Equirepartition dans les espaces homogènes

Antonin Guilloux

N° d'ordre: 8583

UNIVERSITE PARIS-SUD
FACULTE DES SCIENCES D'ORSAY

THESE

Présentée pour obtenir

LE GRADE DE DOCTEUR EN SCIENCES
DE L'UNIVERSITE PARIS XI

Spécialité : Mathématiques

par

Antonin GUILLOUX

EQUIREPARTITION DANS LES ESPACES HOMOGENES

Soutenue le 25 janvier 2007 devant la commission d'examen :

M.	Yves BENOIST	(Directeur de thèse)
M.	Nicolas BERGERON	
M.	Laurent CLOZEL	
M.	Frédéric PAULIN	
M.	Georges TOMANOV	(Rapporteur)

Rapporteur absent le jour de la soutenance :
M. François LEDRAPPIER

Remerciements

Je tiens à exprimer en premier lieu toute ma gratitude à mon directeur de thèse, Yves Benoist. Sa connaissance des mathématiques et son analyse des problèmes, qu'il m'a fait partager avec une disponibilité et une générosité constantes, ont représenté pour moi une aide inestimable. Je le remercie également pour ses encouragements tout au long de mon travail.

MM. Ledrappier et Tomanov m'ont fait l'honneur d'être rapporteurs de ma thèse. Je les remercie sincèrement des remarques, commentaires et conseils qu'ils m'ont prodigués.

Je voudrais aussi exprimer mon immense reconnaissance envers les autres membres de mon jury, qui tous ont profondément influencé mon travail : Nicolas Bergeron, qui m'a écouté, conseillé et encouragé depuis que je l'ai rencontré ; Laurent Clozel, dont les travaux ont été une grande source d'inspiration ; et Frédéric Paulin, pour son énergie et sa confiance, dont j'ai profité toutes ces années à l'ENS.

J'aimerais remercier tous ceux qui, par leur accueil, leurs discussions mathématiques et leur confiance, ont su me faire une place parmi eux. Cette attitude est sans doute le plus grand encouragement, parfois aussi le plus grand réconfort, que j'ai pu recevoir dans le cours de mon travail. Outre les personnes déjà citées, je tiens à remercier tout particulièrement Sorin, Emmanuel, Jean-François et Olivier, ainsi que tous les membres du Département de Mathématiques et Applications de l'ENS et du Laboratoire de Mathématiques d'Orsay.

Ces deux dernières institutions m'ont accueilli à divers titres au long de mon travail de thèse. Je sais gré à leurs équipes des conditions de travail exceptionnelles dont j'ai profité.

Enfin j'aimerais profiter de cette rare occasion pour remercier mes amis, ma famille, ma moitié. Ceux-là savent leurs noms sans que je les aie dits, et ce que signifie leur présence dans ma vie.

INTRODUCTION GÉNÉRALE

Ce travail de thèse porte principalement sur quelques aspects de l'équidistribution dans les espaces homogènes. Il est constitué de trois chapitres indépendants.

Les deux premiers chapitres abordent chacun une technique utilisée pour prouver des résultats d'équidistribution. Le cadre général est de considérer un groupe G contenant un réseau Γ et un sous-groupe H. On veut alors de comprendre la répartition d'une part des orbites de Γ dans $H\backslash G$ et d'autre part des orbites de H dans G/Γ. On verra que ces deux problèmes sont liés par un phénomène de dualité.

Mélange adélique et matrices rationnelles. — Dans le premier chapitre, on se place dans un cadre adélique : G est le groupe des points sur les adèles d'un groupe rationnel $\mathbf{G}$ et Γ est le réseau des points rationnels $\mathbf{G}(\mathbb{Q})$. On s'intéresse à des applications d'un théorème de décroissance des coefficients de la représentation unitaire de G dans l'espace de Hilbert $L^2(G/\Gamma)$. Le théorème que nous utilisons provient d'un article de A. Gorodnik, F. Maucourant et H. Oh ([20]) et généralise un théorème de L. Clozel, H. Oh et E. Ullmo ([13]).

A. Eskin et C. McMullen ont montré dans un cadre réel (Cf [18]) que cette décroissance des coefficients - qui traduit la propriété de mélange de l'action de G sur G/Γ - implique des résultats d'équidistribution des orbites de Γ dans des espaces homogènes. L. Clozel, H. Oh et E. Ullmo ont utilisé cette stratégie pour obtenir l'équidistribution des points de Hecke ([13]) ; et A. Gorodnik, F. Maucourant et H. Oh celle des points de hauteur bornée ([20]).

Nous utilisons ces outils pour étudier la répartition des matrices rationnelles de dénominateur n dans les groupes unitaires ou orthogonaux.

Énonçons plus précisément ces résultats : on appelle dénominateur d'une matrice rationnelle le plus petit commun multiple des dénominateurs de ses coefficients. Pour chaque nombre premier p et entier $k \geq 1$ on note $|.|_p$ la norme du max de la norme des coefficients sur $\mathcal{M}(k, \mathbb{Q}_p)$.

Fixons une forme hermitienne définie positive h sur $\mathbb{Q}[i]^k$. On peut remarquer que s'il existe une matrice rationnelle de dénominateur n dans $SU(h, \mathbb{Q})$, alors à chaque place finie p, il existe une matrice g_p de $SU(h, \mathbb{Q}_p)$ telle que $|g_p|_p = |\frac{1}{n}|_p$.

Alors on montre que la réciproque est vraie pour n suffisament grand et que l'ensemble des matrices de dénominateur n - s'il est non vide - s'équirépartit asymptotiquement. Pour énoncer le théorème, on note $\mathcal{U}_l(h)$ l'ensemble des entiers n tels que pour tout nombre premier p, il existe une matrice de norme $|\frac{1}{n}|_p$ dans $SU(h,\mathbb{Q}_p)$. Alors on a :

Théorème **(1.4** p. 2). — *Soient $k \geq 2$, h une forme hermitienne rationelle définie positive. Notons μ la probabilité de Haar sur $SU(h,\mathbb{R})$. Pour tout entier n, soit Γ_n l'ensemble des matrices rationnelles de $SU(h,\mathbb{R})$ de dénominateur n.*

Alors quand n tend vers l'infini dans $\mathcal{U}_l(h)$, les Γ_n s'équirépartissent dans $SU(h,\mathbb{R})$, c'est à dire :

$$\frac{1}{Card(\Gamma_n)}\sum_{\gamma\in\Gamma_n}\delta_\gamma \xrightarrow[n\in\mathcal{U}_l(h)]{n\to\infty} \mu$$

Nous nous intéressons ensuite au cas des groupes orthogonaux. Ce cas est plus difficile que le précédent ; nous obtenons le résultat suivant :

Théorème **(1.13** p. 12). — *Soient $k \geq 5$, q une $\mathbb{Q}$-forme quadratique définie positive sur $\mathbb{Q}^k$ et μ la probabilité de Haar sur $SO(q,\mathbb{R})$. Pour tout entier n, soit Γ_n l'ensemble des matrices de $SO(q,\mathbb{Q})$ de dénominateur n.*

Alors il existe un entier N tel que quand n tend vers l'infini et que n est premier à N, les Γ_n s'équirépartissent dans $SO(q,\mathbb{R})$, c'est à dire :

$$\frac{1}{Card(\Gamma_n)}\sum_{\gamma\in\Gamma_n}\delta_\gamma \xrightarrow[n \text{ premier à } N]{n\to\infty} \mu$$

Remarquons pour conclure que ces résultats d'équirépartition impliquent comme corollaire l'existence de matrices de dénominateur n quand n est suffisamment grand et vérifie les conditions données.

Ces deux théorèmes seront obtenus comme cas particulier d'un résultat général, le théorème 1.9 p. 6.

Dynamique polynomiale et réseaux. — Dans le second chapitre, nous nous intéressons à des applications de l'étude des orbites polynomiales dans un espace homogène G/Γ. L'intérêt de comprendre ces orbites a notamment été noté par M.S. Raghunathan, ce qui a mené à la preuve par G. Margulis de la conjecture d'Oppenheim ([26]). Cette preuve exploite le comportement des orbites de groupes unipotents dans $SL(3,\mathbb{R})/SL(3,\mathbb{Z})$.

L'étude des orbites unipotentes dans un espace homogène G/Γ (où G est un groupe de Lie réel ou p-adique, et Γ un réseau de G) a été ensuite généralisée, jusqu'à aboutir au théorème de rigidité de M. Ratner : on peut utiliser certaines propriétés des dynamiques polynomiales pour montrer que toute mesure sur G/Γ invariante et ergodique sous l'action d'un groupe unipotent est algébrique, c'est à dire qu'elle est portée par une orbite d'un sous-groupe P de G que Γ rencontre en un réseau, et qu'elle est P-invariante.

Ce théorème a bien évidemment de nombreuses applications pour prouver des résultats d'équirépartition dans G/Γ, mais aussi pour prouver l'équirépartition d'orbites de Γ dans des espaces homogènes sous G. Nous utiliserons le théorème tel qu'on le trouve dans l'article [27] de G. Margulis et G. Tomanov.

À l'aide de ce théorème, F. Ledrappier et M. Pollicott (cf [25]) ont étudié la répartition des orbites d'un réseau de $SL(2,\mathbb{Q}_p)$ dans $\mathbb{Q}_p^2 \setminus \{0\}$. Nous reprenons cette étude en toute dimension supérieure à 2, et nous obtenons alors le résultat suivant :

***Théorème* (2.4 p. 23).** — *Soient $d \geq 2$ un entier, p un nombre premier. On note G le groupe $SL(d,\mathbb{Q}_p)$ et Γ un réseau dans G. On fixe une norme ultramétrique $\|.\|$ sur $\mathcal{M}(d,\mathbb{Q}_p)$, et on note $\Gamma_n = \{\gamma \in \Gamma$ tels que $\|g\| \leq p^n\}$.*

Considérons H le sous-groupe unipotent triangulaire inférieur de G. Soient $q = p^{\frac{d(d-1)}{2}}$ et ν une mesure G-invariante sur $X_d = H\backslash G$.

Alors il existe une constante c et une fonction $\alpha : \begin{cases} X_d^2 & \to & \mathbb{R} \\ v, w & \mapsto & \alpha_v(w) \end{cases}$ telles que pour toute fonction ϕ continue à support compact dans X_d, et pour tout $v \in X_d$, on a la limite :

$$\lim_{n\to\infty} \frac{c}{q^n} \sum_{\gamma\in\Gamma_n} \phi(v.\gamma) = \int_{X_d} \phi(w)\alpha_v(w)d\nu(w)$$

Ensuite, nous voulons obtenir un analogue d'un théorème de N. Shah ([33]), résultat qui a été utilisé notamment par A. Gorodnik et B. Weiss pour prouver un théorème sur les équidistributions d'orbites de réseaux dans les espaces homogènes. Pour cela, il nous faut d'abord reprendre un article de G. Tomanov ([36]) pour généraliser très légèrement un théorème. Ensuite nous sommes en mesure d'adapter la preuve de N. Shah pour obtenir le théorème suivant (on note $\mathcal{V}$ l' ensemble des places de $\mathbb{Q}$, c'est à dire l'union de l'ensemble des nombres premiers et de $\{\infty\}$) :

***Théorème* (2.2 p. 21).** — *Soit $\mathbf{G}$ un groupe algébrique défini sur $\mathbb{Z}$, quasi-$\mathbb{Q}$-simple, $\mathbb{R}$-anisotrope et simplement connexe. Soit S un sous-ensemble fini de $\mathcal{V}$ contenant ∞. Soit Γ un réseau arithméthique de $G = \prod_{\nu\in S} \mathbf{G}(\mathbb{Q}_\nu)$. Notons π la projection de G sur G/Γ et m la probabilité de Haar sur G/Γ.*

Soient, pour tout $\nu \in S$, H_ν le groupe des $\mathbb{Q}_\nu$-points d'un sous-$\mathbb{Q}_\nu$-groupe quasi-simple de $\mathbf{G}(\mathbb{Q}_\nu)$. On suppose que $H = \prod_{\nu\in S} H_\nu$ est non compact et que pour tout ν tel que H_ν est non compact, $H_\nu\Gamma$ est dense dans G. Soit enfin K un sous-groupe compact ouvert de H. On dispose de la probabilité de Haar λ_K sur K.

Alors, pour toute suite (g_n) d'éléments de H tendant vers l'infini, on a la limite suivante dans l'espace des probabilités sur G/Γ :

$$\lim_{n\to\infty} \pi_*((g_n)_*\lambda_K) = m$$

Remarquons que ce résultat ne semble pas pouvoir être obtenu par des techniques de mélange analogue à celles présentées dans le premier chapitre.

Avant de présenter la troisième partie, mentionnons comme témoin des liens entre ces deux techniques et de l'intéret de chacune l'article récent de J. Ellenberg et A. Venkatesh

([17]). Ils obtiennent en effet des résultats proches de ceux présentés dans le premier chapitre en utilisant les techniques étudiées dans le second.

Sous-groupes H-valués. — Le troisième chapitre aborde un problème différent, à savoir l'existence dans le groupe spécial linéaire $SL(n, \mathbb{Q}_p)$ de sous-groupes dont toutes les matrices ont leurs valeurs propres dans un sous-groupe fixé H d'indice fini de $\mathbb{Q}_p^*$.

Dans le cas réel, ce problème a été étudié par Y. Benoist ([5]). Il arrive à la conclusion que $SL(n, \mathbb{R})$ admet un sous-groupe Zariski-dense dont tous les éléments ont leurs valeurs propres positives si et seulement si n n'est pas congru à 2 modulo 4.

Nous obtenons la même condition, sauf si le sous-groupe H contient -1 ; dans ce cas, il n'y a aucune condition :

***Théorème* (3.1 p. 51).** — *Soient n un entier supérieur à 2, k une extension finie de $\mathbb{Q}_p$, où p est un nombre premier, et H un sous-groupe d'indice fini de k^*.*

Alors, $SL(n, k)$ admet un sous-groupe $\mathbb{Q}_p$-Zariski dense, dont toutes les matrices ont toutes leurs valeurs propres dans H si et seulement si ou bien -1 est dans H, ou bien n n'est pas congru à 2 modulo 4.

TABLE DES MATIÈRES

CHAPITRE 1

EXISTENCE ET ÉQUIDISTRIBUTION DES MATRICES DE DÉNOMINATEUR n DANS LES GROUPES UNITAIRES ET ORTHOGONAUX

Introduction

La théorie des formes quadratiques définies positives à coefficients entiers répond de manière satisfaisante aux deux questions suivantes :

– À quelles conditions une forme quadratique donnée représente un entier n (c'est à dire qu'il existe un vecteur entier de norme $\sqrt{n}$) ?
– Quand un entier n est représenté, quelle est la répartition des vecteurs entiers sur l'ellipsoïde des vecteurs de norme $\sqrt{n}$?

Citons les résultats les plus simples, qui sont obtenus quand le rang de la forme quadratique est plus grand que 5 :

Théorème 1.1 **(W. Tartakowsky ([34]), C. Pommerenke ([29]))**
Soit q une forme quadratique définie positive de rang $k \geq 5$ à coefficients entiers. Alors il existe un entier N_0 tel que pour tout $n \geq N_0$, on a l'équivalence entre les deux assertions suivantes :

1. *Pour tout p premier, n appartient à $q(\mathbb{Z}_p^k)$*
2. *n appartient à $q(\mathbb{Z}^k)$*

De plus, l'ensemble des vecteurs v de $\mathbb{Z}^k$ vérifiant $q(v) = n$ s'équirépartit sur l'ellipsoïde $q(x) = n$ quand n tend vers l'infini.

Nous reviendrons dans la partie 1.4 sur ce théorème et sur le cas des formes de petit rang. Nous nous intéressons dans ce chapitre à un analogue dans le cadre des groupes unitaires ou orthogonaux de ce résultat. Présentons dans cette introduction nos résultats dans le cas unitaire (pour le cas orthogonal, on renvoie à nouveau à la partie 1.4). Soit pour $k \geq 2$, $H \in \mathcal{M}(k, \mathbb{Z}[i])$ une matrice hermitienne définie positive, h la forme hermitienne associée. Définissons le dénominateur d'une matrice à coefficients dans $\mathbb{Q}[i]$:

Définition 1.2. — Soient k un entier et A un matrice de $\mathcal{M}(k, \mathbb{Q}[i])$.

Le dénominateur d de A est défini comme le plus petit entier $d \in \mathbb{N}$ tel que dA soit une matrice de $\mathcal{M}(k, \mathbb{Z}[i])$.

Nous voulons comprendre le comportement de l'ensemble des matrices de $SU(h, \mathbb{Q})$ de dénominateur n : à quelles conditions cet ensemble est non vide, et dans ce cas, quelle est sa répartition dans le groupe $SU(h, \mathbb{R})$. On peut reformuler le problème de la façon suivante : A désigne un des anneaux $\mathbb{Z}$ ou $\mathbb{Z}_p$ pour p premier, et $A_i = \mathbb{Z}[i] \otimes_{\mathbb{Z}} A$.

On note alors, pour tout entier n, $\mathcal{T}(n, H, A)$ l'ensemble des matrices $M \in \mathcal{M}(k, A_i)$ de déterminant n^k telles que :

– les coefficients de M sont premiers entre eux,
– M est solution de l'équation (E_n) : $M^*HM = n^2H$.

Dans le cas $A = \mathbb{Z}$ et pour tout entier n, une matrice M est dans $\mathcal{T}(n, H, \mathbb{Z})$ si et seulement si la matrice $\frac{1}{n}M$ est un élément de $SU(h, \mathbb{Q})$ de dénominateur n. De même dans le cas $A = \mathbb{Z}_p$, une matrice M est dans $\mathcal{T}(n, H, \mathbb{Z}_p)$ si et seulement si la matrice $\frac{1}{n}M$ est un élément de $SU(h, \mathbb{Q}_p)$ tel que le sup de la norme p-adique des coefficients soitt la norme p-adique de $\frac{1}{n}$.

On note enfin $\mathcal{U}(H, A)$ l'ensemble des $n \in \mathbb{Z}$ tels qu'il existe $M \in \mathcal{T}(n, H, A)$, et $\mathcal{U}_l(H) = \bigcap_{p \text{ premier}} \mathcal{U}(H, \mathbb{Z}_p)$.

Bien sûr, pour qu'il existe des matrices de dénominateur n dans $SU(h, \mathbb{Q})$, il faut que n soit dans $\mathcal{U}(H, \mathbb{Z})$, et donc il faut que n soit dans $\mathcal{U}_l(H)$.

Le théorème suivant montre que pour n suffisamment grand, c'est la seule condition :

Théorème 1.3. — *Soient $k \geq 2$, $H \in \mathcal{M}(k, \mathbb{Z}[i])$ une matrice hermitienne définie positive. Alors il existe $N_0 \in \mathbb{N}$ tel que pour tout $n \geq N_0$, les deux assertions suivantes sont équivalentes :*

1. *n appartient à $\mathcal{U}_l(H)$*
2. *n appartient à $\mathcal{U}(H, \mathbb{Z})$*

La méthode pour prouver ce théorème est de prouver un résultat plus fort, à savoir l'équirépartition dans $SU(q, \mathbb{R})$ de l'ensemble Γ_n des matrices de dénominateur n, quand n tend vers l'infini dans $\mathcal{U}_l(H)$. Voilà l'énoncé :

Théorème 1.4. — *Soient $k \geq 2$, $H \in \mathcal{M}(k, \mathbb{Z}[i])$ une matrice hermitienne définie positive et h la forme hermitienne associée. Notons μ la probabilité de Haar sur $SU(h, \mathbb{R})$.*

Pour tout entier n, soit Γ_n l'ensemble des $\frac{1}{n}M$ pour $M \in \mathcal{T}(n, H, \mathbb{Z})$.

Alors quand n tend vers l'infini dans $\mathcal{U}_l(H)$, les Γ_n s'équirépartissent dans $SU(h, \mathbb{R})$, c'est-à-dire :

$$\frac{1}{Card(\Gamma_n)} \sum_{\gamma \in \Gamma_n} \delta_\gamma \xrightarrow[n \in \mathcal{U}_l(H)]{n \to \infty} \mu \ .$$

Remarque 1.5. — Pour vérifier la condition $n \in \mathcal{U}_l(H)$, il suffit de vérifier que l'ensemble $\mathcal{T}(n, H, \mathbb{Z}_p)$ est non vide uniquement pour les nombres premiers p divisant n. En effet, si p ne divise pas n, la matrice $n \cdot Id$ appartient à $\mathcal{T}(n, H, \mathbb{Z}_p)$.

La question de la répartition des points rationnels de dénominateur n dans le groupe des points réels d'un groupe algébrique $\mathbf{G}$ défini sur $\mathbb{Q}$ quand n tend vers l'infini a déjà été étudiée par plusieurs auteurs.

Dans le cas où $\mathbf{G}(\mathbb{R})$ est non-compact, A. Eskin et H. Oh (Cf [19]) ont montré que ces points étaient équidistribués suivant la mesure de Haar de $\mathbf{G}(\mathbb{R})$. Pour cela ils utilisent la présence de sous-groupes unipotents dans $\mathbf{G}(\mathbb{R})$ et concluent grâce à des théorèmes de Ratner et Dani-Margulis. Cependant, dans le cas où $\mathbf{G}(\mathbb{R})$ est compact, il n'y a pas d'unipotents dans $\mathbf{G}(\mathbb{R})$, donc on ne peut pas appliquer ces théorèmes.

Une autre méthode pour montrer des théorèmes d'équirépartition est d'utiliser le mélange. On renvoie à l'article d'A. Eskin et C. McMullen ([18]) pour une présentation très claire de cette méthode. Pour pouvoir l'utiliser dans notre cas, il faut disposer d'un résultat de décroissance des coefficients de l'action de $\mathbf{G}$ sur $L^2(\mathbf{G}(\mathbb{A})/\mathbf{G}(\mathbb{Q}))$ (on rappelle que, dans ce cadre $\mathbf{G}(\mathbb{Q})$ est un réseau du groupe des points sur les adèles $\mathbf{G}(\mathbb{A})$). De tels résultats sont prouvés dans l'article de L. Clozel, H. Oh et E. Ullmo ([13]), et complétés dans un article de L. Clozel ([12]), puis de A. Gorodnik, F. Maucourant et H. Oh ([20]) où une décroissance des coefficients de l'action de $\mathbf{G}$ sur $L^2(\mathbf{G}(\mathbb{A})/\mathbf{G}(\mathbb{Q}))$ est montrée sous les hypothèses que $\mathbf{G}$ est un groupe algébrique défini sur un corps de nombres, connexe et absolument quasi-simple (on renvoie au théorème 1.7 pour l'énoncé exact).

C'est ce dernier résultat que nous utiliserons. Commençons par rappeler quelques résultats sur les groupes algébriques et leurs réseaux arithmétiques, ce qui permettra de fixer le cadre de la preuve.

Groupes algébriques et réseaux arithmétiques. — Nous définissons dans cette partie les notations dont nous nous servirons dans ce chapitre. Il nous faudra pour cela faire appel à des résultats sur les groupes algébriques et adéliques. Pour leur preuve, nous renvoyons le lecteur d'une part à l'article [35] de J. Tits (et ses références) pour les résultats spécifiques aux points sur $\mathbb{Q}_p$ d'un groupe algébrique, et d'autre part au livre de V. Platonov et A. Rapinchuk (Cf [28]) pour les propriétés adéliques.

Fixons une fois pour toutes un groupe $\mathbf{G}$ défini sur un corps de nombres K, connexe, quasi-K-simple. Soit $\mathcal{V}$ l'ensemble des places de K. On note $\mathbb{A}$ (resp. $\mathbb{A}^f$, resp. $\mathbb{A}^\infty$) l'anneau des adèles de K (resp. des adèles finies, resp. infinies). On note de plus $G = \mathbf{G}(\mathbb{A})$, et $G^f = \mathbf{G}(\mathbb{A}^f)$, et $G^\infty = \mathbf{G}(\mathbb{A}^\infty)$. On supposera toujours que G^∞ est compact.

Nous disposons alors du sous-groupe $\mathbf{G}(K)$. On rappelle, d'après [28], que c'est un réseau de G, qu'il est irréductible car $\mathbf{G}$ est quasi-K-simple ; et enfin qu'il est cocompact car $\mathbf{G}$ est K-anisotrope.

On appelle réseau arithmétique de G tout sous-groupe Γ tel que $\Gamma \cap \mathbf{G}(K)$ est d'indice fini dans Γ et dans $\mathbf{G}(K)$. D'après ce qui précède, tout réseau arithmétique Γ de G est irréductible et cocompact. On se fixe un tel réseau Γ, ainsi qu'un sous-groupe compact ouvert U de G^f.

On dira qu'une suite d'éléments (g_n) de G tend vers l'infini si pour tout compact C de G, pour n suffisament grand, g_n n'appartient pas à C.

Fixons les dernières notations : on note τ^∞ la projection de G sur G^∞, τ^f la projection de G sur G^f, et enfin π la projection de G sur G/Γ. De plus on note λ la mesure de Haar sur G^f normalisée par $\lambda(U) = 1$; μ la probabilité de Haar sur G^∞. On note enfin m la probabilité sur G/Γ localement proportionnelle à $\mu \otimes \lambda$ et on l'appelle probabilité de Haar sur G/Γ. Le diagramme ci-dessous résume ces données :

$$\begin{array}{ccccc} & & G\ ,\ \mu\otimes\lambda & & \\ & \tau^\infty \swarrow & \tau^f \downarrow & \searrow \pi & \\ G^\infty = G^f\backslash G\ ,\ \mu & & G^f\ ,\ \lambda & & G/\Gamma\ ,\ m \end{array}$$

Enfin, pour les applications, on supposera toujours fixée une base sur $\mathbb{Z}^k$ et $\mathbb{Z}[i]^k$. Ainsi, nous supposons fixée une fois pour toute l'identification entre formes quadratiques (resp. hermitienne) et matrices symétriques (resp. hermitiennes).

Application de la décroissance des coefficients. — On remarque qu'une matrice est de dénominateur n si et seulement si pour tout nombre premier p, le max de la norme p-adique de ses coefficients est la norme p-adique de $\frac{1}{n}$. Donc on peut réénoncer notre problème comme un problème de répartition dans G^∞ de sous-ensembles de Γ définis par certaines conditions sur leur projection dans G^f. C'est dorénavant sous cet angle que nous travaillerons.

Nous montrons dans ce cadre le résultat d'équirépartition suivant (rappelons que U est un sous-groupe compact ouvert fixé de G^f) : pour une suite d'ensembles $H_n \subset G^f$ bi-U-invariants, notons Γ_n l'ensemble des points de Γ dont la projection dans G^f appartient à H_n. Alors, si le cardinal des Γ_n tend vers l'infini, ils s'équirépartissent dans G^∞ vers la mesure de Haar sur G^∞.

C'est l'objet du théorème suivant :

Théorème 1.6. — *Soit $\mathbf{G}$ un K-groupe, quasi-K-simple, connexe avec $G^\infty = \mathbf{G}(\mathbb{A}^\infty)$ compact. Soient U un sous-groupe compact ouvert de $G^f = \mathbf{G}(\mathbb{A}^f)$ et (H_n) une suite de sous-ensembles compacts bi-U-invariants de G^f.*

Soit Γ un sous-groupe arithmétique de $G = \mathbf{G}(\mathbb{A})$ et $\Gamma_n = \Gamma \cap (G^\infty \times H_n)$. Notons τ^∞ la projection de G sur G^∞, et μ la probabilité de Haar sur G^∞. Pour g dans G, on note $\delta_{\tau^\infty(g)}$ la mesure de Dirac en $\tau^\infty(g) \in G^\infty$.

