq 2^l$, on a :

$$\begin{aligned}&2(l-1)+4(l-2)+8(l-3)+\ldots+2^{l-1}\\ &\qquad= 2^l\left(\frac{l-1}{2^{l-1}}+\frac{l-2}{2^{l-2}}+\frac{l-3}{2^{l-3}}+\ldots+\frac{1}{2}\right)\leq 2^l\sum_{h=0}^{\infty}\frac{h}{2^h}\leq 4k\end{aligned}$$

et, donc, pour tous $x_1,\ldots,x_k$ dans E, on a :

$$\begin{aligned}&\nu\left(b^N(x_1+\ldots+x_k,(k-1)\alpha+(k-2)\beta)\right)\\ &\qquad\geq \frac{\gamma^{k-1}\eta^{k-2}}{4^{kr}}\nu\left(b^N(x_1,\beta)\right)\ldots\nu\left(b^N(x_k,\beta)\right),\end{aligned}$$

ce qu'il fallait démontrer. □

Des lemmes 3.2.3 et 3.2.2, on déduit immédiatement le

Lemme 3.2.4. *Supposons ν à croissance concave. Soit N une norme sur E. Il existe des réels $\theta, \eta, \kappa > 0$ tels que, pour tout réel $a \geq 0$ et pour tous réels $a_1, \ldots, a_p$ tels que $a = a_1 + \ldots + a_p$, on ait :*

$$\nu\left(b^N(0, a + p + (p-1)\kappa)\right) \geq \frac{\theta\eta^p}{\left((1+a_1)\ldots(1+a_p)\right)^{r-1}} \nu\left(C^N(a_1, a_1+1)\right)\ldots\nu\left(C^N(a_p, a_p+1)\right).$$

Remarquons aussi le

Lemme 3.2.5. *Soit $f : \mathbb{R}_+ \to \mathbb{R}$ une fonction croissante. Alors on a :*

$$\limsup_{\substack{a\to\infty \\ a\in\mathbb{R}_+^*}} \frac{f(a)}{a} = \limsup_{\substack{n\to\infty \\ n\in\mathbb{N}^*}} \frac{f(n)}{n} \quad \text{et} \quad \liminf_{\substack{a\to\infty \\ a\in\mathbb{R}_+^*}} \frac{f(a)}{a} = \liminf_{\substack{n\to\infty \\ n\in\mathbb{N}^*}} \frac{f(n)}{n}.$$

Démonstration. Pour tout réel $a \geq 1$, on a $\frac{f([a])}{[a]+1} \leq \frac{f(a)}{a} \leq \frac{f([a]+1)}{[a]}$.□

Démonstration de la proposition 3.2.1. Soit N une norme sur E.

D'après le lemme 3.1.1, on a $\tau_\nu^N = \limsup_{a\to\infty} \frac{\log\left(\nu\left(b^N(0,a)\right)\right)}{a}$. Soient $\theta, \eta, \kappa > 0$ comme dans le lemme 3.2.4. Soient $m \geq n \geq 1$ des entiers naturels et $m = pn + q$ la division euclidienne de m par n. On a :

$$\begin{aligned}\nu\left(b^N\left(0, m\left(1 + \frac{\kappa+2}{n}\right)\right)\right) &\geq \nu\left(b^N\left(0, m + (p+1) + p\kappa\right)\right) \\ &\geq \frac{\theta\eta^{p+1}}{\left((1+n)^p(1+q)\right)^{r-1}} \\ &\quad \nu\left(C^N(n, n+1)\right)^p \nu\left(C^N(q, q+1)\right).\end{aligned}$$

Il vient, pour tout $n \geq 1$, d'après le lemme 3.2.5,

$$\left(1 + \frac{\kappa+2}{n}\right) \liminf_{a\to\infty} \frac{\log\left(\nu\left(b^N(0,a)\right)\right)}{a} \geq \left(\frac{1}{n}\log\left(\frac{\eta}{(1+n)^{r-1}}\right) + \frac{\log\left(\nu\left(C^N(n,n+1)\right)\right)}{n}\right).$$

On en déduit, en réutilisant le lemme 3.1.1 :

$$\liminf_{a\to\infty} \frac{\log\left(\nu\left(b^N(0,a)\right)\right)}{a} \geq \limsup_{n\to\infty} \frac{\log\left(\nu\left(C^N(n,n+1)\right)\right)}{n} = \tau_\nu^N$$

et, donc, $\frac{\log\left(\nu\left(b^N(0,a)\right)\right)}{a} \xrightarrow[a\to\infty]{} \tau_\nu^N$.