Supposons que $Card(\Gamma_n)$ tende vers $+\infty$. Alors on a la limite suivante, dans l'espace des probabilités sur G^∞ :

$$\lim_{n\to\infty} \frac{1}{Card(\Gamma_n)} \sum_{\gamma\in\Gamma_n} \delta_{\tau^\infty(\gamma)} = \mu \ .$$

Nous obtiendrons en outre avec le théorème 1.9 un équivalent de $Card(\Gamma_n)$. Ce théorème sera prouvé dans la partie 1.2. De plus, on notera toujours $G_n = G^\infty \times H_n$.

1.1. Représentation unitaire et décroissance des coefficients

Nous présentons dans cette partie le théorème de A. Gorodnik, F. Maucourant et H. Oh. Pour cela, il nous faut comprendre la représentation de G dans l'espace $L^2(G/\Gamma)$.

On note $<,>$ le produit scalaire canonique dans $L^2(G/\Gamma)$ et $g.f$ l'action de $g \in G$ sur une fonction f de $L^2(G/\Gamma)$. Considérons l'ensemble des sous-représentations de dimension 1 dans $L^2(G/\Gamma)$; chacune de ces représentations est associée à un caractère unitaire de G, invariant par Γ. Nous noterons $L^2_0(G/\Gamma)$ le sous-espace stable de $L^2(G/\Gamma)$ orthogonal à toutes les sous-représentations de dimension 1. Notons Λ l'ensemble des caractères unitaires de G triviaux sur Γ. Ils forment une base de l'orthogonal de $L^2_0(G/\Gamma)$.

Nous pouvons maintenant citer le théorème de A. Gorodnik, F. Maucourant et H. Oh (Cf [20], théorème 1.13) :

Théorème 1.7. — *Soit $\mathbf{G}$ un groupe défini sur un corps de nombres K, connexe et absolument quasi-simple. Alors pour toutes fonctions f et h de $L^2_0(G/\Gamma)$, on a :*

$$| < f, g.h > | \xrightarrow{g\to\infty} 0$$

Remarquons que dans [20], le produit scalaire est majoré grâce à une fonction $\bar{\xi}$ construite de manière explicite. Nous n'utiliserons pas ici cette estimée. De plus l'hypothèse d'absolue simplicité de $\mathbf{G}$ n'est pas génante, ainsi que cela avait été noté dans [20] : il existe une extension finie L de K, et $\mathbf{H}$ un L-groupe absolument quasi-simple tels que $\mathbf{G}$ est défini comme la restriction des scalaires de L à K de $\mathbf{H}$ (Cf [8], 6.21.ii). A partir de maintenant, nous supposons donc que le groupe $\mathbf{G}$ est absolument quasi-simple.

Pour appliquer ce théorème, nous devons comprendre comment s'écrit une fonction dans la décomposition de $L^2(G/\Gamma)$ en $L^2_0(G/\Gamma)$ et son orthogonal. Or les fonctions que nous étudierons seront toutes invariantes par le sous-groupe compact ouvert U.

Notons alors Λ_U l'ensemble des caractères unitaires U-invariants de Λ et $G_U = Ker(\Lambda_U)$ l'intersection de tous les $Ker(\chi)$ pour χ appartenant à Λ_U. On dispose alors du lemme suivant, tiré du lemme 3.2 de [20] :

Lemme 1.8. — 1. *l'ensemble $UG^\infty\Gamma$ est inclus dans G_U.*

2. *G_U est d'indice fini N_U dans G.*
3. *on a l'égalité $\displaystyle\sum_{\chi\in\Lambda_U}\chi = N_U 1_{G_U}$ (1_{G_U} étant la fonction caractéristique de G_U).*
4. *Si $f \in L^2(G/\Gamma)$ est définie sur $\pi(G_U)$ et est U-invariante, alors on a :*

$$f - \left(\int_{\pi(G_U)} f dm\right) 1_{\pi(G_U)} \in L_0^2(G/\Gamma)$$

Démonstration. — Le premier point est une conséquence de la continuité des caractères, et du fait que G^∞ est connexe car $\mathbf{G}$ est connexe et $\mathbb{R}$-anisotrope. On en déduit le deuxième car, d'après le théorème 5.1 de [28], l'ensemble $G^\infty U\backslash G/\Gamma$ est fini. Enfin le troisième point exprime le fait que les deux groupes abéliens finis G/G_U et Λ_U sont en dualité.

Pour le dernier point : soit $\chi \in \Lambda$. On veut calculer $< f, \chi >$. Dans un premier temps, si U n'est pas dans le noyau de χ, alors ce produit scalaire est nul. Ensuite, si $\chi \in \Lambda_U$, alors $< f, \chi >= \int_{\pi(G_U)} f dm$. □

Nous pouvons maintenant montrer le théorème 1.6.

1.2. Dualité

Nous allons en réalité montrer un théorème plus précis que le théorème 1.6. En effet, dans les hypothèses de ce théorème, on avait besoin de supposer que $Card(\Gamma_n)$ tend vers l'infini. Cette hypothèse est en pratique difficile à vérifier. Par exemple dans le cadre unitaire décrit dans l'introduction, il faudrait pour appliquer le théorème 1.6 connaître a priori un grand nombre de solutions entières de l'équation (E_n).

Dans le théorème suivant, cette hypothèse est remplacée par l'hypothèse que les compacts $G_n \cap G_U$ sont deux à deux distincts. On remarque que cette hypothèse est à priori plus simple à vérifier, car nous n'avons plus besoin de trouver des solutions entières. Nous reviendrons là-dessus pour les applications dans les parties 1.3 et 1.4.

Théorème 1.9. — *Soit $\mathbf{G}$ un K-groupe, quasi-K-simple, connexe avec $G^\infty = \mathbf{G}(\mathbb{A}^\infty)$ compact. Soient U un sous-groupe compact ouvert de $G^f = \mathbf{G}(\mathbb{A}^f)$ et (H_n) une suite de sous-ensembles compacts de G^f bi-U-invariants. On note $G_n = G^\infty \times H_n$ et on suppose que les ensembles $G_n \cap G_U$ sont deux à deux distincts.*

Soit Γ un sous-groupe arithmétique de $G = \mathbf{G}(\mathbb{A})$ et $\Gamma_n = \Gamma \cap (\mathbf{G}(\mathbb{A}^\infty) \times H_n)$. Notons τ^∞ la projection de G sur G^∞, et μ la probabilité de Haar sur G^∞, et λ la mesure de

Haar sur G^f qui donne poids 1 à U. Pour g dans G, on note $\delta_{\tau^\infty(g)}$ la mesure de Dirac en $\tau^\infty(g) \in G^\infty$.

Alors on a la limite suivante :

$$lim_{n\to\infty} \frac{\mu \otimes \lambda(G/\Gamma)}{\mu \otimes \lambda(G_n \cap G_U)} \sum_{\gamma\in\Gamma_n} \delta_{\tau^\infty(\gamma)} = \mu$$

Notamment, $Card(\Gamma_n)$ est équivalent à $\frac{\mu\otimes\lambda(G_n\cap G_U)}{\mu\otimes\lambda(G/\Gamma)}$

Démonstration. — Fixons une fonction φ continue à support compact sur G^∞, ainsi qu'une suite H_n bi-U-invariante. Nous voulons montrer la limite suivante :

$$\lim_{n\to\infty} \frac{\mu \otimes \lambda(G/\Gamma)}{\mu \otimes \lambda(G_n \cap G_U)} \sum_{\gamma\in\Gamma_n} \varphi(\tau^\infty(\gamma)) = \int_{G^\infty} \varphi d\mu$$

Pour cela, nous définissons la fonction f sur $\mathbf{G}(\mathbb{A})$ en posant $f(g_\infty, g_f) = \varphi(g_\infty)$. Nous posons ensuite $F_n(g,h) = \sum_{\gamma\in\Gamma} f(g\gamma h^{-1})1_{G_n}(g\gamma h^{-1})$ (1_{G_n} étant la fonction caractéristique de G_n).

On remarque alors que pour tout u_1, u_2 dans U et γ_1, γ_2 dans Γ, on a

$$F_n(u_1 g\gamma_1, u_2 h\gamma_2) = F_n(g,h)$$

Ainsi F_n est une fonction continue bornée définie sur $(G/\Gamma)^2$, invariante par l'action à gauche de $U \times U$. De plus, on remarque - en notant e l'élément neutre de G - que :

$$F_n(e,e) = \sum_{\gamma\in\Gamma_n} \varphi(\tau^\infty(\gamma))$$

La fonction φ est continue sur le compact G/Γ, elle est donc uniformément continue. Ainsi, soient $\varepsilon > 0$ et U_ε un voisinage de l'identité dans G^∞ tels que pour tout u et $v \in U_\varepsilon$, pour tout $g \in G^\infty$, $|\varphi(ugv) - \varphi(g)| \leq \varepsilon$. Notons β la fonction $\frac{1}{\mu(U_\varepsilon)}1_{U_\varepsilon}$ - ici 1_{U_ε} est la fonction caractéristique de U_ε dans G^∞. On pose maintenant :

$$\bar{\alpha}(g_\infty, g_f) = \beta(g_\infty)1_U(g_f)$$

$$\text{et } \alpha(g) = \mu \otimes \lambda(G/\Gamma) \sum_{\gamma\in\Gamma} \bar{\alpha}(g\gamma)$$

On voit que α est une fonction dans $L^2(G/\Gamma)$, définie sur $\pi(G_U)$, et d'intégrale par rapport à m égale à 1.

Notons que pour tout $(x,y) \in (G/\Gamma)^2$, si $\alpha(x)\alpha(y) \neq 0$, alors x et y s'écrivent $x = uu_\varepsilon\Gamma$ et $y = vv_\varepsilon\Gamma$ avec u_ε et v_ε dans U_ε, et u et v dans U. Ainsi, on a $F_n(x,y) = \sum_{\gamma\in\Gamma} \varphi(u_\varepsilon\gamma v_\varepsilon^{-1})1_{G_n}(u_\varepsilon\gamma v_\varepsilon^{-1})$. On en déduit que dans ce cas on a :

$$|F_n(x,y) - F_n(e,e)| \leq \varepsilon Card(\Gamma \cap G_n)$$

Cela se traduit par l'inégalité :

$$|F_n(e,e) - \int_{G/\Gamma}\int_{G/\Gamma} F_n(x,y)\alpha(x)\alpha(y)dm(x)dm(y)| \leq \varepsilon Card(\Gamma \cap G_n)$$

Pour fixer les notations, fixons X un relevé de G/Γ dans G. On note $\tilde{\alpha}$ le relevé de α : $\tilde{\alpha} = \alpha \circ \pi$, et on note $\tilde{m} = \frac{\mu\otimes\lambda}{\mu\otimes\lambda(X)}$. Enfin notons $I_{n,\varepsilon}$ l'intégrale :

$$I_{n,\varepsilon} = \int_{G/\Gamma}\int_{G/\Gamma} F_n(x,y)\alpha(x)\alpha(y)dm(x)dm(y)$$

On fait alors le calcul suivant :

$$\begin{aligned} I_{n,\varepsilon} &= \int_X\int_X F_n(x,y)\tilde{\alpha}(x)\tilde{\alpha}(y)d\tilde{m}(x)d\tilde{m}(y) \\ &= \int_X\int_X \sum_{\gamma\in\Gamma} f(x\gamma y^{-1})1_{G_n}(x\gamma y^{-1})\tilde{\alpha}(x)\tilde{\alpha}(y)d\tilde{m}(x)d\tilde{m}(y) \end{aligned}$$

On fait pour tout $\gamma \in \Gamma$ le changement de variable $x\gamma = g$, ce qui permet d'obtenir :

$$I_{n,\varepsilon} = \int_G\int_X f(gy^{-1})1_{G_n}(gy^{-1})\tilde{\alpha}(g)\tilde{\alpha}(y)d\tilde{m}(g)d\tilde{m}(y)$$

On fait maintenant le changement de variables $h = gy^{-1}$ pour tout $g \in G$. On obtient finalement :

$$I_{n,\varepsilon} = \int_G f(h)1_{G_n}(h)\int_X \tilde{\alpha}(hy)\tilde{\alpha}(y)d\tilde{m}(y)d\tilde{m}(h)$$

Or, d'après le théorème 1.7 et le lemme 1.8, on sait que l'intégrale $\int_{G/\Gamma}\alpha(hy)\alpha(y)dm(y)$ tend vers 1 quand h tend vers l'infini dans G_U. En outre, si h n'appartient pas à G_U, car on ne peut pas avoir à la fois y et hy qui appartiennent à G_U. Donc dans ce cas l'intégrale $\int_X \tilde{\alpha}(hy)\tilde{\alpha}(y)d\tilde{m}(y)$ est nulle .

Nous avons besoin du lemme suivant, sans doute déjà connu :

Lemme 1.10. — *Soit C_n une suite de compacts bi-U-invariants 2 à 2 distincts de G^f. Alors on a la limite :* $\lim_{n\to\infty}\lambda(C_n) = +\infty$

Démonstration. — Ce lemme est une conséquence de diverses formules de dénombrement du volume d'une double-classe pour la décomposition de Cartan dans un groupe p-adique. On peut trouver de telles formules dans [10], paragraphe 1.5, ou bien [22], 7.3. Nous en donnons une preuve dans la partie 1.5. □

On en déduit, en posant C_n la projection de $G_n \cap G_U$ sur G^f que $\lambda(C_n) = \mu\otimes\lambda(G_n\cap G_U)$ tend vers l'infini :

$$\mu\otimes\lambda(G_n \cap G_U) \xrightarrow{n\to\infty} \infty$$

Donc on peut continuer le calcul : il existe un compact C de G_U, tel que pour tout $h \in G_U - C$, on a $|\int_{G/\Gamma} \alpha(hy)\alpha(y)dm(y) - 1| \leq \varepsilon$. De plus, par définition de f, on a :

$$\int_G f(h)1_{G_n}(h)d\tilde{m}(h) = \frac{\mu \otimes \lambda(G_n \cap G_U)}{\mu \otimes \lambda(G/\Gamma)} \int_{G^\infty} \varphi d\mu$$

Et alors, pour n suffisament grand, on a :

$$\begin{aligned} |I_{n,\varepsilon} - \frac{\mu \otimes \lambda(G_n \cap G_U)}{\mu \otimes \lambda(G/\Gamma)} \int_{G^\infty} \varphi d\mu| &\leq \varepsilon \frac{\mu \otimes \lambda(G_n \cap G_U)}{\mu \otimes \lambda(G/\Gamma)} \int_{G^\infty} \varphi d\mu + \mu \otimes \lambda(C)\|\varphi\|_\infty \|\tilde{\alpha}\|_\infty^2 \\ &\leq \varepsilon \frac{2\mu \otimes \lambda(G_n \cap G_U)}{\mu \otimes \lambda(G/\Gamma)} \end{aligned}$$

On en déduit que pour n grand, on a l'inégalité

$$|F_n(e,e) - \frac{\mu \otimes \lambda(G_n \cap G_U)}{\mu \otimes \lambda(G/\Gamma)} \int_{G^\infty} \varphi d\mu| \leq \left(\frac{2\mu \otimes \lambda(G_n \cap G_U)}{\mu \otimes \lambda(G/\Gamma)} + Card(\Gamma \cap G_n) \right) \varepsilon$$

C'est à dire qu'on a pour tout $\varepsilon > 0$:

$$\begin{aligned} limsup_{n\to\infty} \frac{\mu \otimes \lambda(G/\Gamma)}{\mu \otimes \lambda(G_n \cap G_U)} (F_n(e,e) - \varepsilon Card(\Gamma \cap G_n)) &\leq \int_{G^\infty} \varphi d\mu + 2\varepsilon \\ liminf_{n\to\infty} \frac{\mu \otimes \lambda(G/\Gamma)}{\mu \otimes \lambda(G_n \cap G_U)} (F_n(e,e) + \varepsilon Card(\Gamma \cap G_n)) &\geq \int_{G^\infty} \varphi d\mu - 2\varepsilon \end{aligned}$$

On conclut en deux étapes : tout d'abord, on applique les deux inégalités précédentes à $\varphi = 1$, auquel cas $F_n(e,e) = Card(\Gamma \cap G_n)$. On en déduit (en faisant tendre ε vers 0) que :

$$\frac{\mu \otimes \lambda(G/\Gamma)}{\mu \otimes \lambda(G_n \cap G_U)} card(\Gamma \cap G_n) \xrightarrow{n\to\infty} 1$$

Enfin, on utilise ce résultat pour traiter le cas général : pour tout $\varepsilon > 0$, on a :

$$\begin{aligned} limsup_{n\to\infty} \frac{\mu \otimes \lambda(G/\Gamma)}{\mu \otimes \lambda(G_n \cap G_U)} F_n(e,e) &\leq \int_{G^\infty} \varphi d\mu + 3\varepsilon \\ liminf_{n\to\infty} \frac{\mu \otimes \lambda(G/\Gamma)}{\lambda(G_n \cap G_U)} F_n(e,e) &\geq \int_{G^\infty} \varphi d\mu - 3\varepsilon \end{aligned}$$

On peut maintenant faire tendre ε vers 0 pour obtenir la limite voulue. Ainsi, le théorème 1.9 est prouvé, et donc aussi le théorème 1.6. $\square$

1.3. Cas des groupes unitaires

Nous prouvons dans cette partie le théorème 1.4, et donc le théorème 1.3. Nous reprenons les notations donnée dans l'introduction.

Preuve du théorème 1.4. — On va appliquer le théorème 1.9 dans le cas suivant : le groupe $\mathbf{G}$ est le $\mathbb{Q}$-groupe $SU(h)$. On note qu'il vérifie bien les hypothèses du théorème et de plus qu'il est simplement connexe (Cf [28], paragraphe 2.3.3). On choisit $\Gamma = SU(h, \mathbb{Q})$, et U le produit pour p premier des compacts ouverts $SU(h, \mathbb{Z}_p)$.

Pour tout p premier et r entier, on note L_{p^r} le sous ensemble de $\mathbf{G}(\mathbb{Q}_p)$ composé des matrices telles que le sup de la valeur absolue des coefficients est p^r. Enfin pour tout n entier avec $n = \prod_{p\ premier} p^{\nu_p(n)}$, on note $H_n = \prod_{p\ premier} L_{p^{\nu_p(n)}}$.

On remarque alors que un entier n appartient à $\mathcal{U}_l(H)$ si et seulement si H_n est non vide. De plus, pour toute matrice M de $\mathcal{M}(h, \mathbb{Z}[i])$, M est dans $\mathcal{T}(n, H, \mathbb{Z})$ si et seulement si $\frac{1}{n}M$ appartient à $\mathbf{G}(\mathbb{R}) \times H_n$. C'est à dire que les ensembles Γ_n définis dans l'énoncé du théorème sont bien égaux à $\Gamma \cap G_n$.

Pour pouvoir appliquer le théorème 1.9, il ne reste plus qu'à montrer que les ensembles $G_n \cap G_U$ sont distincts. Or on remarque que, pour n dans $\mathcal{U}_l(H)$, les H_n sont disjoints donc distincts. Et il en est de même des G_n. Il suffit alors de vérifier que $G_U = G$. Il suffit donc d'appliquer le lemme suivant avec $L = G_U$:

Lemme 1.11. — *Soit* $\mathbf{G}$ *un $\mathbb{Q}$-groupe, quasi-$\mathbb{Q}$-simple et simplement connexe. Alors tout sous-groupe L fermé normal, contenant* $\mathbf{G}(\mathbb{Q})$ *et d'indice fini dans* $\mathbf{G}(\mathbb{A})$ *est égal à* $\mathbf{G}(\mathbb{A})$.

Démonstration. — En effet, si p est un nombre premier tel que $\mathbf{G}(\mathbb{Q}_p)$ est isotrope, alors $\mathbf{G}(\mathbb{Q}_p)$ est engendré par ses unipotents (voir [28], paragraphe 7.2) et notamment ne contient pas de sous-groupe d'indice fini différent de lui-même. Donc le groupe $L \cap \mathbf{G}(\mathbb{Q}_p)$ (ici, on a plongé de façon naturelle $\mathbf{G}(\mathbb{Q}_p)$ dans $\mathbf{G}(\mathbb{A})$) est égal à $\mathbf{G}(\mathbb{Q}_p)$.

Ensuite, par propriété d'approximation forte (Cf [28], théorème 7.12), $\mathbf{G}(\mathbb{Q}_p)\mathbf{G}(\mathbb{Q})$ est dense dans $\mathbf{G}(\mathbb{A})$. Donc $L = \mathbf{G}(\mathbb{A})$. □

Cela finit la preuve des théorèmes 1.4 et 1.3. □

1.4. Cas des groupes orthogonaux

Nous nous intéressons dans cette partie au cas des groupes orthogonaux. Remarquons tout d'abord que les groupes orthogonaux ne sont pas simplement connexes (Cf [28], paragraphe 2.3.2, proposition 2.14), donc le lemme 1.11 ne s'applique pas.

De fait, la question du passage du local au global pour les formes quadratiques à coefficients entiers a été beaucoup étudié, et le théorème cité au début de ce chapitre donne une réponse satisfaisante dans les cas où le rang est supérieur à 5. Esquissons, dans les grandes lignes, la stratégie pour prouver ce théorème :

On dit qu'une forme quadratique q définie positive représente (resp. représente localement) un entier naturel n si n appartient à $q(\mathbb{Z})$ (resp. à $q(\mathbb{Z}_p)$ pour tout p premier). Nous rappelons aussi la définition du genre d'une forme quadratique q : c'est l'ensemble des formes quadratiques équivalentes à q à la fois sur $\mathbb{Q}$ et sur tous les $\mathbb{Z}_p$:

Définition 1.12. — Étant données deux formes quadratiques q et q' à coefficients entiers de rang k, associées respectivement aux matrices Q et Q', on dit qu'elles sont dans le même genre si elles vérifient les propriétés suivantes :
– il existe $g \in GL(k, \mathbb{Q})$ tel que $Q' = {}^t gQg$.
– pour tout p premier, il existe un élément $g_p \in GL(k, \mathbb{Z}_p)$ tel que $Q' = {}^t g_p Q g_p$

On prouve alors que si un entier est représenté localement par une forme quadratique q, il existe une forme dans le genre de q qui le représente (Cf [11], chap. 9 théorème 1.3). Ensuite, on démontre, du moins quand le rang est supérieur à 5, que toutes les formes d'un même genre représentent les mêmes entiers suffisament grands. Cette dernière étape ne fonctionne pas en toute généralité en rang 4, et pas du tout en rang 3, où il faut introduire le concept de genre-spin. Nous ne décrirons pas plus ces théories, et renvoyons à l'article de W. Duke ([15]) pour une présentation historique de ce problème, ainsi qu'à l'article de W. Duke et R. Schulze-Pillot ([16]) pour l'analyse du cas de rang 3.

Présentons maintenant les résultats que nous obtenons : fixons une forme quadratique q rationnelle définie positive de rang $k \geq 3$, de matrice associée Q. Notons, pour tout entier n, et pour $A = \mathbb{Z}$ ou $\mathbb{Z}_p$, $\mathcal{S}(n, q, A)$ l'ensemble des matrices $M \in \mathcal{M}(k, A)$ de déterminant n^k telles que $\frac{1}{n}M$ est de dénominateur, c'est à dire :
– les coefficients de M sont premiers entre eux,
– M est solution de l'équation (F_n) : ${}^t MQM = n^2 Q$.

Notons $\mathcal{R}_l(q)$ l'ensemble des entiers n tels que pour tout p premier, $\mathcal{S}(n, q, \mathbb{Z}_p)$ est non vide. On notera de plus $\mathcal{R}_{genre}(q)$ l'ensemble des entiers n tels qu'il existe une forme q' dans le genre de q avec $\mathcal{S}(n, q', \mathbb{Z})$ non vide.

De la même manière que dans le cas unitaire, nous cherchons des matrices dans $\mathcal{S}(n, q, \mathbb{Z})$, et à comprendre l'image de cet ensemble dans $SO(q, \mathbb{R})$.

Dans le cas des formes de rang supérieur à 5, nous montrons avec le théorème 1.13 que si n est dans $\mathcal{R}_l(q)$ avec en plus la condition que n est premier à un certain entier fixé, et que n est suffisament grand, alors $\mathcal{S}(n, q, \mathbb{Z})$ est non vide, et son image dans $SO(q, \mathbb{R})$ s'équirépartit vers la mesure de Haar.

Ensuite, nous essayons de suivre une stratégie parallèle à celle évoquée plus haut. Nous montrons, cette fois sans restriction sur le rang, que, si n est dans $\mathcal{R}_{genre}(q)$ et suffisament grand, alors $\mathcal{S}(n,q,\mathbb{Z})$ est non vide, et son image s'équirépartit dans $SO(q,\mathbb{R})$. C'est l'objet du théorème 1.18.

1.4.1. Formes de rang supérieur à 5.

— Commençons par le cas du rang supérieur à 5 :

Théorème 1.13. — *Soient $k \geq 5$, q une $\mathbb{Q}$-forme quadratique définie positive sur $\mathbb{Q}^k$ et μ la probabilité de Haar sur $SO(q,\mathbb{R})$. Soit pour un entier n, Γ_n l'ensemble des matrices de $SO(q,\mathbb{Q})$ de dénominateur n.*

Alors il existe un entier N tel que quand n tend vers l'infini et que n est premier à N, les Γ_n s'équirépartissent dans $SO(q,\mathbb{R})$, c'est à dire :

$$\frac{1}{Card(\Gamma_n)} \sum_{\gamma\in\Gamma_n} \delta_\gamma \xrightarrow[n \text{ premier à } N]{n\to\infty} \mu$$

Nous allons à nouveau appliquer le théorème 1.9, cette fois dans le cadre suivant : on considère le groupe $\mathbf{G} = SO(q)$, qui vérifie bien les hypothèses du corollaire. On pose pour tout p premier, $U_p = SO(q,\mathbb{Z}_p)$, et U le produit sur p des U_p.

Soit, pour p premier et m entier, $\tilde{H}_{p^m}$ l'ensemble des matrices de $SO(q,\mathbb{Q}_p)$ telles que le max de la norme p-adique des coefficients est p^m. Maintenant, pour un entier n, pour tout p premier, on note $\nu_p(n)$ la valuation p-adique de n. On pose alors H_n le produit sur les p premiers des $\tilde{H}_{p^{\nu_p(n)}}$. Ces ensembles H_n sont bi-U-invariants et deux à deux disjoints.

On vérifie alors que, pour tout n, l'ensemble Γ_n est exactement $SO(q,\mathbb{Q}) \cap G_n$.

Il nous faut maintenant déterminer un ensemble fini F de nombres premiers tel que si n est premier aux éléments de F, alors $G_n \cap G_U$ est non vide. Il suffira alors de choisir pour N le produit des nombres premiers dans F. Pour cela, on commence par un lemme de réduction des formes quadratiques :

Lemme 1.14. — *Soient $k \geq 5$, q une $\mathbb{Q}$-forme quadratique définie positive sur $\mathbb{Q}^k$. Alors il existe un ensemble fini F de nombres premiers tels que pour tout nombre premier p en dehors de F, on a :*

q est conjuguée par une matrice de $GL(k,\mathbb{Z}_p)$ à une forme quadratique de la forme $q'(x_1,\ldots,x_k) = x_1x_2 + x_3x_4 + q''(x_5,\ldots x_k)$.

Démonstration. — q est conjuguée par $A \in GL(n,\mathbb{Q})$ à une forme quadratique diagonale $\bar{q}$. Soit F l'ensemble des nombres premiers p tels que ou $p=2$ ou bien A n'appartient pas à $GL(k,\mathbb{Z}_p)$ ou $\bar{q}$ n'est pas à coefficients dans $\mathbb{Z}_p^*$ pour la base canonique. Alors, pour tout $p \notin F$, q est conjugué sur $GL(k,\mathbb{Z}_p)$ à une forme quadratique diagonale à coefficients dans $\mathbb{Z}_p^*$.

On vérifie maintenant que pour tout p impair, toute forme quadratique r sur $\mathbb{Q}_p^5$ à coefficients dans $\mathbb{Z}_p^*$ est équivalente sur $\mathbb{Z}_p$ à une forme quadratique $y_1y_2 + +y_3y_4 + \alpha y_5^2$ pour un $\alpha \in \mathbb{Z}_p^*$ (voir [32]). □

On note pour tout $p \notin F$, φ_p l'isomorphisme entre $SO(q, \mathbb{Q}_p)$ et $SO(q', \mathbb{Q}_p)$ donné par le lemme précédent et pour tout m entier, J_{p^m} l'ensemble des matrices de $SO(q', \mathbb{Q}_p)$ telles que le max de la norme p-adique des coefficients est p^m. Comme le changement de base est à coefficients dans $\mathbb{Z}_p$, on a un corollaire du lemme précédent :

Corollaire 1.15. — *Pour tout $p \notin F$, pour tout $m \in \mathbb{N}$, on a $\varphi_p(\tilde{H}_{p^m}) = J_{p^m}$.*

Rappelons que G_U est défini comme l'intersection des noyaux de l'ensemble Λ_U des caractères U et $\mathbf{G}(\mathbb{Q})$ invariants de G.

Soit n un entier. On veut montrer que $G_n \cap G_U$ est non vide. Supposons qu'on dispose de $g \in G$ et $u \in U$ tel que gug^{-1} soit un élément de G_n. Alors, pour tout $\lambda \in \Lambda^U$, $\lambda(gug^{-1}) = 1$, et donc $gug^{-1} \in G_n \cap G_U$.

On voit donc que, pour montrer le théorème 1.13 il suffit de montrer que pour tout n dans $\mathcal{B}$, on peut trouver une paire $(g, u) \in G \times U$ tel que gug^{-1} est dans G_n.

D'après la définition de H_n, il suffit de trouver, pour tout p premier et $m = \nu_p(n)$ entier, une paire $(g, u) \in SO(q, \mathbb{Q}_p) \times U_p$ telle que gug^{-1} appartient encore à $\tilde{H}_{p^m}$. Si $m = 0$, ce qui est le cas notamment si $p \in F$, il suffit de trouver une matrice dans $SO(q, \mathbb{Z}_p)$: la matrice identité convient. Il reste à traiter le cas $\nu_p(n) \neq 0$, pour lequel on sait que $p \notin F$. Donc on peut appliquer les deux lemmes précédents et utiliser l'isomorphisme φ_p. Le théorème est alors une conséquence du lemme suivant :

Lemme 1.16. — *Soient p un nombre premier impair, $m \in \mathbb{N}$, $k \geq 5$ et q' une forme quadratique sur $\mathbb{Q}_p^k$ de la forme $q'(x_1, \ldots, x_k) = x_1x_2 + x_3x_4 + q''(x_5, \ldots x_k)$.*

Alors il existe $g \in SO(q', \mathbb{Q}_p)$, et $u \in SO(q', \mathbb{Z}_p)$ tel que gug^{-1} appartient à J_{p^m}.

Démonstration. — Il suffit de prendre les matrices :

$$g = \begin{pmatrix} p^m & 0 & 0 & 0 & 0 \\ 0 & p^{-m} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & I_{k-4} \end{pmatrix} \text{ et } u = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & I_{k-4} \end{pmatrix}$$

□

On en déduit à nouveau comme corollaire un résultat d'existence :

Corollaire 1.17. — *Soient $k \geq 5$, $Q \in \mathcal{M}(k, \mathbb{Q})$ une matrice symétrique, définie positive.*

Alors il existe deux entiers N et n_0 tels que on a pour tout $n \geq n_0$:

n premire à N implique $\mathcal{S}(n, Q, \mathbb{Z})$ non vide.

1.4.2. Lien avec le genre. — Voilà l'énoncé qui exprime que pour des formes dans le même genre, l'ensemble des dénominateurs de matrices rationnelles dans leur groupe orthogonal sont les mêmes, du moins pour des entiers suffisament grands :

Théorème 1.18. — *Soient $k \geq 3$, q et q' deux formes quadratiques définies positives du même genre.*

Alors, pour n suffisamment grand, s'il existe une matrice rationnelle de dénominateur n dans $SO(q', \mathbb{Q})$, il en existe une dans $SO(q, \mathbb{Q})$.

Démonstration. — On se place exactement dans le cadre de la preuve du théorème 1.13 : on considère à nouveau le groupe $\mathbf{G} = SO(q)$. On pose pour tout p premier, $U_p = SO(q, \mathbb{Z}_p)$, et U le produit sur p des U_p.

On définit encore, pour p premier et m entier, $\tilde{H}_{p^m}$ l'ensemble des matrices de $SO(q, \mathbb{Q}_p)$ telles que le max de la norme p-adique des coefficients est p^m. Maintenant, pour un entier n, pour tout p premier, on note $\nu_p(n)$ la valuation p-adique de n. On pose alors H_n le produit sur les p premiers des $\tilde{H}_{p^{\nu_p(n)}}$. Ces ensembles H_n sont bi-U-invariants et deux à deux disjoints.

Soit maintenant n un entier tel qu'il existe une matrice γ de dénominateur n dans $SO(q', \mathbb{Q})$. Pour prouver le théorème, selon la méthode déjà vue, il nous suffit de montrer qu'alors $G_n \cap G_U$ est non vide. On note Q et Q' les matrices associées à q et q'.

Soient $g_{\mathbb{Q}}$ la matrice rationnelle conjuguant Q à Q', et, pour tout p premier, g_p la matrice de $GL(k, \mathbb{Z}_p)$ conjuguant Q à Q'. On notera g l'élément $(g_{\mathbb{Q}}, (g_p)_{p\,premier})$ de $GL(k, \mathbb{A})$ (ici, $g_{\mathbb{Q}}$ est vu comme un élément de $GL(k, \mathbb{Q}) \subset GL(k, \mathbb{R})$). Considérons l'élément $g\gamma g^{-1}$ de $GL(k, \mathbb{A})$. Alors par définition de g, c'est un élément de $SO(q, \mathbb{A})$. On veut montrer qu'il est dans $G_n \cap G_U$.

Pour cela, commençons par remarquer que pour tout p premier, g_p est dans $GL(k, \mathbb{Z}_p)$. Donc l'élément $g\gamma g^{-1}$ est bien dans G_n (on n'a pas changé la norme p-adique de γ en le conjuguant par g_p).

Soit ensuite λ un caractère de Λ_U, c'est à dire U et Γ-invariant. On veut montrer que $\lambda(g\gamma g^{-1})$ vaut 1.

Définissons sur $SO(q', \mathbb{A})$ le caractère λ' par : pour tout $h \in SO(q', \mathbb{A})$, $\lambda'(h) = \lambda(g_{\mathbb{Q}} h g_{\mathbb{Q}}^{-1})$ (ici $g_{\mathbb{Q}}$ est vu comme l'élément rationel de $GL(k, \mathbb{A})$ dont chaque composant dans $GL(k, \mathbb{R})$ et les $GL(k, \mathbb{Q}_p)$ est la matrice $g_{\mathbb{Q}}$). Comme $g_{\mathbb{Q}}$ est une matrice rationnelle, λ' est $SO(q', \mathbb{Q})$-invariant.

Or on a $\lambda(g\gamma g^{-1}) = \lambda'(g_{\mathbb{Q}}^{-1} g\gamma g^{-1} g_{\mathbb{Q}})$. De plus, par construction, $g^{-1}g_{\mathbb{Q}}$ est un élément de $SO(q', \mathbb{A})$, et γ est un élément de $SO(q', \mathbb{Q})$..

Donc, on a montré le résultat voulu :

$$\lambda(g\gamma g^{-1}) = \lambda'(g_{\mathbb{Q}}^{-1} g\gamma g^{-1} g_{\mathbb{Q}}) = \lambda'(\gamma) = 1$$

Cela termine la preuve : il suffit d'appliquer le théorème 1.9. □

1.4.3. Application à la forme canonique. — Dans cette section, on applique nos résultats au cas de la forme quadratique canonique. On note q_k la forme quadratique canonique $x_1^2 + \ldots + x_k^2$ sur $\mathbb{Z}^k$. La stratégie est la même, mais la différence notable est qu'on sait construire en rang 3 des matrices rationnelles de tout dénominateur impair dans $SO(q_3, \mathbb{Q})$, donc nous n'avons plus de problèmes avec le groupe G_U.

Corollaire 1.19. — *Soient $k \geq 3$ et μ la probabilité de Haar sur $SO(q_k, \mathbb{R})$. Soit pour un entier n, Γ_n l'ensemble des matrices de $SO(q_k, \mathbb{Q})$ de dénominateur n.*

Alors quand n est impair tend vers l'infini, les Γ_n s'équirépartissent dans $SO(q_k, \mathbb{R})$, c'est à dire :

$$\frac{1}{Card(\Gamma_n)} \sum_{\gamma \in \Gamma_n} \delta_\gamma \xrightarrow[n \text{ impair}]{n \to \infty} \mu$$

Démonstration. — Soit n un entier impair. Commençons par construire une matrice rationnelle de dénominateur n :

Lemme 1.20. — *Pour tout entier impair n, il existe une matrice de dénominateur n dans $SO(k, \mathbb{Q})$.*

Démonstration. — Il suffit de le faire pour $SO(q_3, \mathbb{Q})$. Soit alors n un entier impair, et $x = a + ib + jc + kd$ un quaternion à coefficients entiers premiers entre eux de norme n.

Considérons la matrice de l'action de x par conjugaison sur les quaternions purs. Elle s'écrit :

$$\frac{1}{n}\begin{pmatrix} a^2+b^2-c^2-d^2 & 2(bc-ad) & 2(ac+bd) \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(cd-ab) \\ 2(bd-ac) & 2(ab+cd) & a^2-b^2-c^2+d^2 \end{pmatrix}$$

On vérifie alors qu'elle est bien de dénominateur n (il n'y a pas de simplification possible). De plus, par construction c'est une matrice de $SO(q_3, \mathbb{Q})$. □

On en déduit (avec les notations des preuves précédentes) que pour tout n impair, $G_n \cap G_U$ est non vide, car il contient une matrice rationnelle. On en déduit immédiatement le résultat du corollaire, comme application du théorème 1.9. □

1.5. Volume des doubles classes dans la décomposition de Cartan

Nous voulons donner ici une preuve du lemme 1.10. Soit donc $\mathbf{G}$ un groupe algébrique défini sur $\mathbb{Q}$, U un sous-groupe compact ouvert de G^f, et λ la mesure de Haar sur G^f telle que $\lambda(U) = 1$. On veut montrer que si g tend vers l'infini dans G^f, $\lambda(UgU)$ tend aussi vers l'infini.

Remarquons dans un premier temps qu'on a $\lambda(UgU) = Card\,(UgU/U)$. De plus, on peut changer de sous-groupe compact ouvert en vertu du lemme suivant :

Lemme 1.21. — *Si $V \subset U$ est un autre sous groupe compact ouvert de G^f, il existe une constante $c > 1$ telle que pour tout g dans G, on a : $\lambda(VgV) \leq \lambda(UgU) \leq c\lambda(VgV)$*

Démonstration. — Tout d'abord, comme $V \subset U$, il est clair qu'on a $\lambda(VgV) \leq \lambda(UgU)$.

De plus, soit c l'indice $[U : V]$. Alors on fait le calcul :

$$\begin{aligned} Card\,(UgU/U) &= Card\,(U/U \cap gUg^{-1}) \\ &\leq Card\,(U/V \cap gVg^{-1}) \\ &\leq cCard\,(V/V \cap gVg^{-1}) \end{aligned}$$

Les deux inégalités sont ainsi prouvées. □

Fixons un nombre premier p et raisonnons dans le groupe $\mathbf{G}(\mathbb{Q}_p)$. Pour les résultats sur les groupes p-adiques, nous nous réferrons à l'article de J. Tits ([35]), dont nous reprenons les notations.

Résumons les objets fournis par la théorie des groupes p-adiques dont nous aurons besoin : on dispose dans $\mathbf{G}(\mathbb{Q}_p)$ d'un tore maximal $\mathbb{Q}_p$-déployé T_p, et on note N_p son normalisateur et Z_p son centralisateur (ce sont des $\mathbb{Q}_p$-sous-groupes de $\mathbf{G}$).

De plus on définit les objets suivants :

1. Les groupes $X^* = Hom_{\mathbb{Q}_p}(T_p, Mult)$ et $X_* = Hom_{\mathbb{Q}_p}(Mult, T_p)$ des caractères définis sur $\mathbb{Q}_p$ et co-caractères définis sur $\mathbb{Q}_p$ du tore, ainsi que $X^*(Z) = Hom_{\mathbb{Q}_p}(Z_p, Mult)$.
2. L'espace vectoriel $V = \mathbb{R} \otimes X_*$, et le système de racines restreintes $\Phi \subset X^*$ associé au tore T_p.
3. une application ν de $N_p(\mathbb{Q}_p)$ dans le groupe des transformations affines d'un espace A sous V, définie en 1.2 de [35] comme l'unique extension de l'application de $Z_p(\mathbb{Q}_p)$ vérifiant (en notant v_p la valuation p-adique) :
$$\forall\ z \in Z_p(\mathbb{Q}_p) \text{ et } \chi \in X^*(Z), \text{ on a } \chi(\nu(z)) = v_p(\chi(z))$$
4. ${}^vW = N_p(\mathbb{Q}_p)/Z_p(\mathbb{Q}_p)$ le groupe de Weyl fini et $\tilde{W} = N_p(\mathbb{Q}_p)/ker\nu$ qui contient le groupe de Weyl affine W comme sous-groupe distingué d'indice fini. On identifie $\tilde{W}$ comme un sous-groupe des transformations affines de V en choisissant dans A un point spécial comme origine. ${}^vW$ est alors l'ensemble des automorphismes de $\tilde{W}$ fixant l'origine.
5. un choix d'un ensemble Φ^+ de racines positives dans Φ, et donc une chambre C contenant 0 dans V définie comme l'ensemble des points v de V tels que pour tout $\chi \in \Phi^+$, on a $\chi(v) \geq 0$.

6. la chambre vectorielle $Y^+ = \mathbb{R}^+ \otimes C$ de V et un sous-groupe compact ouvert U_p de $\mathbf{G}(\mathbb{Q}_p)$ (le fixateur du point spécial) tels que $\mathbf{G}(\mathbb{Q}_p)$ est l'union des doubles classes U_paU_p pour $a \in Z_p^+ = \nu^{-1}(Y^+)$ (décompostion de Cartan)

De plus, si $n \in Z_p$ est tel que $\nu(n)$ est dans ${}^vW$, alors n appartient à U_p.

Enfin, on peut définir sur $\tilde{W}$ une fonction longueur pondérée à valeur entière (voir le paragraphe 3.3 de [35]) de la façon suivante : on note (r_i) les symétries de W associées à un système de racines simples dans Φ^+. A chacun de ces éléments est associé un entier non nul $d(r_i)$. On écrit tout élément $w \in \tilde{W}$ sous la forme $w = r_{i_1} \dots r_{i_l} w_0$ où $w_0(C) = C$ et $r_{i_1} \dots r_{i_l}$ est un mot réduit dans W. On pose alors $l(w) = d(r_{i_1}) + \ldots + d(r_{i_l})$.

Alors, d'après la section 3.3 de [35] (voir aussi [22], 7.3), pour tout $a \in Z_p^+$, en notant $\nu(a) = w$, on a :

$$Card\,(U_paU_p/U_p) = \frac{\sum_{y \in {}^vW w {}^vW} p^{l(y)}}{\sum_{y \in {}^vW} p^{l(y)}}$$

On tire le corollaire suivant de cette formule :

Corollaire 1.22. — *1. si $a \in Z_p^+$ n'est pas dans U_p, on a $Card\,(U_paU_p/U_p) \geq p$.*

2. si a_n tend vers l'infini dans Z_p^+, on a $Card\,(U_pa_nU_p/U_p) \to +\infty$.

Démonstration. — Commençons par le second point : si a_n tend vers l'infini dans $\mathbb{Z}_p^+$, alors la longueur $l(\nu(a))$ aussi, ce qui suffit.

Pour le premier point : soit a un élément de Z_p^+ qui n'est pas dans U_p. Considérons w_0 le mot le plus court dans ${}^vW\nu(a)$.

Si w_0 ne fixe pas C, alors $l(w_0) \geq 1$ et pour tout $w \in {}^vW$, on a par définition $l(ww_0) = l(w) + l(w_0)$. On en déduit que $Card\,(U_paU_p/U_p)$ est plus grand que $p^{l(w_0)}$, donc que p.

Si w_0 fixe C, alors w_0 n'est pas dans ${}^vW$ (sinon a appartient à U_p). w_0^{-1} envoie donc l'origine de V sur un autre point x. Or il existe dans ${}^vW$ une symétrie s qui envoie x sur un point n'appartenant pas à C. Alors, le point $w_0sw_0^{-1}$ est dans W car W est distingué dans $\tilde{W}$, mais pas dans ${}^vW$, car l'origine est envoyé sur un point en dehors de C, donc n'est pas fixée.

Donc w_0s s'écrit sous la forme rw_0, où r est dans W mais pas dans ${}^vW$. En raisonnant comme précedemment, mais pour l'ensemble ${}^vWrw_0$, on obtient aussi dans ce cas que $Card\,(U_paU_p/U_p)$ est plus grand que p. □

Maintenant que nous disposons de tous ces objets, le lemme 1.10 peut être prouvé :

Preuve du lemme 1.10. — On fixe maintenant le compact ouvert $U_0 = \prod_{p \in \mathcal{P}} U_p$. Considérons une suite (g_n) d'élément de G^f qui tend vers l'infini. Chaque g_n s'écrit comme une suite $(g_{p,n})_{p\,premier}$ dans le produit $\prod_{p\,premier} \mathbf{G}(\mathbb{Q}_p)$. On décompose toutes les coordonées dans la décomposition de Cartan :

$$g_{p,n} \in U_p a_{p,n} U_p, \text{ avec } a_{p,n} \in Z_p^+$$

Soit maintenant A un entier positif. Alors on veut montrer qu'il existe N tel que pour tout $n \geq N$, $\lambda(U_0 g_n U_0) \geq A$.

Soit $P \geq A$ un nombre premier. Pour tout élément g_n tel que il existe $q \geq P$ avec $a_{q,n} \notin U_q$, on a d'après le premier point du corollaire 1.22 :

$$\lambda(U_0 g_n U_0) = \prod_{p \; premier} Card\,(U_p a_{p,n} U_p / U_p) \geq Card\,(U_q a_{q,n} U_q / U_q) \geq q \geq A$$

Par ailleurs, considérons la sous-suite $(g_n)_{n \in S}$ telle que pour tout $n \in S$, et pour tout $p \geq P$, $a_{p,n}$ appartient à U_p.

Si cette sous-suite est finie, le résultat voulu est prouvé. Sinon, comme (g_n) sort de tout compact, il existe un nombre premier $q \leq P$ tel que la suite $(a_{q,n})_{n \in S}$ tend vers l'infini dans Z_q^+. Alors, d'après le deuxième point du corollaire 1.22, on a :

$$\lambda(U_0 g_n U_0) = \prod_{p \; premier} Card\,(U_p a_{p,n} U_p / U_p) \geq Card\,(U_q a_{q,n} U_q / U_q) \xrightarrow{n \to \infty} +\infty$$

Ainsi pour n suffisament grand, $\lambda(U_0 g_n U_0)$ est de toute façon supérieur à A.

Cela montre le résultat pour le groupe compact ouvert U_0. Or on a vu avec le lemme 1.21 que cela suffisait. Donc on a bien le résultat voulu. $\square$

CHAPITRE 2

DYNAMIQUES POLYNOMIALES ET RÉSEAUX DANS LES GROUPES p-ADIQUES

Introduction

Nous étudions dans ce texte des applications des théorèmes de Ratner sur les mesures invariantes par des groupes unipotents dans un cadre p-adique. Cette introduction décrit les résultats obtenus.

Distribution d'orbites de réseau dans le plan. — Pour introduire le sujet, nous présentons ici le cas de la dimension 2 du théorème 2.4. Ce cas est traité par F. Ledrappier et M. Pollicott (Cf [25]).

L'exemple le plus simple d'application de l'étude des dynamiques polynomiales est de considérer un groupe unipotent H dans un $SL(2)$ puis de comprendre ses orbites dans $SL(2)/\Gamma$ où Γ est un réseau. Dans le cas réel, S. Dani et J. Smillie ([14]) ont montré un résultat d'équirépartition, dont nous donnons ici un analogue (voir la proposition 2.7).

Ensuite, on peut exploiter un phénomène de dualité pour déduire du résultat d'équirépartition des horocycles - i.e. des H-orbites - dans G/Γ un résultat d'équirépartition des orbites de Γ dans $H\backslash G$. Ce phénomène est classique et semblable à la dualité du chapitre précédent. Nous reprendrons ici la présentation donnée par A. Gorodnik et B. Weiss ([21]). Cette idée a été utilisée par F. Ledrappier dans le cas réel (Cf [24]), et dans le cas p-adique par F. Ledrappier et M. Pollicott (Cf [25]), et permet d'obtenir le résultat suivant.

Soient p un nombre premier, Γ un réseau de $SL(2,\mathbb{Q}_p)$. On fixe sur $\mathcal{M}(2,\mathbb{Q}_p)$ une norme ultramétrique $\|.\|$, et on note, pour tout entier n, Γ_n l'ensemble $\gamma \in \Gamma$ tels que $\|\gamma\| \leq p^n$. On va s'intéresser à la répartition des orbites sous Γ_n de points de $\mathbb{Q}_p^2$.

Pour tout $v = (v_1, v_2)$ et $w = (w_1, w_2)$ dans $\mathbb{Q}_p^2 \setminus \{0\}$, on défini le nombre $\alpha_v(w)$ comme :

$$\alpha_v(w) = \| \begin{pmatrix} -v_2w_1 & -v_2w_2 \\ v_1w_1 & v_1w_2 \end{pmatrix} \|^{-1}$$

Enfin, on note ν la mesure de Haar sur $\mathbb{Q}_p^2$ qui donne masse $\frac{p^2-1}{p^2}$ à $\mathbb{Z}_p^2$, m la mesure de Haar sur $SL(2,\mathbb{Q}_p)$ qui donne poids 1 à $SL(2,\mathbb{Z}_p)$ et c_Γ le covolume de Γ dans G.

On a alors le théorème suivant :

Théorème 2.1. — *Dans le cadre précédent, soit $v_0 \in \mathbb{Q}_p^2 \setminus \{0\}$.*

Alors pour toute fonction φ continue à support compact dans $\mathbb{Q}_p^2 \setminus \{0\}$, on a la limite :

$$\lim_{n\to\infty} \frac{c_\Gamma}{p^n} \sum_{\gamma\in\Gamma_n} \varphi(v_0.\gamma) = \int_{\mathbb{Q}_p^2} \varphi(w)\alpha_{v_0}(w)d\nu(w)$$

Dans la partie 2.1, nous montrons ce théorème et sa généralisation en toute dimension pour des corps locaux de caractéristique nulle non archimédiens.

Dynamique des groupes unipotents sur un espace homogène dans un cadre S-arithmétique. — Dans un deuxième temps, nous restreignons notre étude à un cadre S-arithmétique : considérons la situation suivante (pour les résultats utilisés ici, nous renvoyons à [28]) : on note $\mathcal{P}$ l'ensemble des nombres premiers, et $\mathcal{V} = \mathcal{P} \cup \{\infty\}$. A tout sous-ensemble fini S de $\mathcal{V}$ contenant ∞, on associe l'anneau $k_S = \prod_{\nu\in\mathcal{V}} \mathbb{Q}_\nu$ (avec la convention $\mathbb{Q}_\infty = \mathbb{R}$) et $\mathbb{Z}_S = \mathbb{Z}\left[\frac{1}{p_1\ldots p_r}\right]$, où $p_1, \ldots, p_r$ sont les éléments de l'ensemble $S_f = S \cap \mathcal{P}$.

Soit $\mathbf{G}$ un groupe algébrique défini sur $\mathbb{Z}$ qu'on supposera toujours quasi-$\mathbb{Q}$-simple, simplement connexe, et $\mathbb{R}$-anisotrope. On note $G = \mathbf{G}(k_S)$. Le groupe $\mathbf{G}(\mathbb{Z}_S)$ est un réseau de G, il est irréductible car $\mathbf{G}$ est quasi-$\mathbb{Q}$-simple ; et enfin il est cocompact car $\mathbf{G}$ est $\mathbb{Q}$-anistrope. Ceci est donc aussi vrai pour tout réseau arithmétique de G (c'est à dire commensurable à $\mathbf{G}(\mathbb{Z}_S)$). On se fixe un tel réseau Γ.

Nous présentons dans la partie 2.2 le théorème de classification des mesures sur G/Γ invariantes par un groupe unipotent de G dans un cadre S-arithmétique. Nous avons ensuite besoin d'un analogue d'un théorème de Dani et Margulis (voir le théorème 2.19), que nous obtenons dans la partie 2.3 en suivant l'étude des dynamiques polynomiales faite par Tomanov (Cf [36]).

Nous utilisons ensuite ces outils pour prouver un analogue arithmétique d'un théorème de Shah.

Un analogue d'un théorème de Shah. — La deuxième application des théorèmes de Ratner que nous donnons est donc un analogue S-arithmétique d'un résultat de Shah (le corollaire 1.2 de [33]) :

Donnons nous $\mathbf{G}$ un groupe défini sur $\mathbb{Z}$, quasi-$\mathbb{Q}$-simple, $\mathbb{R}$-anistrope et simplement connexe, $S \subset \mathcal{V}$ un sous-ensemble fini contenant ∞, et Γ un réseau arithmétique de $G = \mathbf{G}(k_S)$.

On se donne un sous-groupe H de G, et on se demande de quelle manière se répartissent les orbites de H dans G/Γ. Remarquons que, pour espérer obtenir un résultat d'équirépartition, il faut supposer que $H\Gamma$ est dense dans G.

Le résultat suivant décrit, sous ce type d'hypothèses, un phénomène d'équirépartition :

Théorème 2.2. — *Soit* $\mathbf{G}$ *un groupe défini sur* $\mathbb{Z}$*, quasi-*$\mathbb{Q}$*-simple,* $\mathbb{R}$*-anisotrope et simplement connexe. Soit* S *un sous-ensemble fini de* $\mathcal{V}$ *contenant* ∞*. Soit* Γ *un sous-groupe arithméthique de* $G = \mathbf{G}(k_S)$*. Notons* π *la projection de* G *sur* G/Γ *et* m *la probabilité de Haar sur* G/Γ*.*

Soient, pour tout $\nu \in S$*,* H_ν *le groupe des* $\mathbb{Q}_\nu$*-points d'un sous-*$\mathbb{Q}_\nu$*-groupe quasi-simple de* $\mathbf{G}(\mathbb{Q}_\nu)$*. On suppose que* $H = \prod_{\nu \in S} H_\nu$ *est non compact et que pour tout* ν *tel que* H_ν *est non compact,* $H_\nu\Gamma$ *est dense dans* G*. Soit enfin* K *un sous-groupe compact ouvert de* H*. On dispose de la probabilité de Haar* λ_K *sur* K*.*

Alors, pour toute suite (g_n) *d'éléments de* H *qui tend vers l'infini, on a la limite suivante dans l'espace des probabilités sur* G/Γ *:*

$$\lim_{n\to\infty} \pi_*((g_n)_*\lambda_K) = m$$

On rappelle que, pour toute mesure λ sur G et pour tout g dans G, $g_*\lambda$ est la mesure définie par : pour tout A mesurable, $g_*\lambda(A) = \lambda(g^{-1}A)$.