Mais alors, pour tout $n \geq 1$, on a :

$$(n+\kappa+2)\,\tau_\nu^N \geq \log\left(\frac{\eta}{(1+n)^{r-1}}\right) + \log\left(\nu\left(C^N(n,n+1)\right)\right)$$

d'où

$$\nu\left(C^N(n,n+1)\right) \leq \frac{1}{\eta}(1+n)^{r-1}e^{(n+\kappa+2)\tau_\nu^N}.$$

En d'autres termes, il existe un réel $M \geq 0$ tel que, pour tout entier naturel n, on ait :

$$\nu\left(C^N(n,n+1)\right) \leq M(1+n)^{r-1}e^{n\tau_\nu^N}.$$

Il vient, comme $\tau_\nu^N > 0$,

$$\nu\left(b^N(0,n)\right) \leq M\sum_{k=0}^{n-1}(1+k)^{r-1}e^{k\tau_\nu^N} \underset{n\to\infty}{=} O\left(n^{r-1}e^{n\tau_\nu^N}\right).$$

On en déduit le résultat puisque, pour tout réel $a \geq 0$, on a $b^N(0,a) \subset b^N(0,[a]+1)$. $\square$

3.3 Croissance des sous-groupes discrets

La proposition 2.0.4 assure que, si Γ est un sous-groupe Zariski dense de G, l'image par κ de la mesure de comptage de Γ est à croissance concave. Pour appliquer la proposition 3.2.1 et conclure la démonstration du théorème 1.5.1, il nous reste à montrer que les exposants de convergence de cette mesure sont > 0.

Lemme 3.3.1. *Soit Γ un sous-groupe Zariski dense de G. Alors, on a*

$$\limsup_{a\to\infty} \frac{1}{a}\log\sharp\{\gamma\in\Gamma|\,\|\kappa(\gamma)\|\leq a\} > 0.$$

Démonstration. D'après la proposition 1.3.1, Γ contient un élément loxodromique g. Comme Γ est Zariski dense dans G, il existe f dans Γ tel que $f\xi_g^+ \neq \xi_g^+$, que $f\xi_g^+ \notin \mathcal{Q}_g^-$ et que $\xi_g^+ \notin f\mathcal{Q}_g^-$. En raisonnant comme dans la proposition 1.4.7, on voit que ces conditions suffisent à garantir que, quitte à remplacer g et $h = fgf^{-1}$ par une puissance, le semi-groupe engendré par g et h est libre.

Pour $X = (X_1, X_2, X_3)$ dans $\mathfrak{a}$, posons $N(x) = \max(|X_1|, |X_2|, |X_3|)$. Alors, pour tout γ dans G, on a $N(\kappa(\gamma)) = \log(\|\gamma\|)$. En particulier, si $C = \max(\log\|g\|, \log\|h\|)$, pour tout mot γ de longueur r en g et h, on a $N(\kappa(\gamma)) \leq rC$. Il vient, pour r dans $\mathbb{N}$,

$$\sharp\{\gamma \in \Gamma | N(\kappa(\gamma)) \leq rC\} \geq 2^r$$

et, donc,

$$\limsup_{a\to\infty} \frac{1}{a} \log \sharp\{\gamma \in \Gamma | N(\kappa(\gamma)) \leq a\} \geq \frac{1}{C}\log 2,$$

d'où le résultat. □

Montrons aussi que ces exposants sont finis. Rappelons que, d'après [9], il existe $\delta_G > 0$ et $C > 0$ tels que, dans G/K, on ait $\mathrm{vol}(b(x,a)) \underset{a\to\infty}{\sim} Ca^{\frac{r-1}{2}} e^{\delta_G a}$.