La preuve de ce théorème occupera la partie 2.4. On s'inspirera de l'article de Shah (Cf [33]).

Notations et résultats préliminaires. — Nous donnons pour finir quelques notations, résultats et conventions qui nous servirons dans toute la suite.

Tout d'abord, si $\mathbf{G}$ est simplement connexe, pour tout p premier tel que $\mathbf{G}$ est isotrope sur $\mathbb{Q}_p$, d'une part $\mathbf{G}(\mathbb{Q}_p)$ est engendré par ses unipotents et donc n'admet pas de sous-groupe normal d'indice fini autre que lui-même ; d'autre part $\mathbf{G}(\mathbb{Q}_p)\Gamma$ est dense dans G (voir [28] paragraphes 7.2 et 7.4).

Mentionnons ensuite qu'on notera toujours π la projection de G sur G/Γ. Enfin, l'ensemble G/Γ admet une unique probabilité G-invariante. C'est cette mesure qu'on appelle probabilité de Haar sur G/Γ.

Enfin, pour toute $\mathbb{Q}$-variété algébrique $\mathbf{A}$, on notera toujours, sauf mention du contraire, $A = \mathbf{A}(k_S)$ ses k_S-points.

2.1. Dynamique unipotente et réseaux du groupe spécial linéaire

Nous voulons maintenant démontrer le théorème 2.1, et sa généralisation en toute dimension.

2.1.1. Quelques résultats. — Pour toute cette partie on fixe un entier $d \geq 2$, p un nombre premier, k une extension finie de $\mathbb{Q}_p$, le groupe $G = SL(d,k)$, et Γ un réseau de G. Par définition, k est un corps local non archimédien muni d'une norme discrète notée $|.|$, et on note $\varpi > 1$ un générateur dans $\mathbb{R}^*$ de l'image de la norme $|.|$. On notera κ un élément de k de norme ϖ. Enfin, on note $\mathcal{O}$ les entiers de k. Soit K le corps résiduel de k. C'est une extension finie de $\mathbb{F}_p$, de degré $[K, \mathbb{F}_p]$.

On note $E_{i,j}$ les matrices élémentaires de $\mathcal{M}(d,k)$ et H le sous-groupe des matrices unipotentes triangulaires inférieures :

$$H = \{h((t_{i,j})_{1\leq j<i\leq d}) = Id + \sum_{1\leq j<i\leq d} t_{i,j}E_{i,j} \text{ pour } (t_{i,j}) \in k^{\frac{d(d-1)}{2}}\}$$

Notons X_d l'espace $H\backslash G$ et τ la projection de G sur $H\backslash G$. On choisit la mesure de Haar normalisée λ sur H, c'est-à-dire telle que la masse de $\{h((t_{i,j}) \text{ pour } (t_{i,j}) \in \mathcal{O}^{\frac{d(d-1)}{2}}\}$ est 1 (et on notera aussi λ la mesure de Haar normalisée sur $k^{\frac{d(d-1)}{2}}$). On fixe sur G la mesure de Haar m telle que $SL(d, \mathcal{O}) = 1$ et sur $H\backslash G$ la mesure ν telle que m est localement le produit $\lambda \otimes \nu$. On note enfin m' la probabilité de Haar sur G/Γ. Elle est localement égale à $\frac{1}{m(G/\Gamma)}m$.

On se fixe une norme ultramétrique $\|.\|$ sur $\mathcal{M}(d,k)$. On notera pour tout sous-groupe L de G, pour tout entier n et pour tous g_1, g_2 de G :

$$L_n[g_1, g_2] = \{l \in L \text{ tels que } \|g_1^{-1}lg_2\| \leq \varpi^n\}$$

$$\text{et } L_n = L_n[Id, Id]$$

On peut, grâce au lemme suivant, de définir la fonction $\alpha : \begin{cases} X_d^2 & \to & \mathbb{R} \\ v, w & \mapsto & \alpha_v(w) \end{cases}$ qui apparait dans l'énoncé du théorème 2.4 :

Lemme 2.3. — *Soit v et w dans X_d, et $q = \left(p^{[K,\mathbb{F}_p]}\right)^{\frac{d(d-1)}{2}}$. Alors, pour tout g et g' de G tels que $\tau(g) = v$ et $\tau(g') = w$, on a :*

$$\lim_{n\to\infty} \frac{\lambda(H_n[g, g'])}{q^n} = a(g, g') = \alpha_v(w)$$

Démonstration. — En effet, par définition, pour tout g_1 et g_2, on a :

$$H_n[g_1, g_2] = \{h(t_{i,j}) \text{ pour } \|(g_1^{-1}g_2) + \sum_{1\leq j<i\leq d} t_{i,j}(g_1^{-1}E_{i,j}g_2)\| \leq \varpi^n\}$$

Comme la norme est supposée ultramétrique, dès que $\varpi^n > \|g_1^{-1}g_2\|$, on a :

$$H_n[g_1, g_2] = \{h(t_{i,j}) \text{ pour } \|\sum_{1\leq j<i\leq d} t_{i,j}(g_1^{-1}E_{i,j}g_2)\| \leq \varpi^n\}$$

Or, si E est un sous-ensemble de $k^{\frac{d(d-1)}{2}}$, et t est dans k^* est de norme ϖ^n, on a $\lambda(tE) = q^n\lambda(E)$.

Donc, $\lambda(H_n[g_1,g_2])$ est égal pour n suffisamment grand à $q^n a(g_1,g_2)$, où $a(g_1,g_2)$ est la grandeur :

$$\lambda\left(\{h(t_{i,j}) \text{ pour } \| \sum_{1\leq j<i\leq d} t_{i,j}(g_1^{-1}E_{i,j}g_2)\| \leq 1\}\right)$$

Enfin, par invariance de λ, on remarque que si h_1 et h_2 sont dans H, alors on a égalité pour tout g_1 et g_2 dans G entre $\lambda(H_n[h_1g_1,h_2g_2])$ et $\lambda(H_n[g_1,g_2])$. Ainsi la fonction $a(g_1,g_2)$ est bi-invariante à gauche par H. Cela termine la preuve du lemme. □

Le théorème que l'on veut montrer est le suivant :

Théorème 2.4. — *Dans le cadre précédent, soient $v \in X_d$, $q = \left(p^{[K,\mathbb{F}_p]}\right)^{\frac{d(d-1)}{2}}$ et $c_\Gamma = m(G/\Gamma)$.*

Alors pour toute fonction φ continue à support compact dans X_d, on a la limite :

$$\lim_{n\to\infty}\frac{c_\Gamma}{q^n}\sum_{\gamma\in\Gamma_n}\varphi(v.\gamma) = \int_{X_d}\varphi(w)\alpha_v(w)d\nu(w)$$

Remarque 2.5. — Pour montrer le théorème 2.1 annoncé en dimension 2, il suffira de vérifier que les normalisation choisies sont les bonnes. Ceci sera fait dans la partie 2.1.4.

Remarque 2.6. — Dans le cas réel et en dimension 2, pour le même énoncé, il faut supposer que l'orbite $\Gamma.v_0$ est dense dans $\mathbb{R}^2 \setminus \{0\}$. Dans le cas p-adique, cette orbite est automatiquement dense.

Cela est dû au fait que un réseau dans un groupe p-adique ne contient aucun élément unipotent, contrairement au cas réel.

2.1.2. Equidistribution des horocycles. — Nous allons démontrer dans cette section l'équirépartition des orbites de H dans G/Γ. Pour cela nous allons utiliser un théorème de Ratner et Margulis-Tomanov [27] sur la rigidité des mesures invariantes par un groupe unipotent dans G/Γ.

Rappelons qu'on note π la projection de G sur G/Γ, et m' la probabilité de Haar sur G/Γ. Voilà le résultat qui nous intéresse :

Proposition 2.7. — *Avec les notations de la partie précédente, pour tous g_0, g' dans G, et pour toute fonction φ continue sur G/Γ, on a :*

$$\lim_{n\to\infty}\frac{1}{\lambda(H_n[g_0,g'])}\int_{H_n[g_0,g']}\varphi(\pi(g_0h^{-1}))\,d\lambda(h) = \int_{G/\Gamma}\varphi\,dm'$$

Démonstration. — Fixons g_0 et g' ; notons $\pi' : G \to G/\Gamma$ donnée par $\pi'(g) = \pi(g_0g)$ et $\lambda_n = \frac{1}{\lambda(H_n[g_0,g'])}(\lambda_{|(H_n[g_0,g'])^{-1}})$. Le lemme que l'on veut montrer se réénonce sous la forme suivante : $\lim_{n\to\infty}\pi'_*(\lambda_n) = m$.

Commençons par remarquer que G/Γ est compact, donc l'ensemble des $\pi'_*(\lambda_n)$ admet des valeurs d'adhérences dans l'ensemble des probabilités sur G/Γ. Soit M l'une d'entre elles. Pour simplifier les notations, on suppose que $\lim_{n\to\infty} \pi'_*(\lambda_n) = M$.

On veut montrer que M est la probabilité de Haar m' sur G/Γ.

Pour mieux comprendre la mesure M, on doit comprendre ses propriétés d'invariance par des éléments de H. On note N le groupe unipotent des matrices de la forme

$$\begin{pmatrix} 1 & & & & \\ 0 & 1 & & 0 & \\ \vdots & 0 & \ddots & & \\ 0 & & & & \\ * & & \dots & * & 1 \end{pmatrix}$$

Lemme 2.8. — *M est invariante par N et par un ouvert compact de H.*

Démonstration. — Pour prouver cette invariance, nous voulons comprendre l'action d'un élément h sur λ_n. Elle s'écrit :

$$h_*\lambda_n = \frac{1}{\lambda(H_n[g_0, g'])}(\lambda_{|(H_n[g_0,g']h^{-1})^{-1}})$$

Commençons par montrer l'invariance par N. Pour cela fixons $l \in N$. On va en fait montrer que pour n suffisamment grand, λ_n est invariante par l, c'est à dire que l'ensemble $H_n[g_0, g']$ est invariant par multiplication à droite par l^{-1}.

Tout d'abord, par définition de N, pour tout $h \in H$ et $l \in N$, on vérifie la formule suivante :

$$hl = h + l - Id$$

Soit donc n tel que $\varpi^n > \|g_0^{-1}g'\|$. Pour tout $h \in H_n[g_0, g']$ et $l \in N \cap H_n[g_0, g']$, par ultramétricité de la norme, on a :

$$\|g_0^{-1}hlg'\| = \|g_0^{-1}hg' + g_0^{-1}lg' - g_0^{-1}g'\| \leq \varpi^n$$

Donc $H_n[g_0, g']$ est invariant par multiplication à droite par $N \cap H_n[g_0, g']$. On en déduit que pour tout n, λ_n est invariante par $N \cap (H_n[g_0, g'])^{-1}$, et donc que M est invariante par N.

Montrons le deuxième point : on construit un ouvert compact de H qui laisse tous les λ_n invariants pour n assez grand. En effet l'ensemble

$$\{\|g_0^{-1}(h - Id)g'\| \text{ pour } h \in H \text{ avec } 1 \leq \|h - Id\| \leq \varpi\}$$

est compact et évite 0, donc est minoré par un certain ϖ^c. De même l'ensemble

$$\{\|g_0^{-1}(h - Id)lg'\| \text{ pour } h \in H \text{ avec } 1 \leq \|h - Id\| \leq \varpi \text{ et } l \in \mathcal{M}(d, \mathcal{O})\}$$

est majoré par un certain ϖ^d. Soit alors $a = d - c + 1$.

Par construction, pour tout $h \in H$, et $l \in \kappa^{-a}\mathcal{M}(d,\mathcal{O})$, on a :

$$\|g_0^{-1}(h - Id)lg'\| \leq \|g_0^{-1}(h - Id)g'\|$$

Comme la norme $\|.\|$ est ultramétrique, si l appartient à $H_n[g_0, g'] \cap (Id + \kappa^{-a}\mathcal{M}(d,\mathcal{O}))$, si h est dans $H_n[g_0, g']$, et si $\varpi^n > \|g_0^{-1}g'\|$, on fait le calcul :

$$\begin{aligned}
\|g_0^{-1}hlg'\| &= \| - (g_0^{-1}g') + (g_0^{-1}lg') + (g_0^{-1}hg') + (g_0^{-1}(h - Id)(l - Id)g')\| \\
&\leq max(\|g_0^{-1}g'\|, \|g_0^{-1}hg'\|, \|g_0^{-1}lg'\|, \|g_0^{-1}(h - Id)(l - Id)g'\|) \\
&\leq \varpi^n
\end{aligned}$$

Soit alors $l \in H \cap (Id + \kappa^{-a}\mathcal{M}(d,\mathcal{O}))$. D'après le calcul précédent, pour n suffisament grand $H_n[g_0, g']$ est invariant par multiplication à droite par l^{-1}, car l^{-1} appartient aussi à $H \cap (Id + \kappa^{-a}\mathcal{M}(d,\mathcal{O}))$. Donc λ_n est invariant par l, et M aussi. □

Or le théorème 1 de [27] appliqué à notre situation s'énonce ainsi :

***Théorème 2.9* (M. Ratner, G. Margulis, G. Tomanov ([27], Théorème 1))**
Toute probabilité μ sur G/Γ H-invariante et H-ergodique est algébrique :
c'est à dire que le groupe P des éléments de G laissant μ invariante est fermé dans G, rencontre Γ en un réseau ; et il existe un point x de G/Γ tel que μ est la probabilité P-invariante portée par $P.x$.

Soit donc M_0 une composante ergodique de M. Nous voulons déterminer les groupes P qui peuvent convenir dans le théorème précédent. Admettons pour l'instant le lemme suivant, qui est le point clé de la preuve :

Lemme 2.10. — *Soit P un sous-groupe fermé de $SL(d,k)$ admettant un réseau et contenant le groupe N et un ouvert du groupe H. Alors P est tout $SL(d,k)$.*

Grâce à ce lemme, on déduit que tout composant ergodique de M est la probabilité de Haar m' sur G/Γ. Donc $M = m'$. Il ne nous reste qu'à montrer le lemme pour prouver la proposition 2.7. □

La stratégie que nous suivons pour montrer le lemme 2.10 est la suivante : nous commençons par montrer que P est Zariski-dense, donc ouvert. Nous en déduisons par un petit calcul que P contient le tore des matrices diagonales, donc tout le groupe H ainsi que tout le groupe des matrices triangulaires supérieures. On conclut que P contient l'ouvert dense des matrices admettant une décomposition dite LU, et comme P est fermé, $P = SL(d,k)$. Voilà comment mettre en oeuvre cette stratégie :

Preuve du lemme 2.10. — Rappelons le théorème suivant, tiré de la thèse de J.F. Quint ([30]) :

***Théorème 2.11* (J.F. Quint ([30], Théorème C.2.1)).** — *Soient P un $\mathbb{Q}_p$-groupe de Lie et L un sous-groupe nilpotent de P distingué fermé et engendré par ses sous-groupes compacts. Soit Λ un sous-groupe discret de P, et π la projection canonique de P sur $L\backslash P$.*

Alors $\pi(\Lambda)$ est discret dans $L\backslash P$.

On en déduit le lemme suivant :

Lemme 2.12. — *Soit P un sous-groupe fermé de $SL(d,k)$ admettant un réseau. Alors P n'admet pas de sous-groupe unipotent L fermé distingué non compact.*

Démonstration. — Comme P est fermé, P est un $\mathbb{Q}_p$-groupe de Lie. De plus, tout sous-groupe fermé unipotent L est engendré par ses sous-groupes compacts. Donc L vérifie les hypothèses du théorème précédent.

De plus, $\Gamma \cap L$ est réduit à l'identité. En effet, si l est élément de L, alors on a la limite $l^{p^i} \xrightarrow{i\to\infty} Id$. Donc, si l appartient aussi à Γ, l est égal à Id.

Donc il existe un ouvert O de $L\backslash P$ qui ne rencontre pas $\pi(\Gamma)$, c'est à dire que OL ne rencontre pas Γ. Comme P/Γ est compact, cela implique que L est compact. □

Le lemme suivant nous permet de déterminer une partie génératrice ad hoc de $SL(d,k)$:

Lemme 2.13. — *Soit R un sous-groupe fermé de $SL(d,k)$ contenant un ouvert de H, un ouvert du groupe U des matrice triangulaire supérieure, et le groupe N. Alors R est égal à $SL(d,k)$.*

Démonstration. — On montre tout d'abord que R contient le tore des matrices diagonales. Pour cela, il suffit de montrer que R contient toutes les matrices de la forme $D_j(a) = Diag(a^{-1}, 1, \ldots, 1, a, 1 \ldots)$ (a est le j-ème coefficient diagonal) pour tout $2 \leq j \leq d$ et $a \in k^*$. Soit donc $2 \leq j \leq d$ et $a \in k^*$.

Soient $\varepsilon \in k^*$ tel que les deux matrices $U_1 = Id + \varepsilon E_{j,n}$ et $U_2 = Id - \frac{\varepsilon}{a} E_{j,n}$ soient dans R et $x = \frac{a-1}{\varepsilon}$. Alors les deux matrices $N_1 = Id + xE_{n,j}$ et $N_2 = Id - \frac{x}{a} E_{n,j}$ sont dans N, et la formule suivante montre que $D_j(a)$ est dans R :

$$D_j(a) = U_2 N_1 U_1 N_2$$

On en déduit alors que R contient tout H et tout le groupe U des matrices unipotentes triangulaires supérieures. En effet, en notant a la partie entière de $\frac{d}{2}$, si D est la matrice $Diag(p^{-a}, p^{-a+1}, \ldots, p^a)$, alors pour toutes matrices h de H et u de U, on a les limites :

$$D^n h D^{-n} \xrightarrow{n\to\infty} Id \text{ dans H}$$
$$D^{-n} u D^n \xrightarrow{n\to\infty} Id \text{ dans U}$$

Or R contient un ouvert de H et de U et contient d ; donc h et u sont dans R.

Pour conclure : R contient le groupe L des matrices triangulaires inférieures et le groupe U des matrices unipotentes triangulaires supérieures. Donc R contient l'ouvert dense des matrices admettant une décomposition LU (il s'agit des matrices dont tous les mineurs principaux sont non nuls (cf [31], thm 8.1.1)). Comme R est fermé, R est le groupe $SL(d,k)$ tout entier. $\square$

On fixe maintenant un sous-groupe P de $SL(d,k)$ admettant un réseau et contenant le groupe N et un ouvert du groupe H. Rappelons qu'on veut prouver le lemme 2.10, c'est à dire que P est $SL(d,k)$ tout entier. Soit Q la clôture de Zariski de P. On déduit des deux lemmes précédents le résultat suivant :

Lemme 2.14. — *Q est le groupe $SL(d,k)$.*

Démonstration. — Commençons par montrer que Q n'est contenu dans aucun groupe parabolique. En effet, si Q est contenu dans un groupe parabolique Q', alors Q' contient H. Donc le radical unipotent R_u de Q' est inclus dans H.

Alors le groupe $R_u \cap P$ est un sous-groupe unipotent fermé de P distingué dans P. D'après le fait précédent il doit être compact. Or il contient le groupe $R_u \cap N$ qui n'est compact que si $R_u = \{Id\}$.

Donc Q est réductif : son radical unipotent est réduit à l'identité. Ainsi il contient le groupe unipotent opposé à H, qui est un conjugué de H ne rencontrant pas H. Donc Q contient le groupe unipotent des matrices triangulaires supérieures. Le lemme 2.13 implique alors que Q est $SL(d,k)$ tout entier. $\square$

On en déduit que l'algèbre de Lie de P est un idéal de $\mathfrak{sl}_{\mathbb{Q}_p}(d,k)$ car elle est normalisée par P donc par sa clôture algébrique (voir aussi le lemme 2.8 du troisième chapitre). Elle est de plus non-vide car elle contient l'algèbre de Lie de N. Donc l'algèbre de Lie de P est $\mathfrak{sl}_{\mathbb{Q}_p}(d,k)$, c'est à dire que P est ouvert.

Comme P est ouvert, il contient un ouvert de H, un ouvert de U. De plus il contient N et il est fermé. Le lemme 2.13 permet alors de conclure que P est égal à tout $SL(d,k)$ $\square$

2.1.3. Dualité. — L'équidistribution que nous venons de montrer implique le théorème 2.4 par un phénomène classique de dualité. La stratégie que nous employons est une adaptation à notre cas de celle de Gorodnik et Weiss (cf [21]).

Preuve du théorème 2.4. — Soit φ une fonction continue à support compact sur X_d. Nous voulons démontrer l'égalité suivante :

$$\lim_{n\to\infty} \frac{m(G/\Gamma)}{q^n} \sum_{\gamma\in\Gamma_n} \varphi(v_0.\gamma) = \int_{X_d} \varphi(w)\alpha_{v_0}(w)d\nu(w)$$

Pour simplifier les notations, on remarque que quitte à conjuguer H, Γ et la norme par g_0, on peut supposer que $g_0 = Id$.

Pour prouver cette égalité, nous allons utiliser la proposition 2.7 ; construisons, à partir de φ, une fonction sur G.

Tout d'abord, soit P^+ le sous-groupe des matrices triangulaires supérieures. Alors l'application produit de $P^+ \times H$ dans G est un homéomorphisme local sur un ouvert de G. Donc on dispose d'une section locale au voisinage de v_0 de la projection τ de G dans X_d. En translatant, on dispose de telles sections locales au voisinage de tout point de X_d. Quitte à réduire le support de φ, on peut supposer qu'il est dans le support d'une telle section qu'on note σ.

Nous avons besoin d'une propriété d'invariance de la norme, et pour cela nous raisonnons comme dans la partie précédente. Pour tout b dans G, l'ensemble

$$\{\|(h - Id)b\| \text{ pour } h \in H \text{ avec } 1 \leq \|h - Id\| \leq \varpi\}$$

est compact et évite 0, donc est minoré par un certain ϖ^c. De même l'ensemble

$$\{\|(h - Id)lb\| \text{ pour } h \in H \text{ avec } 1 \leq \|h - Id\| \leq \varpi \text{ et } l \in \mathcal{M}(d, \mathcal{O})\}$$

est majoré par un certain ϖ^d.

Soit alors K_b le sous-groupe compact ouvert :

$$SL(d, \mathcal{O}) \cap \left(Id + \kappa^{d-c+1}\mathcal{M}(d, \mathcal{O})\right)$$

Alors, pour tout $l \in K_b$, et $h \in H$, on a l'égalité $\|(h - Id)b\| = \|(h - Id)lb\|$.

Quitte à réduire encore le support de φ, on peut supposer qu'il existe $b \in G$ tel que le relevé par σ du support de φ est inclus dans $K_b b$. Dorénavant b est fixé, et on notera $K = K_b$, et A un majorant de $\{\|kb\| \text{ pour } k \in K\}$. Par construction de K, on a la propriété suivante :

$$\text{pour tout } l \in Kb, \text{ et pour tout } n \text{ avec } \varpi^n > A, \text{ on a } H_n[Id, l] = H_n[Id, b] \qquad (1)$$

Pour g tel que $v_0.g$ est dans le support de φ, on définit $\bar{g}$ comme $\sigma(v_0.g) \in Kb$. On pose alors $u_g = \bar{g}g^{-1} \in H$.

Soit enfin ψ une fonction définie sur H, à support dans le compact $H \cap K$, positive d'intégrale 1.

On définit la fonction $f : G \to \mathbb{R}$ par $f(g) = \psi(u_g)\varphi(v_0.g)$. Le résultat suivant relie les valeurs de φ aux intégrales de f sur H_n.

Lemme 2.15. — *Pour tout n tel que $\varpi^n > A$, pour $g \in G$ on a l'alternative suivante :*
- *Si $g \in G_n$, on a $\varphi(v_0.g) = \displaystyle\int_{H_n[Id,b]} f(h^{-1}g)d\lambda(h)$.*
- *Si au contraire g n'est pas dans G_n, alors $\int_{H_n[Id,b]} f(h^{-1}g)d\lambda(h) = 0$*

Démonstration. — Par définition, on a l'équivalence suivante : g appartient à G_n si et seulement si $\|u_g^{-1}\bar{g}\| \leq \varpi^n$. Or si u est dans le support de ψ, u est dans K, et on a aussi par construction $\|u_g^{-1}u\bar{g}\| \leq \varpi^n$. À l'inverse, si g n'est pas dans G_n, on a $\|u_g^{-1}u\bar{g}\| > \varpi^n$.

C'est à dire qu'on a l'alternative suivante :

$$g \in G_n \quad \Rightarrow \quad \text{le support de } \psi \text{ est inclus dans } u_g H_n[Id, \bar{g}] \tag{2}$$

$$g \notin G_n \quad \Rightarrow \quad \text{le support de } \psi \text{ est disjoint de } u_g H_n[Id, \bar{g}] \tag{3}$$

Or, l'égalité suivante est vérifiée : $u_g u = u_{u^{-1}g}$. Dès que $\varpi^n > A$, cela permet, avec l'égalité (1), de faire le calcul :

$$\begin{aligned}
\int_{H_n[Id,b]} f(h^{-1}g)d\lambda(h) &= \int_{H_n[Id,\bar{g}]} \varphi(v_0.(h^{-1}g))\psi(u_g h)d\lambda(h) \\
&= \varphi(v_0.g)\int_{u_g H_n[Id,\bar{g}]} \psi(h)d\lambda(h)
\end{aligned}$$

Cela montre l'alternative recherchée, grâce aux deux implications (2) et (3). $\square$

On en déduit immédiatement la formule suivante, pour $\varpi^n > A$:

$$\sum_{\gamma\in\Gamma_n} \varphi(v_0.\gamma) = \sum_{\gamma\in\Gamma} \int_{H_n[Id,b]} f(h^{-1}\gamma)d\lambda(h)$$

Rappelons que la proposition 2.7 énonce un résultat d'équirépartition dans G/Γ. Il nous faut donc pour l'appliquer disposer d'une fonction définie sur G/Γ. Définissons, pour g dans G :

$$F(g) = \sum_{\gamma\in\Gamma} f(g\gamma)$$

Cette fonction est bien définie, car f est à support compact et Γ est un réseau de G, donc notamment un ensemble discret. On voit que F est Γ-invariante à droite et donc que F est bien définie sur G/Γ. Enfin on a, dès que $\varpi^n > A$:

$$\sum_{\gamma\in\Gamma_n} \varphi(v_0.\gamma) = \int_{H_n[Id,b]} F(h^{-1})d\lambda(h)$$

Rappelons que nous cherchons un équivalent de $\sum_{\gamma\in\Gamma_n} \varphi(v_0.\gamma)$. On procéde en deux étapes.

Première étape : $m(G/\Gamma)\sum_{\gamma\in\Gamma_n} \varphi(v_0.\gamma)$ est équivalent quand n tend vers $+\infty$ à $\int_{G_n} \varphi(v_0.g)dm(g)$

Fixons $\varepsilon > 0$. D'après la formule précédente et la proposition 2.7, pour n suffisamment grand on a :

$$|\sum_{\gamma\in\Gamma_n} \varphi(v_0.\gamma) - \lambda(H_n[Id,b])\int_{G/\Gamma} F dm'| < \varepsilon\lambda(H_n[Id,b])$$

Or, on peut écrire $m(G/\Gamma)\lambda(H_n[Id,b])\int_{G/\Gamma} Fdm'$ sous la forme :

$$\begin{aligned}
m(G/\Gamma)\lambda(H_n[Id,b])\int_{G/\Gamma} Fdm' &= \lambda(H_n[Id,b])\int_G fdm \\
&= \int_{H_n[Id,b]}\left(\int_G f(h^{-1}g)dm\right)d\lambda \\
&= \int_G\int_{H_n[Id,b]} f(h^{-1}g)d\lambda dm \\
&= \int_{G_n}\varphi(v_0.g)dm(g)
\end{aligned}$$

La dernière égalité découle du lemme 2.15. Cela montre l'équivalence annoncée.

Deuxième étape : $\frac{1}{q^n}\int_{G_n}\varphi(v_0.g)dm(g)$ est égal, pour n grand, à $\int_V \varphi(w)\alpha_{v_0}(w)d\nu(w)$.

Remarquons tout d'abord que pour tout $w \in \tau(Kb)$, avec $w = v_0.g$, pour tout $h \in H$, on a $v_0.(h\sigma(w)) = v_0.g$. De plus tout élément g' de G_n tel que $v_0.g' = w$ est de la forme $h\sigma(w)$ pour un certain $h \in H_n[Id,\sigma(w)]$.

Donc on peut faire le calcul :

$$\begin{aligned}
\int_{G_n}\varphi(v_0.g)dm(g) &= \int_V\int_{H_n[Id,\sigma(w)]}\varphi(w)d\nu(w)d\lambda(h) \\
&= q^n\int_V \varphi(w)\frac{\lambda(H_n[Id,\sigma(w)])}{q^n}d\nu(w)
\end{aligned}$$

Pour conclure, on remarque que le support de φ est supposé inclus dans $\tau(Kb)$. Donc d'après l'égalité 1, on a pour $\varpi^n > A$, $\lambda(H_n[Id,\sigma(w)]) = \lambda(H_n[Id,b])$.

Donc la suite de fonctions $w \to \varphi(w)\frac{\lambda(H_n[Id,\sigma(w)])}{q^n}$ est constante (pour n suffisamment grand) et égale à $w \to \varphi(w)\frac{\lambda(H_n[Id,b])}{q^n} = \varphi(w)\,a(Id,b)$ qui est intégrable. De plus, d'après le lemme 2.3, pour tout w dans le support de φ, on a l'égalité pour n grand :

$$\varphi(w)\frac{\lambda(H_n[Id,\sigma(w)])}{q^n} = \varphi(w)\,\alpha_{v_0}(w)$$

L'égalité suivante est alors vérifiée pour n suffisament grand :

$$\frac{1}{q^n}\int_{G_n}\varphi(v_0.g)dm(g) = \int_V \varphi(w)\,\alpha_{v_0}(w)d\nu(w)$$

En utilisant le résultat de la première étape, on obtient bien la limite annoncée, à savoir :

$$\lim_{n\to\infty}\frac{m(G/\Gamma)}{q^n}\sum_{\gamma\in\Gamma_n}\varphi(v_0.\gamma) = \int_V \varphi(w)\alpha_{v_0}(w)d\nu(w)$$

Ceci termine la preuve du théorème 2.4. □

2.1.4. Retour sur la dimension 2. — Vérifions pour finir que quand en dimension 2, le théorème 2.4 qu'on vient de montrer est effectivement le théorème 2.1 :

Preuve du théorème 2.1. — Il suffit de vérifier que la fonction α et la mesure ν définie pour le théorème 2.1 sont bien les mêmes que celles définies pour le théorème 2.4.

On vérifie tout d'abord que les deux définitions de la fonction $\alpha_v(w)$ coïncident à la constante.

La seule chose qu'il reste à vérifier est donc que les définitions de la mesure ν coïncident aussi. Soit donc ν' la mesure de Haar de $\mathbb{Q}_p^2$, qui donne poids $\frac{p^2-1}{p^2}$ à $\mathbb{Z}_p^2$, restreinte à $X_2 = \mathbb{Q}_p^2 \setminus \{0\}$. Soient λ la mesure normalisée de Haar sur H et m la mesure de Haar normalisée de $G = SL(2, \mathbb{Q}_p)$. On note τ la projection de G sur $H\backslash G$.

On veut alors montrer que m est localement le produit $\lambda \otimes \nu'$.

Or on dispose de la section σ continue de τ définie sur l'ouvert de mesure pleine $V = \{(v_1, v_2) \in X_k \text{ tels que } v_1 \neq 0\}$ par :

$$\sigma(v_1, v_2) = \begin{pmatrix} v_1 & v_2 \\ 0 & v_1^{-1} \end{pmatrix}$$

Dans ces conditions, pour tout $t \in \mathbb{Q}_p$ et $(v_1, v_2) \in V$, on a la formule :

$$h(t)\sigma_1(v_1, v_2) \quad = \quad \begin{pmatrix} v_1 & v_2 \\ tv_1 & tv_2 + v_1^{-1} \end{pmatrix} \tag{4}$$

On vérifie alors que pour tout $v = (v_1, v_2)$ dans V_1, pour tout $g \in G$ avec $v.g \in V$, il existe $c \in \mathbb{Q}_p$ tel que on a $h(t)\sigma(v)g = h(t + c)\sigma(v.g)$ pour tout $t \in \mathbb{Q}_p$. Or la mesure ν' est invariante par l'action de G à droite, car G agit par endomorphismes linéaires de déterminant 1.

Donc la mesure sur $H \times \sigma(V)$ donnée par $\lambda \otimes \nu'$ est une mesure invariante par G. Déterminons l'ensemble $SL(2, \mathbb{Z}_p) \cap (H \times \sigma(V))$ et calculons sa masse pour la mesure $\lambda \otimes \nu'$:

d'après la formule (4), pour tout $(v_1, v_2) \in \mathbb{Q}_p^2 \setminus \{0\}$, l'intersection $SL(2, \mathbb{Z}_p) \cap (H \times \sigma(v_1, v_2))$ est non vide si et seulement si v_1 est dans $\mathbb{Z}_p \setminus \{0\}$, v_2 dans $\mathbb{Z}_p$ et l'un des deux est inversible. On a donc l'alternative suivante :

- $(v_1, v_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p$. Alors l'ensemble des $t \in \mathbb{Q}_p$ tels que $h(t)\sigma_1(v_1, v_2)$ est dans $SL(2, \mathbb{Z}_p)$ est exactement $\mathbb{Z}_p$.
- v_1 est un entier p-adique non nul et non inversible, et v_2 est dans $\mathbb{Z}_p^*$. Dans ce cas, l'ensemble des $t \in \mathbb{Q}_p$ tels que $h(t)\sigma_1(v_1, v_2)$ est dans $SL(2, \mathbb{Z}_p)$ est exactement $-v_1^{-1}v_2^{-1} + \mathbb{Z}_p$, donc est un translaté de $\mathbb{Z}_p$.

Dans les deux cas, une fois le couple (v_1, v_2) fixé, l'ensemble des T tels que $h(t)\sigma(v_1, v_2)$ est dans $SL(2, \mathbb{Z}_p)$ est de masse 1. De plus, si A est l'ensemble des couples $(v_1, v_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p$ tels que l'un des deux est inversible, alors $\nu'(A) = 1$, vue la normalisation choisie pour ν'.

Donc la masse de $SL(2,\mathbb{Z}_p)\cap(H\times\sigma(V))$ pour la mesure $\lambda\otimes\nu'$ est 1. Comme cette intersection est un ouvert dense, et que m donne poids 1 à $SL(2,\mathbb{Z}_p)$, cela prouve que m est bien localement le produit $\lambda\otimes\nu'$. □

2.2. Mesures invariantes par des unipotents dans un cadre arithmétique

Commençons par énoncer le théorème de rigidité des mesures qui permet de donner une description précise des mesures sur G/Γ invariantes par les groupes unipotents.

Dans cette partie et la suivante, on fixe $\mathbf{G}$ un $\mathbb{Q}$-groupe $\mathbb{R}$-anisotrope, S un sous-ensemble fini de $\mathcal{V}$ contenant ∞, et on dispose de l'anneau k_S. On fixe un réseau arithmétique Γ de G.

2.2.1. Rigidité des mesures. — Nous définissons maintenant, d'après G. Tomanov (Cf [36]), une classe de sous-$\mathbb{Q}$-groupes de $\mathbf{G}$: un sous-groupe connexe $\mathbf{A}$ de $\mathbf{G}$ est de la classe $\mathcal{F}$ (ou appartient à $\mathcal{F}$) si pour tout sous-groupe algébrique normal strict $\mathbf{B}$ de $\mathbf{A}$, on peut trouver un ν dans S tel que $\mathbf{A}(\mathbb{Q}_\nu)$ contient un élément unipotent en dehors de $\mathbf{B}(\mathbb{Q}_\nu)$. On note que $\mathcal{F}$ est dénombrable car c'est un ensemble de sous-groupes $\mathbb{Q}$-algébriques.

Pour un groupe $\mathbf{P}$ de classe $\mathcal{F}$, on remarque que $P\cap\Gamma$ est un réseau arithmétique de P, car P n'admet pas de $\mathbb{Q}$-caractère non trivial (Cf [36]). Donc les orbites de P dans G/Γ sont fermées.

Cette définition est motivée par le théorème suivant, qui décrit les mesures sur G/Γ qui sont invariantes et ergodiques sous l'action d'un groupe unipotent :

***Théorème 2.16* (Tomanov ([36], Théorème 2)).** — *Soient* $\mathbf{G}$ *un groupe défini sur* $\mathbb{Q}$, Γ *un sous-groupe arithmétique de* $G=\mathbf{G}(k_S)$, U *un sous-groupe engendré par ses sous-groupes unipotents à un paramètre. Soit* l *une probabilité sur* G/Γ U*-invariante et* U*-ergodique.*

Alors il existe un sous-groupe $\mathbf{P}\subset\mathbf{G}$ *de classe* $\mathcal{F}$, *un sous-groupe* P' *de* $P=\mathbf{P}(k_S)$ *d'indice fini, et un point* $x=g_0\Gamma$ *de* G/Γ *tel que* Ug_0 *est inclus dans* g_0P', $g_0P'g_0^{-1}x$ *est un fermé de* G/Γ, *et* l *est la probabilité invariante par* $g_0P'g_0^{-1}$ *sur* $g_0P'g_0^{-1}x$.

Nous renvoyons pour la preuve à l'article de G. Tomanov ([36]).

Grâce à ce théorème, on peut donner une description des mesures sur G/Γ qui sont invariantes par un groupe unipotent, mais pas forcément ergodiques. Soit donc U un groupe engendré par ses éléments unipotents, et l une mesure sur G/Γ U-invariante.

Si $\mathbf{P}$ est de classe $\mathcal{F}$, on note $X(P,U)$ l'ensemble $\{g\in G$ tels que $Ug\subset gP\}$, et $S(P,U)$ l'union $\displaystyle\bigcup_{\mathbf{P}'\in\mathcal{F}\,,\,\mathbf{P}'\subset\mathbf{P}} X(P',U)$. On voit que $X(P,U)$ est une sous variété algébrique de G. Ces ensembles permettent de décomposer la mesure l de la façon suivante :

Pour un groupe $\mathbf{P}$ de classe $\mathcal{F}$, on note $l_{\mathbf{P}}$ la restriction de l à $\pi(X(P,U)) - \pi(S(P,U))$. Toute composante ergodique de $l_{\mathbf{P}}$ est de la forme décrite dans le théorème, pour ce groupe $\mathbf{P}$. De plus, on a $l = \sum_{\mathbf{P}\in\mathcal{F}} l_{\mathbf{P}}$ (c'est une somme dénombrable), car les ensembles $\pi(X(P,U)) - \pi(S(P,U))$ sont deux à deux disjoints.

Nous voulons donc comprendre comment des orbites de groupes unipotents se comportent au voisinage des sous-variétés de la forme $\pi(X(P,U) - S(P,U))$. Le théorème 2.19 permettra cela. Mais nous avons besoin de fixer une "bonne" représentation de G pour l'énoncer.

2.2.2. Le théorème de Chevalley. — Le théorème de Chevalley permet de définir cette représentation particulière de $\mathbf{G}$ qui nous sera utile dans toute la suite de la preuve. On fixe pour cette partie un sous-$\mathbb{Q}$-groupe $\mathbf{P}$ de $\mathbf{G}$. Considérons $\mathbf{N}(\mathbf{P})$ le normalisateur dans $\mathbf{G}$ du sous-groupe $\mathbf{P}$. C'est un sous-$\mathbb{Q}$-groupe de $\mathbf{G}$.

Pour plus de détail concernant l'énoncé suivant, nous renvoyons au livre d'A. Borel (Cf [7]), notamment les paragraphes 5 et 6.

***Théorème 2.17* (Chevalley, Cf [7], 5.1).** — *Soit* $\mathbf{H}$ *un* $\mathbb{Q}$*-groupe linéaire, et* $\mathbf{Q}$ *un sous-*$\mathbb{Q}$*-groupe.*

Alors il existe une représentation fidèle $\mathbf{H} \to \mathbf{GL}(\mathbf{V})$ *définie sur* $\mathbb{Q}$ *et une droite* $\mathbf{D}$ *de* $\mathbf{V}$ *définie sur* $\mathbb{Q}$ *telles que* $\mathbf{Q}$ *est le stabilisateur de la droite* $\mathbf{D}$.

Soit donc ρ la représentation que ce théorème permet de définir pour le sous-groupe $\mathbf{P}$ du groupe $\mathbf{G}$ avec lesquels on travaille. On se donne un $\mathbb{Q}$-point v_P dans $\mathbf{D}(\mathbb{Q})$. Quitte à le multiplier par un entier, on peut même supposer que v_P est à coordonnées entières. A partir de maintenant, nous considérerons le point v_P comme un point du k_S-module $\mathbf{V}(k_S)$. On note η la fonction de de G dans $\mathbf{V}(k_S)$ donnée par $\eta(g) = \rho(g).v_P$.

Soit $\mathbf{N_1}(\mathbf{P})$ le sous-$\mathbb{Q}$-groupe de $\mathbf{G}$ défini comme le stabilisateur de v_P. Alors, en reprenant le vocabulaire de Borel, la fonction η est une application d'orbite (pour l'action à droite de $\mathbf{N_1}(\mathbf{P})$ sur $\mathbf{G}$), au sens où c'est un morphisme surjectif entre les variétés $\mathbf{G}$ et $\rho(\mathbf{G})v_P$ qui est invariant par l'action de $\mathbf{N_1}(\mathbf{P})$ à droite sur $\mathbf{G}$.

2.2.3. Linéarisation des sous-variétés singulières. — On veut comprendre comment traduire la théorie exposée ci-dessus en termes des k_S-points de $\mathbf{G}$. On considère les groupes $N(P)$ et $N_1(P)$. On note enfin $\Gamma_P = \Gamma \cap N(P)$ et $\Gamma_N = \Gamma \cap N_1(P)$.

On a alors les résultats suivants :

Proposition 2.18. —
- *L'orbite* $\eta(\Gamma)$ *est discrète dans l'espace vectoriel* $V_G = \mathbf{V}(k_S)$.
- *L'ensemble* $N_1(P)\Gamma/\Gamma$ *est un fermé de* G/Γ.

Démonstration. — On sait d'une part que le sous-groupe $\mathbf{V}(\mathbb{Z}_S)$ est discret dans $\mathbf{V}(k_S)$ (Cf [28]) et d'autre part que ρ est définie sur $\mathbb{Q}$, donc l'ensemble $\rho(\mathbf{G}(\mathbb{Z}_S))v_P$ est discret dans $\mathbf{V}(k_S)$, et de plus, $\eta(\Gamma)$ est inclus dans une union finie de translatés de cet ensemble, par hypothèse d'arithméticité de Γ.

Pour la deuxième assertion, considérons une suite $g_k = n_k\gamma_k$ dans $N_1(P)\Gamma$ et supposons qu'elle converge vers g. On veut montrer que $g\Gamma/\Gamma$ appartient à $N_1(P)\Gamma/\Gamma$. On peut réécrire l'égalité sous la forme $\gamma_k^{-1} = g_k^{-1}n_k$, et donc, on a $\eta(g_k^{-1}) = \eta(\gamma_k^{-1})$. Donc, comme $\eta(\Gamma)$ est discret, la suite stationne, et il existe $\gamma_0 \in \Gamma$ tel que pour tout k, γ_k^{-1} appartient à $\gamma_0\Gamma_P$.

Mais alors $g_k\gamma_0$ est un élément de $N_1(P)$, donc sa limite $g\gamma_0$ aussi, et $g\Gamma$ est inclus dans $N_1(P)\Gamma$. Ainsi la deuxième assertion est démontrée. □

Enfin, considérons un sous-groupe U de G engendré par ses éléments unipotents. Alors l'ensemble $X(P,U) = \{g \in G \text{ tels que } Ug \subset gP\}$ est un fermé de Zariski de G $N_1(P)$-invariant. Donc son image par l'application quotient η -qui est Zariski-ouverte et surjective - est fermée dans $\eta(G)$. Cependant, nous aurons besoin de travailler avec la topologie de Zariski de V_G tout entier, et pas seulement de $\eta(G)$. On notera donc $F(P,U)$ la clôture de Zariski dans V_G de $\eta(X(P,U))$.

Explicitons la topologie de Zariski sur les k_S-modules : un polynôme Q sur $k_S[X_1,\ldots,X_n]$ n'est rien d'autre que la donnée de polynômes Q_ν pour tout ν dans S. Donc un fermé de Zariski d'un k_S-module $M = \prod_{\nu\in S} M_p$ est un produit de fermés de Zariski de chacun des M_p.

La représentation que nous avons défini dans cette partie permettra de traduire des phénomènes ayant lieu dans le groupe G sur le k_S-module V_G.

2.3. Dynamique polynomiale dans G/Γ

2.3.1. Orbites polynomiales proches de sous-variétés algébriques. — Nous énonçons maintenant un théorème qui permet de controller les orbites sous une action polynomiale qui sont proches d'ensembles du type $\pi(X(P,U) - S(P,U))$. Nous n'aurons besoin que de considérer des fonctions polynomiales à variables dans k_f et non k_S tout entier (rappelons qu'on note $k_f = \prod_{p\in S_f} \mathbb{Q}_p$). Commençons par définir la notion de fonction polynomiale dans un $\mathbb{Q}$-groupe $\mathbf{H}$ linéaire : une fonction $f = (f_p)_{p\in S_f}$ de $(k_f)^m$ dans H est dite polynomiale de degré d si pour tout p de S_f, f_p est une fonction de $\mathbb{Q}_p^m$ telle que les composantes matricielles de f_p dans $\mathbf{H}(\mathbb{Q}_p)$ sont polynomiales de degré d. L'ensemble de ces fonctions sera notée $\mathcal{P}_{d,m}(H)$. On note de plus θ_m la mesure de Haar sur $(k_f)^m$ telle que $\theta_m(\prod_{p\in S_f}\mathbb{Z}_p^m) = 1$.

On rappelle qu'on a défini sur $\mathbb{Q}$ une fonction η de G dans un k_S-module V_G grâce au théorème de Chevalley, et appelé $F(P,U)$ la clôture de Zariski de $\eta(X(P,U))$ dans V_G.

Théorème 2.19 **(G. Tomanov ([36] Proposition 3.4)**. — *Soient* $\mathbf{G}$ *un* $\mathbb{Q}$*-groupe* $\mathbb{R}$*-anisotrope,* Γ *un sous-groupe arithmétique de* $G = \mathbf{G}(k_S)$*,* U *un sous-groupe de* G *engendré par ses unipotents, et* $\mathbf{P}$ *un sous groupe de classe* $\mathcal{F}$*. Soient enfin* C *un compact de* $X(P,U)\Gamma/\Gamma$*,* d *et* m *deux entiers et* $\varepsilon > 0$*.*

Alors il existe un compact D *de* $F(P,U)$ *tel que pour tout voisinage relativement compact* W_0 *de* D *dans* V_G*, il existe un voisinage* W *de* C *dans* G/Γ*, tel que tout* m*, pour toute boule* B *de* $(k_f)^m$*, pour toute fonction* f *de* $\mathcal{P}_{(d,m)}(G)$ *l'alternative suivante se présente :*

– *On peut trouver un* γ *dans* Γ *tel que* $\eta(f(B)\gamma) \subset W_0$

– $\theta_m(\{t \in B$ *tels que* $(f(t)\Gamma/\Gamma) \in W\}) < \varepsilon\theta_m(B)$*.*

Pour donner une idée intuitive, on peut dire que ce théorème affirme que si les points $f(t)$ dans G passent une proportion non négligeable du temps proche de l'ensemble $X(P,U)\Gamma$, alors on va trouver un point de $\eta(\Gamma)$ qui va en être le témoin, au sens où son image par $f(B)$ va rester *tout le temps* proche de $F(P,U)$.

Notre énoncé diffère de celui de G. Tomanov car on n'envisage pas seulement l'action d'un groupe unipotent à un paramètre, mais celle d'une fonction polynomiale à plusieurs variables. La preuve que nous donnons est calquée sur la preuve de G. Tomanov.

2.3.2. Fonctions polynomiales. — Commençons par un lemme préliminaire sur les fonctions polynomiales dans un corps p-adique. Ce lemme explique qu'une fonction polynôme, si elle reste petite par rapport à 1 pendant un certain temps, va être inférieure à 1 pendant longtemps :

Lemme 2.20 **(G. Tomanov)**. — *Soient* ε *et* α *deux réels positifs,* d*,* m *et* s *trois entiers positifs, et* p *un nombre premier fixé. Soit* $f = (f_1, \dots, f_s)$ *une fonction polynomiale de* $(\mathbb{Q}_p)^m$ *dans* $(\mathbb{Q}_p)^s$ *de degré inférieur à* d*.*

On pose $\delta = \frac{\varepsilon^d}{2(d+1)^d}$*, et on note* $\|.\|$ *la norme sup sur* $(\mathbb{Q}_p)^s$ *et* $(\mathbb{Q}_p)^m$ *dans la base canonique. De plus, on note* θ_m *le produit de* m *fois la mesure de Haar* θ_1 *sur* $\mathbb{Q}_p$ *qui donne masse* 1 *à l'ensemble* $\mathbb{Z}_p$*.*

Alors pour toute boule $B = B(t_0, r)$ *de* $(\mathbb{Q}_p)^m$*, telle que* $\|f(t_0)\| \geq \alpha$*, on a l'estimation suivante :*

$$\theta_m \{t \in B \text{ tels que } \|f(t)\| \leq (\delta)^m \alpha\} \leq mp\varepsilon\theta_m \{t \in B \text{ tels que } \|f(t)\| \leq \alpha\}$$

Démonstration. — Tout d'abord, deux boules pour la norme sup dans $(\mathbb{Q}_p)^m$ sont soit disjointes soit l'une est incluse dans l'autre. On en déduit que l'ensemble des $t \in B$ tels qu'on a $\|f(t)\| \leq \alpha$ est une réunion disjointe de boules B'' maximales pour la propriété “pour tout $t \in B''$, on a $\|f(t)\| \leq \alpha$”. Pour chacune de ces boules B'', considérons la boule B' de rayon immédiatement supérieur. De sorte qu'on a $\theta_m \{t \in B' \text{ tels que } \|f(t)\| \leq \alpha\} \geq \frac{1}{p}\theta_m(B')$

Il suffit donc de montrer que, pour une telle boule B', on a :

$$\theta_m \{t \in B' \text{ tels que } \|f(t)\| \leq (\delta)^m \alpha\} \leq m\varepsilon\theta_m(B')$$

Or par définition, il existe un t dans B' tel que $\|f(t)\| \geq \alpha$, et ce point t, comme tout point de la boule, est le centre de cette boule. Enfin en appliquant des transformations linéaires, on peut supposer que $t = 0$ et $r = \alpha = 1$.

Pour résumer, on est ramené à démontrer le lemme suivant :

Lemme 2.21. — *Soient ε un réel positif; d, m et s trois entiers positifs. On considère $f = (f_1, \ldots, f_s)$ une fonction polynomiale de $(\mathbb{Q}_p)^m$ dans $(\mathbb{Q}_p)^s$ de degré inférieur à d qui vérifie que $\|f(0)\| \geq 1$.*

On pose $\delta = \frac{\varepsilon^d}{2(d+1)^d}$. Alors, on a l'inégalité :

$$\theta_m \left(\{t \in B(0,1) \text{ tels que } \|f(t)\| \leq \delta^m\}\right) \leq m\varepsilon$$

La preuve se fait alors par récurrence sur le nombre m de variables. On commence par montrer la propriété de propagation, qui est facile, avant d'initialiser au cas $m = 1$.

Propagation :

Supposons le lemme vrai pour tous les $m \leq M$. On veut le montrer pour $M + 1$. Soit donc f une fonction polynomiale de $(\mathbb{Q}_p)^{M+1}$ dans $(\mathbb{Q}_p)^s$, de degré inférieur à d. En écrivant $(\mathbb{Q}_p)^{M+1} = \mathbb{Q}_p \times (\mathbb{Q}_p)^M$, on peut écrire $B(0,1) = B_1(0,1) \times B_M(0,1)$. Alors, d'après l'hypothèse de récurrence, l'ensemble I_M des $T \in B_M$ tels que $\|f(0,T)\| < \delta^M$ est de mesure petite : $\theta_M(I_M) \leq M\varepsilon$.

Et pour tout point T en dehors de I_M, on a à nouveau par hypothèse de récurrence, $\theta_1(\{t \in B_1 \text{ tels que } \|f(t,T)\| < \delta^{M+1}\} \leq \varepsilon$.

On tire facilement de ces deux majorations l'inégalité voulue :

$$\theta_{M+1} \left(\{t \in B \text{ tels que } \|f(t)\| \leq \delta^{M+1}\}\right) \leq (M+1)\varepsilon$$

Il reste à initialiser la récurrence.

Initialisation : Le cas $m = 1$ est fait dans [36], mais nous refaisons ici sa preuve. Pour simplifier les notations, on note θ la mesure θ_1.

On peut faire une autre simplification : on sait que $\|f(0)\| \geq 1$, c'est à dire qu'il existe $1 \leq i \leq s$ tel que $|f_i(0)| \geq 1$. Or, si on montre que $\theta\left(\{t \in B(0,1) \text{ tels que } |f_i(t)| \leq \delta\}\right) \leq \varepsilon$, alors le lemme 2.21 est démontré. Donc il suffit de démontrer ce lemme avec $s = 1$.

On raisonne alors par l'absurde. On note A l'ensemble défini comme

$$\{t \in B(0,1) \text{ tels que } |f_i(t)| \leq \delta\}$$

et on suppose $\theta(A) > \varepsilon$.

Alors, on trouve $d+1$ points de A $a_0, \ldots a_d$, distants deux à deux d'au moins $\frac{\varepsilon}{d+1}$. En effet on raisonne par récurrence : on choisit a_0 quelconque dans A. Si, pour $k < d$ on a

$k+1$ points $a_0, \dots a_k$, distants deux à deux d'au moins $\frac{\varepsilon}{d+1}$, la mesure de l'union disjointe $\bigcup_0^k B(a_i, \dfrac{\varepsilon}{d+1})$ est égale à $\frac{(k+1)\varepsilon}{d+1} < \varepsilon$. Or on a supposé que la mesure $\theta(A)$ est plus grande que ε. Donc on trouve un point a_{k+1} dans A distant d'au moins $\frac{\varepsilon}{d+1}$ des points $a_0, \dots a_k$.

En écrivant l'interpolation de Lagrange de f aux points $(a_i)_{0\leq i\leq d}$, on obtient, pour tout t de $\mathbb{Q}_p$:

$$f(t) = \sum_{i=0}^{d} f(a_i) \prod_{j\neq i} \frac{t-a_j}{a_i-a_j}$$

Après avoir posé $t=0$ dans l'égalité précédente, on observe que chaque terme de la somme est de valeur absolue inférieure à $\delta\left(\frac{d+1}{\varepsilon}\right)^d \leq \frac{1}{2}$. En utilisant l'ultramétricité de la valeur absolue, on obtient que $|f(0)| \leq \frac{1}{2}$. C'est bien la contradiction recherchée. Et le cas $m=1$ du lemme est prouvé.