Lemme 3.3.2. *Soit Γ un sous-groupe discret de G. Pour tout x dans G/K, on a*

$$\sharp\{\gamma \in \Gamma | d(x, \gamma x) \leq a\} \underset{a\to\infty}{=} O(a^{\frac{r-1}{2}} e^{\delta_G a}).$$

Démonstration. Comme Γ est discret dans G et que G agit proprement sur G/K, il existe un réel $r > 0$ tel que, pour tout γ dans Γ tel que $\gamma x \neq x$, on ait $\gamma b(x,r) \cap b(x,r) = \emptyset$. Alors, pour tout $a > 0$, on a

$$\sharp\{\gamma \in \Gamma | d(x, \gamma x) \leq a\} \leq \sharp(\Gamma \cap K)\mathrm{vol}(b(x, a + r)).$$

Le résultat en découle.□

Nous pouvons à présent conclure la

Démonstration du théorème 1.5.1. D'après la proposition 2.0.4, l'image par κ de la mesure de comptage de Γ est à croissance concave et, d'après les lemmes 3.3.1 et 3.3.2, elle est de type strictement divergent, à exposant fini. Le résultat découle alors de la proposition 3.2.1. □

Bibliographie

[1] H. Abels, G. Margulis, G.A. Soifer, Semigroups containing proximal linear maps, *Israel J. Math.* **91** (1995), no. 1-3, 1-30.

[2] R. Alperin, An elementary account of Selberg's lemma, *Enseign. Math.* **33** (1987), no. 3-4, 269-273.

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

[4] A. Borel, *Linear algebraic groups*, Graduate Texts in Mathematics, 126, Springer-Verlag, New York, 1991, xii+288 pp.

[5] A. Borel, Harish-Chandra, Arithmetic subgroups of algebraic groups, *Ann. of Math. (2)* **75** (1962), 485-535.

[6] A. Eskin, C. McMullen, Mixing, counting, and equidistribution in Lie groups, *Duke Math. J.* **71** (1993), no. 1, 181-209.

[7] S. Gallot, D. Hulin, Dominique, J. Lafontaine, *Riemannian geometry*, Universitext, Springer-Verlag, Berlin, 2004, xvi+322 pp.

[8] S. Helgason, *Differential geometry, Lie groups, and symmetric spaces*, Graduate Studies in Mathematics, 34, American Mathematical Society, Providence, RI, 2001, xxvi+641 pp.

[9] S. Helgason, *Groups and geometric analysis. Integral geometry, invariant differential operators, and spherical functions*, Mathematical Surveys and Monographs, 83, American Mathematical Society, Providence, RI, 2000, xxii+667 pp.

[10] D. Johnson, J.J. Millson, Deformation spaces associated to compact hyperbolic manifolds, *Discrete groups in geometry and analysis (New Haven, Conn., 1984)*, 48-106, Progr. Math., 67, Birkhäuser Boston, Boston, MA, 1987.

[11] G. Prasad, $\mathbb{R}$-regular elements in Zariski-dense subgroups, *Quart. J. Math. Oxford Ser. (2)* **45** (1994), no. 180, 541-545.

[12] J.-F. Quint, Divergence exponentielle des sous-groupes discrets en rang supérieur, *Comment. Math. Helv.* **77** (2002), no. 3, 563-608.

[13] J.-F. Quint, Groupes de Schottky et comptage, *Ann. Inst. Fourier (Grenoble)* **55** (2005), no. 2, 373-429.

[14] M.S. Raghunathan, *Discrete subgroups of Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 68. Springer-Verlag, New York-Heidelberg, 1972, ix+227 pp.

[15] J. Tits, Free subgroups in linear groups, *J. Algebra* **20** (1972), 250-270.

[16] V.S. Varadarajan, *Lie groups, Lie algebras, and their representations*, Graduate Texts in Mathematics, 102, Springer-Verlag, New York, 1984, xiii+430 pp.

[17] R.J. Zimmer, *Ergodic theory and semisimple groups*, Monographs in Mathematics, 81, Birkhäuser Verlag, Basel, 1984, x+209 pp.