La preuve par récurrence est donc finie, on a montré le lemme 2.20.

□

2.3.3. Fonctions polynomiales et sous-variétés algébriques. — À partir du lemme précédent, on déduit un résultat sur les fonctions polynomiales qui restent proches d'un fermé algébriques :

***Proposition 2.22* (G. Tomanov).** — *Soient s, d et m trois entiers et M un ensemble Zariski-fermé de $(\mathbb{Q}_p)^s$. Soient ε un réel positif, et A un compact de M. Alors il existe un compact C de M contenant A tel que :*

pour tout voisinage W_0 de C dans $(\mathbb{Q}_p)^s$, il existe un voisinage relativement compact W de A dans $(\mathbb{Q}_p)^s$ tel que pour toute fonction f de $\mathcal{P}_{d,m}(GL(s,\mathbb{Q}_p))$, pour tout $x \in (\mathbb{Q}_p)^s - W_0$, pour toute boule $B = B(0,r)$ de $(\mathbb{Q}_p)^m$, on a :

$$\theta_m\left(\{t \in B \textit{ tels que } f(t)x \in W\}\right) \leq \varepsilon\theta_m\left(\{t \in B \textit{ tels que } f(t)x \in W_0\}\right)$$

A nouveau, la différence avec l'énoncé de G. Tomanov est le fait d'envisager des fonctions polynômes à plusieurs variables. Et encore une fois, nous pouvons suivre sa preuve.

Démonstration. — On remarque qu'il suffit de montrer cette proposition pour un compact A de la forme $A = M\cap B(0,R)$ pour un réel positif R quelconque (ici, $B(0,R)$ est une boule dans l'espace vectoriel $(\mathbb{Q}_p)^s$). On fixe donc deux entiers d et m et ε un réel strictement positif.

Soient $f_1, \dots, f_l$ des polynômes à s indéterminées tels que M est l'ensemble annulateur des (f_i). On note k un majorant du degré des (f_i), et $n = kd$. On pose $\delta = \frac{\varepsilon^n}{2(n+1)^n}$, et $C = M \cap B(0, R\delta^{-m})$.

On veut montrer que ce compact C convient pour la proposition. On se donne donc un voisinage W_0 compact de C, une fonction f appartenant à $\mathcal{P}_{d,m}(GL(s,\mathbb{Q}_p))$ et un point $a \notin W_0$.

Alors les composantes de l'application de $\mathbb{Q}_p^m$ dans $\mathbb{Q}_p^s$ donnée par $t \to f(t)a$ sont polynomiales de degré inférieur à d, et donc $F_i(t) = f_i(f(t)a)$ est un polynôme en m variables de degré inférieur à n pour tout $1 \leq i \leq l$.

On peut alors trouver un voisinage W_1 de C inclus dans W_0 qui se définisse avec les normes des polynômes F_i : techniquement il existe $\alpha > 0$ tel que l'ensemble :

$$W_1 = \{v \in (\mathbb{Q}_p)^s \text{ tels que } \forall 1 \leq i \leq l,\ |F_i(v)| \leq \alpha\} \cap B(0,(R+\alpha)\delta^{-m})$$

est inclus dans W_0. Cette définition de W_1 nous permet d'utiliser le lemme 2.20. En effet, il est naturel de poser $W = \{v \in (\mathbb{Q}_p)^s \text{ tels que } \forall 1 \leq i \leq m,\ |F_i(v)| \leq \alpha\delta^m\} \cap B(0,R+\alpha)$. C'est un voisinage relativement compact de A. Il suffit alors de montrer qu'il convient.

Soit donc $B = B(0,r)$ une boule dans $(\mathbb{Q}_p)^m$. Alors pour toute boule $B' \subset B$ telle que $f(B')a$ est inclus dans W_1 et B' est maximale pour cette propriété, il existe un point t_0 de B' tel que ou bien on a $\|f(t_0)a\| \geq R\delta^{-m}$, ou bien $|F_i((t_0)| \geq \alpha$ pour un certain i.

Mais alors, d'après le lemme 2.20, appliqué à $t \to (F_1,\ldots,F_l,f)$, on a les deux inégalités suivantes :

$$\begin{aligned}\theta_m\{t \in B' \text{ tels que } f(t)x \in W\} &\leq \varepsilon m\theta_m(B') \\ &\leq m\varepsilon\theta_m\{t \in B' \text{ tels que } f(t)x \in W_0\}\end{aligned}$$

Cette inégalité est vraie pour toute boule B' comme décrit ci-dessus, elle est donc vraie pour la boule B elle-même.

La proposition est ainsi démontrée. □

On en déduit le corollaire suivant, qui permet de traiter plusieurs nombres premiers. Pour cela, par un léger abus de langage qui permet de ne pas alourdir encore les notations, on note toujours θ_1 la mesure de Haar sur k_f qui est le produit des mesures θ_1 sur chacun des $\mathbb{Q}_p$; et θ_m la mesure produit sur $(k_f)^m$:

Corollaire 2.23. — *Soient M un ensemble Zariski-fermé de $(k_f)^s$, d, m deux entiers. Soient ε un réel positif, et A un compact de M. Alors il existe un compact C de M contenant A tel que :*

pour tout voisinage W_0 de C dans $(k_f)^s$, il existe un voisinage relativement compact W de A dans $(\mathbb{Q}_p)^s$ tel que pour toute fonction f de $\mathcal{P}_{(d,m)}(GL(s,k_f))$, pour tout $x \in (k_f)^s - W_0$, pour toute boule $B = B(0,r)$ de $(k_f)^m$, on a :

$$\theta_m(\{t \in B \text{ tels que } f(t)x \in W\}) \leq \varepsilon\theta_m(\{t \in B \text{ tels que } f(t)x \in W_0\})$$

Démonstration. — On a l'inégalité composante par composante : il suffit de prendre comme compact C le produit des compacts qu'on obtient dans la proposition 2.22, et pour W_0 choisi

- qu'on peut supposer être un produit quitte à le réduire - on obtient dans chaque $(\mathbb{Q}_p)^s$ un W_p, et on peut prendre $W = \prod W_p$. On vérifie aisément que cela convient. □

2.3.4. Le théorème de G. Tomanov. — Il reste donc à prouver le théorème 2.19. Là encore nous nous inspirons de G. Tomanov, mais nous profitons de la compacité de G/Γ pour simplifier la preuve.

Preuve du théorème 2.19. — Il est naturel de vouloir appliquer le corollaire 2.23. Pour cela on fait la construction suivante : soit C' un relevé compact de C dans G. Posons alors $A = \eta(C')$. C'est un compact de $F(P, U)$, qui est un fermé de Zariski de V_G. On fixe un $\varepsilon > 0$. On remarque en outre que si f est une fonction de $\mathcal{P}_{d,m}(G)$, alors $\rho \circ f$ appartient à $\mathcal{P}_{d',m}(GL(V_G))$, pour un certain d' (on rappelle que ρ est la représentation de G dans $GL(V_G)$ telle que $\eta(g) = \rho(g)v_P$).

Donc on peut utiliser directement le corollaire 2.23, avec le ε fixé, le compact A défini et l'entier d'. On obtient alors un compact D de $F(P, U)$ qui vérifie ce corollaire, et qui est notre candidat pour montrer le théorème 2.19. Remarquons avant de continuer qu'on peut toujours réduire W_0 : en effet, si pour un certain W_0, on trouve un W qui convient, alors il conviendra pour tous les W_0' qui contiennent W_0.

Fixons donc un voisinage W_0 de D dans V_G, qu'on peut supposer relativement compact quitte à le réduire, et on cherche un voisinage W de C dans G/Γ. On procède ainsi : le corollaire 2.23 nous donne un voisinage V de A relativement compact tel que pour toute fonction f de $\mathcal{P}_{d,m}(GL(s, k_f))$, pour tout $x \in (k_f)^s - W_0$, pour toute boule $B = B(0, r)$ de $(k_f)^m$, on a :

$$\theta_m\left(\{t \in B \text{ tels que } f(t)x \in V\}\right) \leq \varepsilon\theta_m\left(\{t \in B \text{ tels que } f(t)x \in W_0\}\right)$$

On pose ensuite $W' = \eta^{-1}(V)$, puis $W = W'\Gamma/\Gamma$. C'est bien un voisinage de C dans G/Γ, il reste à montrer qu'il convient.

Nous fixons donc une boule B de $(k_f)^m$ et une fonction f dans $\mathcal{P}_{d,m}(G)$, et supposons que la première possibilité du théorème est fausse, c'est à dire que pour tout $\gamma \in \Gamma$, il existe t dans B tel que $\eta(f(t)\gamma)$ n'est pas dans W_0. On veut alors montrer que la deuxième possibilité est bien vérifiée, c'est à dire qu'on a $\theta_m(\{t \in B \text{ tels que } (f(t)\Gamma/\Gamma) \in W\}) < \varepsilon\theta_m(B)$.

Or on a vu que si γ appartient à Γ, alors la fonction $t \to \rho(f(t)\gamma)$ appartient à $\mathcal{P}_{d',m}(GL(V_G))$. De plus d'après l'hypothèse faite, il existe t dans B tel que $\eta(f(t)\gamma) = \rho(f(t)\gamma)v_P$ n'est pas dans W_0. Donc, on peut appliquer le corollaire 2.23, et on obtient l'inégalité suivante, pour tout γ dans Γ :

$$\theta_m(\{t \in B \text{ tels que } \eta(f(t)\gamma) \in V\}) < \varepsilon\theta_m(\{t \in B \text{ tels que } \eta(f(t)\gamma) \in W_0\})$$

On aimerait ainsi contrôler à t fixé l'ensemble des γ dans Γ tel que $\eta(f(t)\gamma) \in W_0$. Le lemme suivant nous donne l'existence d'une borne uniforme à son cardinal.

Lemme 2.24. — *Soit E un compact de V_G. Alors il existe un entier N_0 tel que pour tout $g \in G$, le cardinal de l'ensemble $\{\gamma \in \Gamma/\Gamma_N$ tels que $\eta(g\gamma) \in E\}$ est inférieur à N_0.*

Démonstration. — Comme G/Γ est compact, il existe un ensemble E' compact tel que $G = E'\Gamma$. Soit $g = e\gamma_0$ dans G.

Alors l'ensemble $\{\gamma \in \Gamma/\Gamma_N$ tels que $\eta(g\gamma) \in E\}$ est envoyé par η sur l'ensemble des points de $\eta(\Gamma)$ appartenant au compact $\rho(e^{-1})E$. Donc, il est de cardinal inférieur au cardinal de $\eta(\Gamma) \cap \rho(E'^{-1})E$. Or le deuxième membre de cette intersection est compact et le premier discret dans V_G, donc leur intersection est finie de cardinal un certain entier N_0. On en déduit que le cardinal de $\{\gamma \in \Gamma/\Gamma_N$ tels que $\eta(g\gamma) \in E\}$ est inférieur à N_0. Le lemme est donc bien prouvé.

□

Donnons nous un voisinage compact D' de D fixé indépendamment du W_0 choisi. On dispose donc d'un entier N_0 tel que, pour tout t dans B, l'ensemble des $\gamma \in \Gamma/\Gamma_N$ tel que $\eta(f(t)\gamma) \in D'$ est de cardinal inférieur à N_0. Et quitte à réduire encore une fois W_0 à son intersection avec D', on suppose qu'il a la même propriété. On note dorénavant Γ_0 un ensemble de représentants de Γ/Γ_N.

Rappelons notre objectif. On veut montrer l'inégalité :

$$\theta(\{t \in B \text{ tels que } (f(t)\Gamma/\Gamma) \in W\}) < \varepsilon\theta(B)$$

On écrit alors, par définition de W et de V l'égalité ensembliste suivante :

$$\{t \in B \text{ tels que } f(t)\Gamma/\Gamma \in W\} = \bigcup_{\gamma_0 \in \Gamma_0} \{t \in B \text{ tels que } \eta(f(t)\gamma_0) \in V\}$$

Traduit en terme de mesure, cela nous donne la suite d'inégalités suivante :

$$\begin{aligned}
\theta_m(\{t \in B \text{ tels que } f(t)\Gamma/\Gamma \in W\}) &\leq \sum_{\gamma_0 \in \Gamma_0} \theta_m(\{t \in B \text{ tels que } \\
&\qquad\qquad \eta(f(t)\gamma_0) \in V\}) \\
&\leq \varepsilon \sum_{\gamma_0 \in \Gamma_0} \theta_m(\{t \in B \text{ tels que } \\
&\qquad\qquad \eta(f(t)\gamma_0) \in W_0\}) \\
&\leq N_0\varepsilon\theta_m(B)
\end{aligned}$$

La dernière inégalité s'obtient grâce à la définition de N_0 : à chaque instant $t \in B$, il y a au plus N_0 classes modulo Γ_N, représentées par $\gamma_1, \ldots, \gamma_{N_0}$ dans Γ_0 telles que $\eta(f(t)\gamma_i) \in W_0$.

On a donc bien le résultat voulu, N_0 ne dépendant pas de W_0. □

Grâce à ce théorème et au théorème 2.16, nous pouvons comprendre les mesures U-invariantes sur G/Γ.

2.4. Equirepartition des orbites de H dans G/Γ

Nous passons à la deuxième application : le théorème 2.2. Nous suivons pour cela la stratégie de N. Shah (Cf [33]) : on commence par prouver une proposition intermédiaire semblable au théorème, mais pour des mesures portées par un certain groupe unipotent, en utilisant les outils expliqués dans les parties 2.2 et 2.3, puis nous décomposons la mesure sur K en de telles mesures.

2.4.1. Préliminaires. — Pour énoncer la proposition intermédiaire, nous avons besoin d'une décomposition de Cartan dans le groupe H de la forme $H = K_0 A^+ D K_0$. Pour cela fixons A_p un tore maximal $\mathbb{Q}_p$ déployé dans H_p, pour chaque p de S tel que H_p est non compact. On dispose alors d'un système de racines (restreintes) simples positives Φ_p. Soit A_p^+ le sous-semigroupe de A_p associé à la chambre définie par Φ_p. Alors, il existe un compact K_p et un ensemble fini D_p dans le centralisateur de A_p tel que H_p est l'union disjointe : $H_p = \bigcup_{a \in A_p^+ \,,\, d \in D_p} K_p a d K_p$. Pour l'existence de tels objets, on renvoie à [35].

Dans le cas où ν appartient à S et H_ν est compact, on prend $K_\nu = H_\nu$, et A_ν ainsi que D_ν sont réduits à l'identité. On considère maintenant A^+ le produit pour ν dans S des A_ν^+, de même, K_0 et D sont le produit respectivement des K_ν et D_ν. Φ est l'union des Φ_ν. Si α appartient à $\Phi_\nu \subset \Phi$, et $a = (a_\nu)_{\nu \in S}$ appartient à A^+, alors on pose $\alpha(a) = \alpha(a_\nu)$.

Considérons maintenant une suite (a_n) d'éléments de A^+, non bornée. Nous définissons une hypothèse sur la suite (a_n) :

Définition 2.25. — Une suite (a_n) d'éléments de A^+, non bornée est dite simplifiée si pour tout α dans Φ, on a l'alternative :
- Soit $\alpha(a_n)$ est une suite bornée
- Soit $\alpha(a_n)$ tend vers l'infini avec n

On peut dans ce cas définir le sous groupe de H

$$U^+ = \left\{ h \in H \text{ tels que } \lim_{n \to \infty} a_n^{-1} h a_n = e \right\}$$

On remarque alors que c'est un sous-groupe de H dont tous les éléments sont unipotents.

Voilà le résultat d'équirépartition des mesures portées par le groupe U^+ :

Proposition 2.26. — *Soit* $\mathbf{G}$ *un groupe défini sur* $\mathbb{Z}$, *quasi-*$\mathbb{Q}$*-simple,* $\mathbb{R}$*-anistrope et simplement connexe. Soit* S *un sous-ensemble fini de* $\mathcal{V}$ *contenant* ∞. *Soit* Γ *un sous-groupe arithméthique de* $G = \mathbf{G}(k_S)$. *Notons* π *la projection de* G *sur* G/Γ *et* m *la probabilité de Haar sur* G/Γ.

Soient, pour tout $\nu \in S$, H_ν *le groupe des* $\mathbb{Q}_\nu$*-points d'un sous-*$\mathbb{Q}_\nu$*-groupe quasi-simple de* $\mathbf{G}(\mathbb{Q}_\nu)$. *On suppose que* $H = \prod_{\nu \in S} H_\nu$ *est non compact et que pour tout* ν *tel que* H_ν *est non compact,* $H_\nu \Gamma$ *est dense dans* G. *Soit enfin* K *un sous-groupe compact ouvert de* H. *On dispose de la probabilité de Haar* λ_K *sur* K.

Soient (a_n) une suite d'éléments de A^+ non-bornée et simplifiée, le sous-groupe $U^+ = \{h \in H$ tels que $lim_{n\to\infty} a_n^{-1} h a_n\}$ et l une probabilité sur U absolument continue par rapport à la mesure de Haar l_U sur U^+. Soit enfin h_0 dans H, et on note pour tout h dans H, $\pi'(h) = \pi(hh_0)$.

Nous avons alors la limite suivante dans l'espace des probabilités sur G/Γ :

$$\lim_{n\to\infty} \pi'_*((a_n)_* l) = m$$

C'est à dire que pour toute fonction φ continue sur G/Γ, on a :

$$\int_{U^+} \varphi(a_n h h_0 \Gamma/\Gamma) dl(h) \xrightarrow{n\to\infty} \int_{G/\Gamma} \varphi dm$$

Remarque 2.27. — On remarque que dans l'énoncé de ce lemme, on se permet de "tordre" la projection π de G dans G/Γ par un élément h_0 de H.

La démonstration de cette proposition fera appel à l'étude des orbites des groupes unipotents que nous avons faite. Nous avons de plus besoin d'un lemme supplémentaire sur la représentation ρ.

2.4.2. Action combinée d'un tore et d'un groupe unipotent. — Le phénomène qui nous intéresse est le suivant : pour une représentation ρ de H dans un k_S-module V, l'action combinée des a_n et d'un ouvert de U^+ envoie tout point non globalement invariant à l'infini. Voilà l'énoncé précis :

Lemme 2.28. — *Soit $\rho = (\rho_\nu)_{\nu\in S}$ une k_S-représentation de H dans un k_S-module $V = \prod_{\nu\in S} V_\nu$ de dimension finie, muni d'une norme quelconque $\|\ \|$. Soient (a_n) une suite d'éléments de A^+ non-bornée et simplifiée, et Ω un ouvert de l'ensemble*

$$U^+ = \left\{h \in H \text{ tels que } \lim_{n\to\infty} a_n^{-1} h a_n = 1\right\}$$

Soit N le sous-groupe normal de H engendré par U^+.

Soit Λ un ensemble discret de V. Soit (v_n) une suite de points de Λ dont aucun n'est N-invariant.

Alors, on a sup $\{\|\rho(a_n\omega)v_n\|$ pour $\omega \in \Omega\} \xrightarrow{n\to\infty} \infty$.

Démonstration. — Tout d'abord, en notant V^N le module des points N-invariants, et W son supplémentaire N-invariant, on peut noter pour tout n, $v_n = v_n^N + w_n$. Si w_n tend vers 0, alors, comme Λ est discret, v_n^N tend vers l'infini.

Or H est un produit de $\mathbb{Q}_\nu$-groupes quasi-simples, pour ν dans S. Donc, comme la suite (a_n) est simplifiée, la suite a_n est bornée dans H/N. Par définition, v_n^N est N-invariant, donc il existe une constante $c > 0$ tel que pour tout n entier, et pour tout ω dans Ω, on a $\|\rho(a_n\omega)v_n\| > c\|v_n^N\|$. Le lemme est donc vrai dans ce cas.

Donc on suppose que $\|w_n\|$ est minorée. Et, quitte à extraire une sous-suite, on suppose que la norme de la projection v'_n de w_n dans un sous-module irréductible V' de V est minorée. On peut donc normaliser les v'_n pour qu'ils soient de norme 1. Or la sphère unité dans cet espace est compacte, donc, quitte à extraire une sous-suite, on peut supposer que v'_n tend vers un point v. Ici on a bien-sûr perdu l'hypothèse de discrétude de Λ, mais nous n'en aurons plus besoin.

Le lemme suivant explique que l'on peut supposer que v a une composante U^+-invariante non-nulle. Pour cela, définissons V^U l'espace des points U^+-invariants de V. Il admet un unique supplémentaire V^- invariant par la suite (a_n). Notons $v = v_U + v_-$ et p_U la projection sur V^U parallèlement à V^-. Montrons le lemme suivant :

Lemme 2.29. — *Soient $\rho = (\rho_\nu)_{\nu\in S}$ une k_S-représentation de H dans un k_S-module $V = \prod_{\nu\in S} V_\nu$ de dimension finie, (a_n) une suite d'éléments de A^+ non-bornée et simplifiée et Ω un ouvert de l'ensemble $U^+ = \{h \in H$ tels que $lim_{n\to\infty} a_n^{-1} h a_n = 1\}$. Soit v un point de V de norme* 1.

Alors, il existe ω_0 dans Ω tel que $p_U(\omega_0 v)$ est non nulle.

Démonstration. — On démontre ce lemme par l'absurde : supposons que l'ensemble Ωv est inclus dans V^-. Considérons alors le k_S-module V_Ω engendré par tous les ωv pour $\omega \in \Omega$. Il est de type fini, donc il est engendré par des points $\omega_1 v, \dots, \omega_k v$. Et il existe un voisinage de l'identité Ω' dans U^+ tel que pour tout $1 \leq i \leq k$, $\Omega' \omega_i$ est inclus dans Ω.

Donc V_Ω est invariant par Ω'. Or le fait de stabiliser un sous-module est une propriété Zariski-fermée, donc V_Ω est invariant par toute l'adhérence de Zariski de Ω' dans U^+, c'est à dire par U^+ tout entier.

On applique maintenant le théorème de Lie-Kolchin (plus exactement pour chaque ν de S, on applique ce théorème à la représentation ρ_ν de H_ν dans V_ν) : V_Ω est un module invariant par un groupe unipotent, donc ce groupe a un point fixe dans V_Ω. Or V_Ω est inclus dans le supplémentaire des points fixes de U. Nous avons la contradiction recherchée. □

Ainsi il reste plus qu'à montrer qu'un point U^+-invariant et non N-invariant est envoyé à l'infini.

Lemme 2.30. — *Soit v_0 un point de V qu'on suppose U^+-invariant mais pas N-invariant. Alors $\|\rho(a_n)v_0\|$ tend vers l'infini avec n.*

Démonstration. — Quitte à décomposer, on suppose que chaque ρ_ν est une représentation irréductible de H_ν.

On raisonne par l'absurde : on suppose que $\|\rho(a_n)v_0\|$ reste borné. On va montrer que pour tous les points v de V, $\|\rho(a_n)v\|$ reste borné, puis que tous ces points sont U^+-invariants. Ils seront alors N-invariants, ce qui sera notre contradiction.

Notons W le sous-k_S-module de V composé de tous les w de V tels que la suite $(\rho(a_n)w)$ reste bornée. Et soit P^- le parabolique opposé à U^+ :

$$P^- = \left\{ g \in H \text{ tels que } a_n g a_n^{-1} \text{ reste bornée } \right\}$$

Alors, on vérifie que $\rho(P^-)v_0$ est inclus dans W ; comme v_0 est U^+-invariant, $\rho(P^-U^+)v_0$ est inclus lui aussi dans W. Or l'ensemble des h de H tels que $\rho(g)v_0$ appartient à W est un k_S-fermé algébrique et P^-U^+ est un ouvert de H. Donc $\rho(H)v_0$ est inclus dans W, et finallement $V = W$ par irréducibilité.

Fixons maintenant un élément v de V, et ω dans U^+. Soit Ω un voisinage ouvert compact de l'identité dans U^+. Alors, par définition, il existe un entier i tel que $a_i^{-1} w a_i$ appartient à Ω. On en déduit que $\rho(\omega)v$ appartient à $\rho(a_i\Omega)v$, qui est inclus dans un compact B indépendant de i, car on a vu que v est dans $W = V$.

Donc $\rho(U^+)v$ est inclus dans B. Or U^+ est un groupe unipotent, donc $\rho(U^+)v$ est l'image de tout k_S par une fonction polynomiale à plusieurs variables. Cette image ne peut-être bornée que si la fonction est constante. Donc v est U^+ invariant.

Ainsi le noyau de la représentation ρ contient U^+, donc N. Ce qui est une contradiction avec le fait que l'action de N est supposée non trivialle. □

Ainsi le lemme 2.28 est démontré. □

Maintenant que ce lemme est prouvé, nous avons tous les outils nécessaires à la démonstration de la proposition 2.26. Nous la faisons dans la partie suivante.

2.4.3. Equirépartition des mesures portées par un groupe unipotent. — On veut donc montrer cette proposition 2.26. La stratégie que nous suivons est de montrer en premier lieu que toute mesure limite est invariante par le groupe unipotent U tout entier. On peut alors utiliser le thórème 2.19 et le lemme 2.28 pour montrer que cette mesure limite est la probabilité de Haar sur G/Γ.

Preuve de la proposition 2.26. — On peut supposer sans perte de généralité que l est à support compact dans U^+.

Remarquons tout d'abord que la suite $(\pi'_*((a_n)_*l))$ est une suite de probabilités sur G/Γ. Or G/Γ est compact, donc l'ensemble des probabilités sur G/Γ est lui même compact. On dispose donc d'une valeur d'adhérence M, et on veut montrer que cette valeur d'adhérence est m, la probabilité de Haar sur G/Γ. Pour simplifier, on suppose $\pi'_*((a_n)_*l) \xrightarrow{n\to\infty} M$.

Fait : M est U^+-invariante.

Démonstration. — On utilise ici l'action dilatante de la suite (a_n) sur les éléments de U^+. Si u appartient à U^+, on note $u_n = a_n^{-1} u a_n$. Alors, par définition, u_n tend vers 1, et on voit que $ua_n = a_n u_n$. Ainsi, si φ est une fonction continue à support compact sur G/Γ, et si on note f la densité de l par rapport à l_U, on fait le calcul suivant :

$$\begin{aligned}\int_{G/\Gamma}\varphi d(u_*\pi'_*((a_n)_*l)) &= \int_{U^+}\varphi(\pi'(a_nu_nz))dl(z)\\ &= \int_{U^+}\varphi(\pi'(a_nu_nz))f(z)dl_U(z)\\ &= \int_{U^+}\varphi(\pi'(a_nz))f(u_n^{-1}z)dl_U(z)\end{aligned}$$

Cette dernière égalité s'obtient par U^+-invariance de l_U. On en déduit alors l'inégalité suivante :

$$|\int_{G/\Gamma}\varphi d(\pi'_*((a_n)_*l)) - \int_{G/\Gamma}\varphi d(u_*\pi'_*((a_n)_*l))| \leq (sup|\varphi|)\int_{U^+}|f(u_nz)-f(z)|dl_U(z)$$

En passant à la limite en n dans l'inégalité précédente, on voit que $u_*M = M$. Donc M est bien invariante par tout le groupe U □

Nous pouvons maintenant utiliser la théorie exposée dans la partie 2.3.

D'après le théorème 2.16, il existe un sous-groupe $\mathbf{P}$ de $\mathbf{G}$ de la classe $\mathcal{F}$ tel que $M(\pi(X(P,U^+)))$ est strictement positive. On veut montrer que $\mathbf{P} = \mathbf{G}$. Pour cela, on va utiliser le théorème 2.19. Soit donc C un compact de $\pi(X(P,U^+))$ de mesure strictement positive.

Pour chaque p de S_f, on note $\mathcal{U}_p$ l'algèbre de Lie de la composante $U^+\cap H_p$ de U^+ dans H_p (comme $\mathbf{G}(\mathbb{R})$ est compact, l'éventuelle intersection $U^+\cap H_\infty$ est réduite à l'identité). Les algèbres $\mathcal{U}_p$ peuvent être réduites à un point mais elles sont de toute façon en bijection avec $\mathbb{Q}_p^{m_p}$ pour un certain entier $m_p \geq 0$. On note exp_p la fonction exponentielle de $\mathbb{Q}_p^{m_p}$ dans $U^+\cap H_p$. C'est une fonction polynomiale, car $\mathcal{U}_p$ est nilpotente.

On note alors $\mathcal{U} = \prod_{p\in S_f}\mathcal{U}_p$, et on note exp le produit des fonctions exp_p. Quitte à rajouter des variables muettes, on suppose que exp est une fonction polynomiale de $(k_f)^m$ dans G de degré au plus un certain d. De plus il existe une boule B de $(k_f)^m$ telle que la mesure l est absolument continue par rapport à la mesure $(exp_{|B})_*(\theta_m)$ (le fait d'avoir rajouté des variables ne change que des constantes multiplicatives, et donc pas l'absolue continuité).

C'est à dire qu'il existe un $\varepsilon > 0$ tel que pour tout sous-ensemble E de C, on a :

$$\text{Si } \frac{1}{\theta_m(B)}(exp_{|B})_*(\theta_m)(E) < \varepsilon \text{ , alors } \pi'_*(l)(E) < \frac{M(C)}{2}.$$

On peut donc appliquer le théorème 2.19 aux fonctions $\Theta_n(t) = a_nexp(t)h_0$, au compact C et au ε qu'on vient de définir. On dispose alors d'un compact D de $F(P,U)$ tel que pour tout voisinage W_0 de D, il existe un voisinage W de C tel que pour tout n, on ait l'alternative :

– il existe $\gamma_n \in \Gamma$ tel que $\eta(\Theta_n(B)\gamma_n) \subset W_0$
– $\theta_m(\{t \in B \text{ tels que } \Theta_n(t)\Gamma/\Gamma \in W\}) < \varepsilon\theta_m(B)$

On fixe un voisinage relativement compact W_0 de D. On veut montrer qu'on est dans le premier cas de l'alternative ci-dessus. En effet la deuxième possiblité se traduit par :

$$\frac{1}{\theta_m(B)}\pi'_*((exp_{|B})_*(\theta_m))(a_n^{-1}W) < \varepsilon$$

Ceci, par définition de ε, implique alors que $\pi'_*((a_n)_*l)(W) < \frac{M(C)}{2}$. Or W contient C, et $\pi'_*((a_n)_*l)$ tend vers M, donc pour n grand, on ne remplit pas la deuxième condition de l'alternative.

Ainsi, quitte à extraire une sous-suite, on peut supposer qu'on est toujours dans le premier cas : pour tout n positif, il existe $\gamma_n \in G$ tel que $\eta(\Theta_n(B)\gamma_n) \subset W_0$.

On peut alors appliquer le lemme 2.28. Pour cela, il est naturel de penser à la représentation ρ de G dans le k_S-module V associée à $\mathbf{P}$ définie à la partie 2.2.2, et de la considérer comme une représentation de H dans V. Notons Λ l'ensemble disret $\eta(h_0\Gamma)$.

Nous sommes donc dans les conditions du lemme 2.28. Donnons nous une norme $\|.\|$ sur V, et notons N le sous-groupe normal de H engendré par U^+. Il existe un nombre premier $p_0 \in S_f$ tel que H_{p_0} est non compact et N contient un sous-groupe d'indice fini H'_{p_0} de H_{p_0}.

Par construction, $\eta(\Theta_n(B)\gamma_n)$ est inclus dans W_0 ; on obtient ainsi :

$$sup\,\{\|\rho(a_n exp(t))\eta(h_0\gamma_n))\| \text{ pour } t \in B\} \text{ est borné.}$$

Cela contredit la conclusion du lemme 2.28. C'est donc que l'hypothèse de ce lemme n'est pas vérifiée, c'est à dire que, pour un certain entier n, le point $\eta(h_0\gamma_n)$ est N-invariant.

Nous avons fait la plus grande partie du travail, et il reste à conclure. En reprenant les notations et les résultats de la partie 2.2.3, on obtient : $N \subset \gamma_n N_1(P)\gamma_n^{-1}$. Autrement dit, $\gamma_n N_1(P)\gamma_n^{-1}$ contient H'_{p_0}. Ainsi la projection de $N_1(P)$ dans G/Γ est un fermé contenant $\gamma_n^{-1}H'_{p_0}\Gamma/\Gamma$, donc est égal à G/Γ (on a supposé que $H_{p_0}\Gamma/\Gamma$ est dense dans G/Γ). Donc $N_1(P)$ contient un ouvert de G

Donc $N_1(P)$ est Zariski-dense dans G, et on obtient $N_1(P)G$, c'est-à-dire que $\mathbf{P}$ est un sous-groupe normal de $\mathbf{G}$, et $\mathbf{P}$ est d'indice fini dans $\mathbf{G}$ ($\mathbf{G}$ est supposé quasi-$\mathbb{Q}$-simple). Donc, d'après le théorème 2.16, M est invariante par un sous-groupe P' d'indice fini de G et tel que $\pi(P)$ est un fermé de G/Γ. Mais alors, par simple connexité de $\mathbf{G}$, P contient tous les facteurs isotropes de G, et $P\Gamma$ est dense dans G. Donc M est G-invariante, et donc M est l'image de la mesure de Haar de G. La proposition 2.26 est ainsi démontrée. □

Nous pouvons maintenant utiliser l'équirépartition sous l'action de a_n des mesures portées par U^+ dans G/Γ pour prouver celle de la probabilité de Haar sur K.

2.4.4. Équirépartition des grandes sphères. — Rappelons tout d'abord que nous voulons montrer le théorème 2.2, c'est à dire que, pour toute suite (g_n) d'éléments de H qui tend vers l'infini, on a la limite suivante dans l'espace des probabilités sur G/Γ :

$$\lim_{n\to\infty}\pi_*((g_n)_*\lambda_K) = m$$

Maintenant que nous disposons de la proposition 2.26, ce n'est plus très difficile. En effet, l'idée est de décomposer sur des ouverts du type $P^-U^+ \cap K$ la mesure $\lambda_{|P^-U^+}$ en une intégrale de mesures sur U^+. Toutes ces mesures s'équirépartissant, on peut en déduire l'équirépartition de la mesure λ. Il s'agit là d'un avatar de l'idée qu'une grande sphère ressemble localement à une horosphère. Voilà la preuve précise :

Démonstration. — Tout d'abord, on peut noter pour tout n, $g_n = k_n^1 a_n d_n k_n^2$ en utilisant la décomposition de Cartan définie dans la partie 2.4.1 (ici on a $a_n \in A^+$, $d_n \in D$, et k_n^1, $k_n^2 \in K_0$). Quitte à extraire une sous-suite, on peut supposer que (a_n) est simplifiée, que $d_n = d$ est constante, et que k_n^1 et k_n^2 admettent une limite k_1 et k_2 dans K_0.

Soit alors $K' = (dk_2)K(dk_2)^{-1}$. C'est bien un sous-groupe compact ouvert de H. Soit π' la projection tordue par dk_2 : $\pi'(h) = \pi(hdk_2)$, pour h dans H. Alors, on voit que si $\lim_{n\to\infty}(k_1)_*\pi'_*((a_n)_*\lambda_{K'}) = m$, on a aussi $\lim_{n\to\infty}\pi_*((g_n)_*\lambda_K) = m$.

Pour montrer le théorème 2.2, il suffit donc de montrer que pour tout groupe compact ouvert K, toute suite simplifiée (a_n), et tout h_0 dans H, en posant $\pi'(h) = \pi(hh_0)$, on a $\lim_{n\to\infty}\pi'_*((a_n)_*\lambda_{|K}) = m$.

On suppose donc que a_n est simplifiée, et on dispose des sous-groupes P^- et U^+. Les algèbres de Lie de P^- et U^+ sont en somme directe, il existe donc un sous-groupe ouvert K' de K pour lequel $(P^-U^+) \cap K'$ est homéomorphe à $(P^- \cap K') \times (U^+ \cap K')$. Soit donc J l'ouvert de K défini par $J = (P^-U^+) \cap K'$. Par compacité de K, il existe $k_1, \ldots, k_r$ des points de K tels qu'on a : $K = \bigcup_{i=1}^{r} Jk_i$.

Donc, en notant π_i la projection "tordue" par k_i : $\pi_i(k) = \pi'(kk_i)$, on voit qu'il existe des mesures $(\nu_i)_{i=1,\ldots,r}$ portées par J, et absolument continue par rapport à λ_K telles que $\pi'_*(\lambda_K) = \sum_{i=1}^r(\pi_i)_*(\nu_i)$. On est alors ramené à démontrer le lemme suivant :

Lemme 2.31. — *Dans le cadre du théorème 2.2, soient (a_n) une suite simplifiée, ν une mesure sur J absolument continue par rapport à λ, et h_0 appartenant à K. On note pour tout k de K, $\pi'(k) = \pi(kh_0)$.*

Alors on a :

$$lim_{n\to\infty}\pi'_*((a_n)_*\nu) = \nu(J)m$$

Nous nous consacrons maintenant à prouver ce lemme.

Démonstration. — On note l_P la mesure de Haar sur P^+, et l_U celle sur U^+. Comme J est homéomorphe à $(P^- \cap K') \times (U^+ \cap K')$, la mesure ν est absolument continue par rapport au produit $l_P \otimes l_U$.

Rappelons alors un résultat sur la décomposition de mesures dans une situation produit (voir par exemple la proposition 6.1 de [33]) :

Proposition 2.32. — *Soient (X,μ) et (Y,λ) deux espaces mesurés, et ν une mesure sur $X\times Y$ absolument continue par rapport à $\mu\otimes\lambda$. Alors il existe une mesure ν_1 sur X absolument continue par rapport à μ, et pour presque tout x dans X une mesure ν_x sur $\{x\}\times Y$ absolument continue par rapport à $\delta_x\otimes\lambda$ telles que $\nu=\int_X \nu_x d\nu_1(x)$. C'est à dire :*

Pour toute fonction f continue à support compact sur $X\times Y$, la fonction $x\to\displaystyle\int_{\{x\}\times Y} f d\nu_x$ est μ-mesurable, et

$$\int_{X\times Y} f d\nu=\int_X\left(\int_{\{x\}\times Y} f d\nu_x\right)d\nu_1(x)$$

Dans notre cas, on obtient la décomposition suivante : il existe une mesure n sur $P^-\cap J$ et une fonction $w\to n_w$ de $P^-\cap J$ vers les mesure sur $U^+\cap J$ absolument continues par rapport à l_U telles que la mesure ν vérifie la formule :

$$\nu=\int_{P^-} n_w dn(w)$$

Or, d'après la proposition 2.26, pour presque tout w, on a la limite :

$$\pi'_*((a_i)_*n_w)\xrightarrow{i\to\infty} n_w(U^+\cap J)m$$

où m est toujours la probabilité de Haar sur G/Γ. De plus, si w est dans P^-, alors, $a_iwa_i^{-1}$ tend vers une limite w_0. On en déduit la limite :

$$\pi'_*((a_iw)_*n_w)\xrightarrow{i\to\infty} n_w(U^+\cap J)(w_0)_*m=n_w(U^+\cap J)m$$

Considérons alors φ une fonction continue à support compact sur G/Γ. En utilisant le théorème de convergence dominée, on fait le calcul suivant :

$$\begin{aligned}
\int_{G/\Gamma}\varphi\, d(\pi'_*((a_i)_*\nu)) &= \int_{P^-\cap J}\left(\int_{U^+\cap J}\varphi(\pi'(a_iwu))\,dn_w(u)\right)dn(w)\\
&= \int_{P^-\cap J}\left(\int_{G/\Gamma}\varphi\, d(\pi'_*((a_iw)_*n_w))\right)dn(w)\\
&\xrightarrow{n\to\infty} \left(\int_{P^-\cap J} n_w(U^+\cap J)\,dn(w)\right)\int_{G/\Gamma}\varphi\, dm\\
&= \nu(J)\int_{G/\Gamma}\varphi\, dm
\end{aligned}$$

□

Le lemme est ainsi démontré et on a vu que le lemme était suffisant pour montrer le théorème 2.2. Donc le théorème est prouvé. $\square$

CHAPITRE 3

SOUS-GROUPES H-LOXODROMIQUES

Introduction

Dans ce chapitre, nous trouvons les conditions nécessaires et suffisantes pour qu'il existe un sous-groupe de $SL(n,k)$ - où k est un corps local - dont toutes les matrices ont leur spectre inclus dans un sous-groupe d'indice fini H de k^*. Nous arrivons au résultat suivant :

Théorème 3.1. — *Soient n un entier supérieur à 2, k une extension finie de $\mathbb{Q}_p$, où p est un nombre premier, et H un sous-groupe d'indice fini de k^*.*

Alors, $SL(n,k)$ admet un sous-groupe $\mathbb{Q}_p$-Zariski dense, dont toutes les matrices ont toutes leurs valeurs propres dans H si et seulement si ou bien -1 est dans H, ou bien n n'est pas congru à 2 modulo 4.

Dans son article "Automorphismes des cônes convexes" (Cf [5]), Y. Benoist démontre notamment que $SL(n,\mathbb{R})$ admet un sous-groupe Zariski-dense dont toutes les matrices ont leur spectre inclus dans $\mathbb{R}^{+*}$ si et seulement si n n'est pas congru à 2 modulo 4.

On remarque alors qu'on retrouve la condition donnée dans [5] pour le cas réel, sauf si -1 est dans H, auquel cas il n'y a aucune obstruction à l'existence de ces sous-groupes.

Pour montrer ce théorème, nous étudierons dans un premier temps les éléments proximaux et loxodromiques des groupes Zariski-denses. Nous montrons ainsi, avec le théorème 3.3, que si Γ est un sous-groupe Zariski-dense de $SL(n,k)$ dont toutes les matrices ont leur spectre inclus dans k, alors Γ contient au moins un élément diagonalisable sur k à valeurs propres de modules distincts.

Dans un second temps, nous définissons et étudions la notion de H-valuation, qui est l'analogue de la notion de positivité dans [5]. Nous étudions notamment comment le fait que toutes les valeurs propres des matrices d'un groupe soient dans H peut se comprendre avec cette notion. C'est l'objet des propositions 3.16 et 3.23. Ce sont d'ailleurs ces deux dernières propositions qui seront cruciales pour la démonstration des deux théorèmes 3.15 et 3.21.

Le théorème 3.1 est alors une conséquence directe des théorèmes 3.3 et 3.21.

Cadre de la preuve

Nous définissons ici les objets qui nous serviront tout au long du chapitre.

Dans toute la suite, k désignera $\mathbb{Q}_p$ ou une extension finie de $\mathbb{Q}_p$ -donc un corps local muni d'une valeur absolue notée $|.|$-, H un sous-groupe d'indice fini de k^*, et V sera un k-espace vectoriel de dimension n. On notera $\mathbb{P}(V)$ l'espace projectif associé à V et V^* son dual. On notera d l'indice de H dans k^*, et $S = k^*/H$. On remarque que, le corps étant de caractéristique nulle, H est ouvert et fermé dans k^*.

On définit aussi l'espace $\mathbb{Q}(V)$ des hyperplans pointés : tout élément a de $\mathbb{P}(V) \times \mathbb{P}(V^*)$ est vu comme un couple (kv_a, V_a) où v_a est un élément de V, et V_a est un hyperplan de V. On note alors $\mathbb{Q}(V) = \{a = (kv_a, V_a) \in \mathbb{P}(V) \times \mathbb{P}(V^*) \ / \ v_a \in V_a\}$. Enfin on note X la variété des drapeaux de V.

On travaillera avec des actions de $GL(V)$ sur les espaces $\mathbb{P}(V)$, $\mathbb{P}(V^*)$, $\mathbb{Q}(V)$ et X. Ce sont les actions naturelles induites par l'action de $GL(V)$ sur V.

Dans ce texte, la seule notion de Zariski-densité utilisée sera celle de $\mathbb{Q}_p$-Zariski-densité, c'est à dire qu'on identifie k^m à $\mathbb{Q}_p^{m[k:\mathbb{Q}_p]}$ pour tout m. Ainsi, une partie de k^m est dite $\mathbb{Q}_p$-Zariski-dense (ou parfois Zariski-dense) si son image dans $\mathbb{Q}_p^{m[k:\mathbb{Q}_p]}$ est Zariski-dense.

3.1. Proximalité

3.1.1. Définitions. — Nous rappelons ici des résultats sur les actions proximales. On se restreint aux sous-groupes de $GL(n,k)$, ce qui amène quelques simplifications dans les énoncés. On pourra se reporter à la bibliographie (Cf [1], [3], [4]) pour les preuves qui ne sont pas faites.

Soit g dans $GL(V)$. On note $\lambda_1(g), \dots, \lambda_n(g)$ les valeurs propres de g répétées avec multiplicité avec $|\lambda_1| \geq |\lambda_2| \ldots \geq |\lambda_n|$. On dit que g est proximal si $|\lambda_1(g)| > |\lambda_2(g)|$.

On s'intéresse ici non seulement à la première valeur propre, mais aussi à toutes les autres. Donc nous avons besoin de définir la notion d'éléments loxodromiques, de la manière suivante :

Définition 3.2. — On dit que $g \in SL(n,k)$ est loxodromique s'il est diagonalisable dans k et que toutes ses valeurs propres sont de multiplicité 1 et de valeurs absolues distinctes. Cela équivaut à dire que son image $\Lambda^m(g)$ par la représentation de $SL(n,k)$ dans $\Lambda^m V$ est proximale pour tout m compris entre 1 et $n-1$.

De plus on dit qu'un sous-groupe Γ de $GL(n,k)$ est proximal (resp. loxodromique) s'il contient un élément proximal (resp. loxodromique).

On peut alors énoncer le théorème annoncé :

Théorème 3.3. — *Soient k une extension finie de $\mathbb{Q}_p$, et Γ un sous-groupe $\mathbb{Q}_p$-Zariski-dense de $SL(n,k)$. On suppose que tout élément g de Γ est trigonalisable sur k.*
Alors Γ est loxodromique.

On peut remarquer que nous avons besoin d'une hypothèse de trigonalisabilité, qui n'était pas nécessaire dans le cas réel. Nous ne pouvons pas nous en passer sur $\mathbb{Q}_p$: $SL(n,\mathbb{Z}_p)$ est un sous-groupe Zariski-dense non loxodromique de $SL(n,\mathbb{Q}_p)$.

La démonstration du théorème peut se décomposer en deux étapes. Dans un premier temps, nous supposons l'existence d'un sous-groupe Γ qui vérifie les hypothèses du théorème, mais pas la conclusion. Nous arrivons alors à construire un sous-groupe G d'un $SL(d,k)$ qui est compact, $\mathbb{Q}_p$-Zariski-dense, et dont toutes les matrices sont trigonalisables sur k.

Dans un deuxième temps, nous montrons le lemme suivant :

Lemme 3.4. — *Soient $d \geq 2$ un entier, et G un sous-groupe compact, $\mathbb{Q}_p$-Zariski-dense de $SL(d,k)$. Alors, G possède des éléments non trigonalisables sur k.*

Nous utiliserons dans cette preuve la notion de projecteur associé :

Définition 3.5. — Si g est un élément de $GL(n,k)$, on appelle projecteur associé à g, noté π_g, le projecteur sur la somme des espaces caractéristiques de g associés aux valeurs propres de module maximal parallèlement à la somme des autres espaces caractéristiques.

On a alors la propriété suivante :

Propriété 3.6. — *Soit γ un élément de End(k^n). Alors on peut trouver une suite $(c_i)_{i\in\mathbb{N}}$ d'éléments de k telle qu'une extraction de $c_i\gamma^i$ converge vers un projecteur, qui est alors le projecteur π_g associé à γ.*

Démonstration. — On renvoie au lemme 3.8 de [4] pour la preuve de cette propriété. Il faut seulement remarquer que, comme nous sommes dans le cas p-adique, nous n'avons pas besoin de la semisimplicité de g. En effet, si u est unipotent, alors u^{p^m} tend vers Id quand m tend vers $+\infty$. □

3.1.2. Construction d'un groupe compact. — Nous raisonnons donc par l'absurde, et cherchons à construire un sous-groupe compact d'un $SL(d,k)$.
Soit Γ un sous-groupe Zariski-dense de $SL(n,k)$. On remarque tout d'abord que le groupe engendré par Γ et les homothéties de k^n est Zariski-dense dans $GL(n,k)$. Donc, dorénavant, Γ désigne un sous-groupe $\mathbb{Q}_p$-Zariski-dense de $GL(n,k)$ qui contient les homothéties.

On suppose donc que tous les éléments de Γ sont trigonalisables sur k, mais que Γ n'est pas loxodromique. Le fait d'avoir rajouté les homothéties dans le groupe ne change pas ces propriétés.

De plus, on note V l'espace vectoriel k^n.

1. Action sur $\Lambda^{\frac{n(n-1)}{2}}(End(V))$. — Pour tout g dans $GL(n,k)$, on peut définir son action adjointe sur End(V) par $Ad(g)(A) = gAg^{-1}$, puis $\rho(g) = \Lambda^{\frac{n(n-1)}{2}}(Ad(g))$ l'action induite de g sur $V' = \Lambda^{\frac{n(n-1)}{2}}(End(V))$. On remarque alors facilement que g est loxodromique si et seulement si $\rho(g)$ est proximal : En effet si les valeurs propres de g sont notées (répétées avec leur multiplicité) $\lambda_1, \dots, \lambda_n$, avec $|\lambda_1| \geq |\lambda_2| \dots \geq |\lambda_n|$ alors les modules des valeurs propres de $\rho(g)$ sont les produits $\mu_I = \prod_{(i,j)\in I} \frac{|\lambda_i|}{|\lambda_j|}$, où I est un ensemble de $\frac{n(n-1)}{2}$ couples d'entiers inférieurs à n. On voit que μ_I est maximal pour $I = \{(i,j) \ / \ i < j\}$. Enfin aucun autre ensemble n'atteint cette valeur si et seulement si la suite $|\lambda_1| \geq |\lambda_2| \geq \dots \geq |\lambda_n|$ est strictement décroissante.

De plus, si g est trigonalisable sur k, alors $\rho(g)$ l'est aussi.

On note alors, pour $\gamma \in GL(n,k)$, $W(\gamma) \subset V'$ la somme des espaces caractéristiques de $\rho(\gamma)$ pour les valeurs propres de module maximal, et $\mu(\gamma)$ la dimension de $W(\gamma)$. Soit $\mu = \inf \ \{\mu(\gamma) \ \gamma \in \Gamma\}$. On a supposé que Γ n'est pas loxodromique, c'est à dire que $\mu \geq 2$.

Posons $\Gamma_\mu = \{g \in \Gamma \mid \mu(g) = \mu\}$. Cet ensemble est non vide.

2. Restriction de l'action de Γ *à un sous-espace.* — Nous allons maintenant "restreindre" l'action de Γ à un sous-espace de $\Lambda^{\frac{n(n-1)}{2}}(\mathrm{End}(V))$, en vue d'obtenir un sous-groupe de $SL(\mu,k)$.

Soit g dans Γ_μ. Considérons $\pi = \pi_{\rho(g)}$ le projecteur sur $W = W(g)$ parallèlement à la somme des autres espaces caractéristiques.

On définit φ de la façon suivante : si γ est dans Γ, alors on pose $\varphi(\gamma) = \pi\rho(\gamma)\pi$.

Soit K le semigroupe engendré par $\varphi(\Gamma)$. On peut considérer que K est inclus dans $\mathrm{End}(W)$. Alors l'adhérence de Zariski de K contient $\varphi(GL(n,k))$ et donc est $\mathrm{End}(W)$.

Soient G' le semigroupe $K \cap SL(W)$, et G son adhérence topologique.

D'une part si $\gamma \in G$, alors toutes les valeurs propres de γ sont de même module égal à 1. Sinon on pose $\gamma = \varphi(g_1)\dots\varphi(g_r)$, avec $g_1, \dots g_r \in \Gamma$. On sait alors que la dimension ν de la somme des espaces caractéristiques associé aux valeurs propres de module maximal de $\pi\rho(g_1)\pi\rho(g_2)\dots\pi\rho(g_r)\pi$ vérifie $\nu < \mu$. Or il existe des constantes c_n telles que π est une valeur d'adhérence de $c_n\rho(g)^n$, d'après la proposition 3.6.

Donc il existe $n \in \mathbb{N}$ tel que $\mu(g^n g_1 g^n g_2 \dots g^n g_r g^n) = \nu < \mu$, ce qui est absurde car $g^n g_1 g^n \dots g_r g^n$ appartient à Γ.

D'autre part G est Zariski-dense dans $SL(W)$. En effet le sous-semigroupe des matrices de K de déterminant égal à une puissance μ-ième est toujours Zariski-dense dans $GL(W)$, car il est d'indice fini. Or ce sous-semigroupe est égal à $k^* \times G'$. Donc G' est Zariski-dense dans $SL(W)$, et G aussi.

En outre, le lemme suivant nous montre que G est compact, car il agit irréductiblement, étant Zariski-dense :

Lemme 3.7. — *Soit k une extension finie de $\mathbb{Q}_p$, et G un semigroupe de $End(k^d)$ qui agit irréductiblement sur k^d, dont toutes les valeurs propres sont de valeur absolue inférieure à 1. Alors G est relativement compact.*

Démonstration. — Soit A l'algèbre associative engendrée par G. Montrons que la trace, notée Tr, est non dégénérée sur A.

Pour cela on remarque que, comme k^d est un G-module simple, c'est aussi un A-module simple. Donc l'algèbre A est simple, et on sait alors, d'après le lemme de Schur et le théorème de Wedderburn (Cf [23], pp. 643 et 649) que $A=\mathrm{End}_L(k^d)$, où $L=\mathrm{End}_A(k^d)$ est une algèbre à division.

Donc pour tout élément a non nul de A, on trouve un b dans A tel que ab soit un projecteur de rang 1 dans le L-espace vectoriel k^d. Et alors $Tr(ab) = [L, k] \neq 0$. La trace est donc bien non-dégénérée sur A.

Soit alors (h_i) une base de A formée d'éléments de G, (e_i) sa base duale. Soit $g \in K$. Soit $\varphi_g(x) = Tr(gx)$.

On a bien $\varphi_g = \sum Tr(gh_i)e_i$. Or $gh_i \in G$. Or $\mid Tr(gh_i) \mid \leq d$ car toutes les valeurs propres sont inférieures à 1 en module. Donc la norme de la forme linéaire φ_g est bornée par Cd où C est une constante. Donc la norme de φ_g est bornée indépendamment de g. Donc les coefficients de g sont bornés en valeur absolue indépendamment de g.

On a bien montré que G est relativement compact. □

Ici, G étant de plus fermé, il est bien compact.

Ainsi G est un groupe, car c'est un semigroupe compact formé d'éléments inversibles.

Et toutes les matrices de G sont trigonalisables sur k, car les matrices de K sont limites de matrices de Γ, qui sont trigonalisables, donc toutes les matrices de K sont trigonalisables, donc toutes celles de G aussi.

Pour résumer : on a construit un sous-groupe compact $\mathbb{Q}_p$-Zariski-dense de $SL(W)$ dont toutes les matrices sont trigonalisables sur k.

La partie suivante montrera que cette situation est impossible.

3.1.3. Eléments non trigonalisables des sous-groupes compacts de $SL(d, k)$. —

Le but de cette section est de montrer le lemme suivant, qui permet facilement de conclure le raisonnement par l'absurde :

Lemme 3.8. — *Soit G un sous-groupe compact $\mathbb{Q}_p$-Zariski-dense de $SL(d, k)$, avec $d \geq 2$. Alors G contient une matrice non trigonalisable sur k.*

G est un sous-$\mathbb{Q}_p$-groupe de Lie de $SL(d, k)$, car c'est un sous-groupe compact. Soit donc $\mathcal{G}$ son algèbre de Lie (sur $\mathbb{Q}_p$). C'est une sous-algèbre de Lie de $sl(d, k)$, la $\mathbb{Q}_p$-algèbre de

Lie de $SL(d,k)$. Elle est non réduite à 0, sinon G serait discret, donc fini, donc ne serait pas Zariski-dense.

De plus, comme G est $\mathbb{Q}_p$-Zariski-dense dans $SL(d,k)$, $\mathcal{G}$ est un idéal de la $\mathbb{Q}_p$-algèbre $sl(d,k)$. C'est l'objet du lemme suivant :

Lemme 3.9. — *Soit $G \subset G' \subset GL(d,\mathbb{K})$ deux $\mathbb{K}$-groupes de Lie, où $\mathbb{K}$ est un corps local de caractéristique nulle. Soit $\mathcal{G}$ et $\mathcal{G}'$ leur algèbre de Lie respective. Alors si G est Zariski-dense dans G', $\mathcal{G}$ est un idéal de $\mathcal{G}'$*

Démonstration. — On sait que pour tout $h \in G$, Ad_h stabilise $\mathcal{G}$. Or cette propriété s'écrit comme l'annulation de polynômes en les coefficients de h.

On en déduit par Zariski-densité de G, que pour tout $g \in G'$, Ad_g stabilise $\mathcal{G}$. Donc, pour tout $y \in \mathcal{G}'$, on a $ad_y(x) \in \mathcal{G}$.

C'est à dire que $\mathcal{G}$ est un idéal de $\mathcal{G}'$. □

Or d'après [9], paragraphe 6, numéro 10, la $\mathbb{Q}_p$-algèbre de Lie $sl(d,k)$ est simple. Donc $\mathcal{G}$ est tout $sl(d,k)$.

Il suffit maintenant de remarquer que $sl(d,k)$ contient des matrices non trigonalisables sur k. Soit x l'une d'entre elles. Quitte à multiplier x par une puissance de p, on peut supposer qu'elle est de norme strictement inférieure à 1 et que $exp(x)$ est dans G.

Alors $exp(x)$ est une matrice de G qui est non trigonalisable sur k. En effet, ses valeurs propres sont les exponentielles des valeurs propres de x, donc elles vivent dans le même corps.

Le lemme est ainsi démontré.

Ceci conclut la démonstration par l'absurde. On a bien démontré le théorème 3.3.

3.2. Ensembles limites et H-valuation dans $\mathbb{Q}(V)$

Nous disposons d'un outil pour étudier un groupe proximal Γ : les ensembles limites de l'action du groupe sur les espaces $\mathbb{P}(V)$, $\mathbb{Q}(V)$. Ils sont définis comme les plus petits fermés invariants par Γ de ces espaces (voir le lemme 3.10).

Nous introduirons ensuite la notion de H-valuation d'un ensemble de $\mathbb{Q}(V)$.

Cela permettra dans la prochaine partie de comprendre les conditions pour que tout élément g proximal de Γ vérifie $\lambda_1(g) \in H$.

3.2.1. Ensembles limites. — Nous disposons de deux lemmes qui nous assurent l'existence de ces ensembles limites. Pour les énoncer, nous avons besoin de quelques définitions supplémentaires.

Soit Γ un sous-groupe de $GL(V)$. On dit qu'une partie F de V, $\mathbb{P}(V)$, $\mathbb{Q}(V)$... est Γ-invariante si pour tout $\gamma \in \Gamma$, on a $\gamma F \subset F$. On dit que Γ est fortement irréductible s'il n'existe pas de parties F Γ-invariantes de V égales à une réunion finie de sous-espaces vectoriels autres que $\{0\}$ et V.

Si un élément g de $GL(n,k)$ est proximal, on note $x_g^+ \in \mathbb{P}(V)$ la droite propre associée à $\lambda_1(g)$, et $y_g^- \in \mathbb{P}(V^*)$ la droite propre de ${}^tg$ associée à $\lambda_1(g)$. Le noyau de y_g^- est l'unique hyperplan g-invariant supplémentaire à x_g^+. Si g et g^{-1} sont proximaux, on dit que g est biproximal. Dans ce cas, on note $x_g^- = x_{g^{-1}}^+$, $y_g^+ = y_{g^{-1}}^-$, et $a_g^+ = (x_g^+, y_g^+)$. a_g^+ est le point fixe attracteur de g dans $\mathbb{Q}(V)$. De même, on note $a_g^- = a_{g^{-1}}^+ = (x_g^-, y_g^-)$ le point fixe répulseur de g.

Une partie Λ de $\mathbb{P}(V)\times\mathbb{P}(V^*)$ est dite transverse si pour deux éléments distincts (kv_1, V_1) et (kv_2, V_2) - où v_1 et v_2 sont deux vecteurs de V et V_1 et V_2 deux hyperplans de V - v_1 n'appartient pas à V_2. On reviendra sur cette notion dans la partie suivante.

On dispose de plus sur V de la norme max dans une base fixé, que l'on notera $\|.\|$. On peut alors en déduire de manière naturelle une norme sur V^* toujours notée $\|.\|$, et des distances sur $\mathbb{P}(V)$ et $\mathbb{Q}(V)$ que l'on note toutes les deux d. On définit la distance sur $\mathbb{P}(V)$ par la formule suivante :

$$d(x,y) = \inf\{\|u-v\| \text{ tel que } u \in x, v \in y, \|v\| = \|u\| = 1\}$$

On note que pour le choix de la norme fait, cet ensemble est non vide.

On dispose alors du lemme suivant :

Lemme 3.10. — *Soient k un corps local et Γ un sous-groupe irréductible proximal de $SL(n,k)$. Alors d'une part :*

1. *L'ensemble Γ_{prox} des éléments proximaux de Γ est encore Zariski-dense dans Γ*
2. *Soit $\Lambda_\Gamma^{\mathbb{P}}$ l'adhérence de l'ensemble $\{x_g^+ \,/\, g \in \Gamma_{prox}\}$. Tout fermé non vide Γ-invariant de $\mathbb{P}(V)$ contient $\Lambda_\Gamma^{\mathbb{P}}$. Donc l'action de Γ sur $\Lambda_\Gamma^{\mathbb{P}}$ est minimale.*
3. *Pour tous $\varepsilon > 0$, x^+ et x^- dans $\Lambda_\Gamma^{\mathbb{P}}$, l'ensemble*
   $\{g \in \Gamma_{prox} \,/\, d(x_g^+, x^+) < \varepsilon \,,\, d(x_g^-, x^-) < \varepsilon\}$ est encore Zariski-dense dans Γ.
4. *$\Lambda_\Gamma^{\mathbb{P}}$ contient une partie transverse dense.*

Et d'autre part :

1. *L'ensemble Γ_{bip} des éléments biproximaux de Γ est encore Zariski-dense dans Γ*
2. *Soit $\Lambda_\Gamma^{\mathbb{Q}}$ l'adhérence de l'ensemble $\{a_g^+ \,/\, g \in \Gamma_{bip}\}$. Tout fermé non vide Γ-invariant de $\mathbb{Q}(V)$ contient $\Lambda_\Gamma^{\mathbb{Q}}$. Donc l'action de Γ sur $\Lambda_\Gamma^{\mathbb{Q}}$ est minimale.*
3. *Pour tous $\varepsilon > 0$, a^+ et a^- dans $\Lambda_\Gamma^{\mathbb{Q}}$, l'ensemble*
   $\{g \in \Gamma_{bip} \,/\, d(a_g^+, a^+) < \varepsilon \,,\, d(a_g^-, a^-) < \varepsilon\}$ est encore Zariski-dense dans Γ.
4. *$\Lambda_\Gamma^{\mathbb{Q}}$ contient une partie dense et transverse.*

Ces ensembles $\Lambda_\Gamma^{\mathbb{P}}$ et $\Lambda_\Gamma^{\mathbb{Q}}$ sont les ensembles limites de Γ sur respectivement $\mathbb{P}(V)$ et $\mathbb{Q}(V)$. Le deuxième notamment nous sera très utile, une fois que nous aurons défini la notion de H-valuation d'une partie de $\mathbb{Q}(V)$.

Nous énonçons maintenant un lemme similaire traitant des éléments loxodromiques. Remarquons que si un élément g de $SL(n,k)$ est loxodromique, alors son action sur la variété des drapeaux X a un point fixe attracteur. Si g est un élément loxodromique, on note z_g^+ ce drapeau attracteur. z_g^+ est le drapeau engendré par la base $(x_1,\ldots,x_n)$ où x_i est un vecteur propre associé à la valeur propre λ_i. On note z_g^- le drapeau $z_{g^{-1}}^+$.

Lemme 3.11. — *Soit k un corps local et Γ un sous-groupe Zariski-dense qui contient un élément loxodromique de $SL(n,k)$. Alors :*

1. *L'ensemble Γ_{lox} des éléments loxodromiques de Γ est aussi Zariski-dense dans $SL(n,k)$*
2. *Soit Λ_Γ^X l'adhérence de l'ensemble $\{z_g^+ \ / \ g \in \Gamma_{lox}\}$. Tout fermé non vide Γ-invariant de X contient Λ_Γ^X. Donc l'action de Γ sur Λ_Γ^X est minimale.*
3. *Pour tous $\varepsilon > 0$, z^+ et z^- dans Λ_Γ^X, l'ensemble $\{g \in \Gamma_{lox} \ / \ d(z_g^+, z^+) < \varepsilon\,,\ d(z_g^-, z^-) < \varepsilon\}$ est encore Zariski-dense dans Γ.*
4. *Λ_Γ^X contient une partie dense et transverse.*

Démonstration. — Nous renvoyons pour la démonstration de ces deux lemmes à la bibliographie. Plus précisément, le point 1 est démontré dans l'appendice A.5 de [6]. Les autres points sont démontrés dans [3]. □

3.2.2. H-valuation. — Nous introduisons maintenant la notion de H-valuation. Dans le cas de l'article d'Y. Benoist, cette notion -appelée positivité- est reliée aux parties convexes de l'espace projectif. Mais ici nous ne disposons pas de convexité, et donc nous devons nous passer de cette vision des choses.

Soit a un élément de $\mathbb{P}(V)\times\mathbb{P}(V^*)$. On note alors $a = (x_a, y_a)$, et on choisit arbitrairement des vecteurs non nuls v_a et f_a appartenant respectivement à x_a et y_a. On définit η_{ab} comme égal à 0 si $f_a(v_b) = 0$, à la classe de $f_a(v_b)$ dans S sinon ; et $\zeta_{ab} = \eta_{ab}^{d-1}\eta_{ba}$ (on rappelle que d est l'indice de H dans k^*). Ces grandeurs dépendent des choix faits, mais nous n'utiliserons que des produits de ces grandeurs qui eux ne dépendront pas de ces choix.

Soit Λ une partie de $\mathbb{P}(V) \times \mathbb{P}(V^*)$. On voit alors que Λ est transverse si pour tout couple (a,b) d'éléments distincts de Λ, on a $f_a(v_b) \neq 0$. On dit que Λ est H-valuée si on peut choisir pour tout $a \in \Lambda$ les vecteurs v_a et f_a de telle sorte que pour tout couple (a,b) d'éléments de Λ, $f_a(v_b)$ appartient à $H \cup \{0\}$. Enfin, si p est un entier plus grand que 2, on dit que Λ est H-valuée p à p si toute partie à p éléments de Λ est H-valuée. Un triplet de Λ est dit H-antivalué si pour tout choix des f_a et v_a, on peut trouver un couple (a,b) du triplet tel que $f_a(v_b) \notin H$. On dit que Λ est H-antivaluée 3 à 3 si tous les triplets sont H-antivalués.

On appelle valeur d'un triplet (a, b, c) de $\mathbb{Q}(V)$ le produit $\epsilon_{abc} = \zeta_{ab}\zeta_{bc}\zeta_{ca}$. Il ne dépend pas des choix effectués, car S est un groupe fini d'ordre d. On vérifie alors que le triplet (a, b, c) est H-valué (respectivement H-antivalué) si et seulement si $\epsilon_{abc} \in \{0, 1\} \subset S \cup \{0\}$ (respectivement $((S \setminus \{1\}) \cup \{0\})$).

On peut donner un critère de H-valuation :

Lemme 3.12. — *Soit Λ une partie de $\mathbb{P}(V) \times \mathbb{P}(V^*)$ contenant plus de 4 éléments, telle qu'il existe $\Lambda' \subset \Lambda$ dense et transverse. Alors Λ est H-valué si et seulement si pour tout quadruplet (a, b, c, e) de Λ, le produit $\eta_{ac}^{d-1}\eta_{be}^{d-1}\eta_{ae}\eta_{bc}$ vaut 0 ou 1.*

En particulier Λ est H-valué si et seulement si il est H-valué 4 à 4.

Démonstration. — On peut supposer que Λ est transverse.

On voit que le produit considéré $\eta_{ac}^{d-1}\eta_{be}^{d-1}\eta_{ae}\eta_{bc}$ ne dépend pas des choix faits. Donc si Λ est H-valuée, ces produits valent 0 ou 1.

Pour la réciproque, on a par hypothèses que pour tout (a, b, c, e),

$$\eta_{ac}^{d-1}\eta_{be}^{d-1}\eta_{ae}\eta_{bc} = 1$$

Si Λ a quatre éléments a, b, c et e, alors en appliquant l'hypothèse aux quadruplets (a, b, c, e), (c, a, b, e) et (b, c, a, e) puis en faisant le produit des égalités obtenues, on obtient : $\eta_{ac}^{d-1}\eta_{ca}\eta_{ba}^{d-1}\eta_{ab}\eta_{cb}^{d-1}\eta_{bc} = 1$.

Donc si on choisit v_a arbitrairement, on peut faire les choix de f_a, v_b, f_b, v_c et f_c tels que on a : $\eta_{ac} = \eta_{ca} = \eta_{ba} = \eta_{ab} = \eta_{cb} = \eta_{bc} = 1$. On peut choisir de plus v_e et f_e tels que on a $\eta_{ae} = \eta_{ea} = 1$. Les égalités données par l'hypothèse assurent alors que $\eta_{ec} = \eta_{ce} = \eta_{be} = \eta_{eb} = 1$. Il suffit enfin d'appliquer l'hypothèse aux quadruplets du type (a, b, a, c) pour montrer que $\eta_{aa} = \eta_{bb} = \eta_{cc} = \eta_{ee} = 1$. Donc Λ est bien H-valuée.

Si maintenant Λ a plus de quatre éléments, on commence par choisir un a arbitrairement, et on fixe v_a. On peut alors faire des choix pour toute partie de Λ à quatre éléments contenant a. On vérifie alors que tous ces choix sont cohérents en regardant des parties qui ont trois éléments en commun. On en déduit que Λ est H-valué. □

3.2.3. H-valuation 3 à 3.

— La H-valuation 3 à 3 joue un rôle particulièrement important. On peut donner un critère de H-valuation 3 à 3 :

Lemme 3.13. — *Soit Λ une partie de $\mathbb{Q}(V)$ qui contient une partie Λ' dense et transverse. Alors Λ est H-valuée 3 à 3 si et seulement si on peut faire le choix des vecteurs v_a et f_a tels que pour tout couple (a, b) de points de Λ, on a $\zeta_{ab} \in \{0, 1\}$.*

Démonstration. — On peut à nouveau supposer Λ transverse.

Si on peut faire les choix comme dans l'énoncé du lemme, alors pour tout triplet (a, b, c) d'éléments de Λ, on a $\epsilon_{abc} = 1$. Donc Λ est H-valuée 3 à 3.

Réciproquement, si Λ est H-valuée 3 à 3, alors pour tout triplet (a, b, c) d'éléments de Λ, on a $\epsilon_{abc} = 1$. On fixe un a dans Λ et on choisit v_a ainsi que tous les f_b arbitrairement.

On choisit alors les vecteurs v_b tels que si $b \neq a$, alors $\zeta_{ab} = 1$. En utilisant l'hypothèse, on voit que si b et c sont deux éléments distincts de Λ, alors $\zeta_{bc} = 1$. □

3.3. Action sur la H-sphère et H-proximalité

L'étude de l'action d'un élément proximal g de $GL(n,k)$ sur l'espace projectif ne suffit pas pour décider si sa valeur propre $\lambda_1(g)$ est dans H.

Pour cela il faut regarder un espace plus gros qu'on appelle la H-sphère. On définit cette H-sphère, notée $\mathbb{S}(V)$ comme l'ensemble $(V \setminus \{0\})/H$. C'est un revêtement à d feuillets de $\mathbb{P}(V)$. On peut définir une distance sur $\mathbb{S}(V)$ à valeur dans $\mathbb{R}$ de la façon suivante :

Soit $|H|$ l'ensemble des normes d'éléments de H. Soient $x \in u$ et $y \in v$.

On pose $D(u,v) =$

- 3 si $\frac{\|x\|}{\|y\|}$ n'est pas dans $|H|$ (ça ne dépend pas du choix de x et y).
- $\frac{1}{\|x\|}\inf\{\|x - y'\|$ pour $y' \in v,$ avec $\|y'\| = \|x\|\}$, sinon. A nouveau cela ne dépend pas du choix de x et de y, et on voit que dans ce cas $D(u,v) \leq 1$.

Grâce à cette distance on peut construire des relevés de boules de l'espace projectif sur $\mathbb{S}(V)$ de la façon suivante : si x appartient à $\mathbb{P}(V)$, et que $u \in \mathbb{S}(V)$ se projette sur x, alors la boule de centre u et de rayon ε de $\mathbb{S}(V)$ se projette bijectivement sur la boule de centre x et de rayon ε (pour $\varepsilon < 1$).

3.3.1. Lien entre l'action sur la H-sphère et proximalité. — Définissons tout d'abord la notion de H-proximalité :

Un élément g de $SL(n,k)$ est H-proximal (resp. H-biproximal, resp. H-loxodromique) s'il est proximal (resp. biproximal, loxodromique) et que $\lambda_1(g)$ est dans H (resp. $\{\lambda_1(g), \lambda_n(g)\}$ est dans H, resp. toutes les valeurs propres sont dans H).

On dit de même qu'un sous-groupe Γ de $SL(n,k)$ est H-proximal (resp. H-loxodromique) s'il est proximal (resp. loxodromique) et que tout élément proximal (resp. loxodromique) est H-proximal (resp. H-loxodromique).

On a vu qu'un élément de $SL(n,k)$ est proximal si et seulement si son action sur l'espace projectif a un point fixe attracteur. On remarque de même que cet élément est H-proximal si et seulement s'il a un point fixe attracteur dans $\mathbb{S}(V)$. Il en a alors exactement d.

On peut alors continuer cette analyse et étudier l'action des groupes H-proximaux sur la H-sphère. Soit Γ un sous-groupe Zariski-dense de $SL(n,k)$. On appelle $\Lambda_\Gamma^{\mathbb{S}}$ le relevé sur la H-sphère de l'ensemble $\Lambda_\Gamma^{\mathbb{P}}$

On obtient alors la propriété suivante :

Propriété 3.14. — *Soit Γ un sous-groupe Zariski-dense de $SL(n,k)$. Alors Γ est H-proximal si et seulement si il existe un fermé Γ-invariant F de $\Lambda_\Gamma^{\mathbb{S}}$ tel que $\Lambda_\Gamma^{\mathbb{S}}$ est l'union disjointe des ensembles $(\alpha F)_{\alpha \in S}$.*

Dans ce cas l'action de Γ *sur* F *est minimale.*

Démonstration. — Supposons qu'on a ce fermé F et cette décomposition de $\Lambda_\Gamma^{\mathbb{S}}$. Soit alors g un élément proximal de Γ. On sait que x_g^+ appartient à $\Lambda_\Gamma^{\mathbb{P}}$. Soit α la classe de la valeur propre $\lambda_1(g)$ dans S. Soit $x^+ \in F$ un relevé de x_g^+. Alors on a par hypothèse $g(x^+) = \alpha x^+ \in F$. Donc $\alpha = 1$ et g est H-proximal.

Réciproquement, supposons que Γ est H-proximal. Soit F un fermé minimal de $\Lambda_\Gamma^{\mathbb{S}}$ pour l'action de Γ. On sait que l'action de Γ sur $\Lambda_\Gamma^{\mathbb{P}}$ est minimale, donc F se projette sur $\Lambda_\Gamma^{\mathbb{P}}$. Donc on sait que $\Lambda_\Gamma^{\mathbb{S}}$ est l'union des $(\alpha F)_{\alpha \in S}$. Il reste à montrer que cette union est disjointe.

Soit donc $\alpha \in S$ tel que $\alpha F \cap F \neq \emptyset$. Alors par minimalité, on obtient $\alpha F = F$. Soit g un élément proximal de Γ, et $x^+ \in F$ un relevé de x_g^+. L'orbite sous Γ de x^+ est dense dans F, donc il existe $h \in \Gamma$ tel que $h(x^+)$ est très proche de αx^+. Alors pour n grand, $h_n = g^n h g^n$ est proximal, donc H-proximal. Or $x_{h_n}^+$ est très proche de x_g^+. Soit donc y^+ proche de x^+ un relevé de $x_{h_n}^+$. Alors $h_n(y^+)$ est très proche de αx^+. Donc, comme H est ouvert, $\lambda_1(h_n)$ a pour classe α dans S. Donc $\alpha = 1$, et l'union est bien disjointe.

D'autre part, on voit que dans ces conditions l'action de Γ sur F est bien minimale. □

3.3.2. Sous-groupes H-proximaux. — La question de l'existence de sous-groupes H-proximaux est un premier pas vers la démonstration du théorème 3.1. Nous avons alors le théorème suivant :

Théorème 3.15. — *Soit* k *un corps local et* H *un sous-groupe ouvert d'indice fini de* k^**. Alors les trois propositions suivantes sont équivalentes :*

1. $SL(n,k)$ *admet un sous-groupe Zariski dense dont tous les éléments sont* H*-proximaux.*
2. $SL(n,k)$ *admet un sous-groupe Zariski dense et* H*-proximal.*
3. -1 *appartient à* H *ou* n *est différent de 2.*

Nous allons tout d'abord énoncer un autre résultat, qui nous permettra de montrer le théorème.

Proposition 3.16. — *Considérons* Γ *un sous-groupe proximal fortement irréductible de* $SL(n,k)$*. Alors les cinq conditions suivantes sont équivalentes :*

1. Γ *contient un sous-groupe Zariski-dense dont tous les éléments sont* H*-proximaux.*
2. Γ *contient un sous-groupe Zariski-dense et* H*-proximal.*
3. Γ *contient un sous-groupe Zariski-dense* Δ *tel que* $\Lambda_\Delta^{\mathbb{Q}(V)}$ *est* H*-valué.*
4. $\Lambda_\Gamma^{\mathbb{Q}(V)}$ *n'est pas* H*-antivalué trois à trois.*
5. $\Lambda_\Gamma^{\mathbb{Q}(V)}$ *contient une partie infinie transverse* H*-valuée.*

Montrons dans un premier temps que cette proposition implique le théorème.

Démonstration. — L'équivalence entre le premier et le deuxième point du théorème est dans la proposition. Il reste donc à prouve que $SL(n,k)$ contient des sous-groupes Zariski-denses et H-proximaux si et seulement si n est différent de 2 ou bien -1 est dans H.

Commençons par un lemme qui permet de comprendre pourquoi la condition est nécessaire

Lemme 3.17. — *Soit* Γ *un sous-groupe proximal fortement irréductible de* $SL(n,k)$ *préservant une forme bilinéaire* b*. Alors on a l'alternative suivante :*

- *si* b *est symétrique, alors* $\Lambda_\Gamma^{\mathbb{Q}(V)}$ *est* H*-valué.*
- *si* b *est antisymétrique, alors si* -1 *n'appartient pas à* H*,* $\Lambda_\Gamma^{\mathbb{Q}(V)}$ *est* H*-antivalué 3 à 3.*

Démonstration. — Soit b la forme bilinéaire préservée. Notons alors $K = \{g \in SL(n,k) \,/\, \forall v,\, w \;:\; b(gv, gw) = b(v,w)\}$. On peut supposer $\Gamma = K$. Alors l'ensemble $\Lambda_\Gamma^{\mathbb{Q}(V)}$ est l'orbite fermée de K dans $\mathbb{Q}(V)$. Or cette orbite est définie comme suit : pour tout $v \in V$, on note v^* la forme linéaire $v' \mapsto b(v,v')$. Alors $\Lambda_H^{\mathbb{Q}} = \{(v, v^*) \;:\; / \, v \in V\}$ s'identifie à l'ensemble des droites isotropes.

On choisit donc pour tout a dans $\Lambda_\Gamma^{\mathbb{Q}(V)}$ un vecteur v_a arbitraire, et on pose $f_a = b(v_a, .)$.

Alors, dans le premier cas, pour tout couple (a,b), on a $\zeta_{ab} = 1$. Donc pour tout triplet (a,b,c), $\epsilon_{abc} = 1$ ou 0 et $\Lambda_\Gamma^{\mathbb{Q}(V)}$ est H-valué.

Et, dans le deuxième cas, pour tout couple (a,b), on a $\zeta_{ab} = -1$. Donc pour tout triplet (a,b,c), $\epsilon_{abc} = -1$ ou 0. Donc, si -1 n'est pas élément de H, $\Lambda_\Gamma^{\mathbb{Q}(V)}$ est H-antivalué. □

Montrons maintenant le théorème. Nous distinguons le cas de la dimension 2.

Cas 1 : n=2

En dimension 2, $SL(2,k)$ préserve une forme bilinéaire symplectique. Donc pour $n = 2$, il faut que -1 appartienne à H. Auquel cas, vu les choix que l'on peut faire, $\Lambda_\Gamma^{\mathbb{Q}(V)}$ est H-valué et donc on vérifie les conditions de la proposition 3.16.

Cas 2 : $n \geq 3$

Il suffit maintenant de construire un triplet H-valué pour $SL(n,k)$. En effet, $\Lambda_\Gamma^{\mathbb{Q}(V)}$ n'est alors pas H-antivaluée trois à trois, et la proposition 3.16 implique que Γ admet un sous-groupe Zariski-dense proximal.

Soit donc $(e_1, e_2, \ldots, e_n)$ une base de k^n. Soit a un élément de H de norme plus grande strictement que 1.

Soit $g \in SL(n,k)$ dont la matrice dans cette base est :

$$\begin{pmatrix} a & & & & \\ & 1 & & 0 & \\ & & \ddots & & \\ & 0 & & 1 & \\ & & & & a^{-1} \end{pmatrix}$$

Soit maintenant $h \in SL(n,k)$ qui est représenté par la même matrice mais cette fois dans la base $(e_1 + 2e_2 + e_n, e_1 - e_n, \ldots, e_n)$.

Alors un calcul rapide montre que le triplet (a_g^+, a_g^-, a_h^+) est H-valué. Il suffit en effet de faire les choix suivants pour les représentants de a_g^+, a_g^- et a_h^+ :

- $a_g^+ = [(e_1, e_n^*)]$
- $a_g^- = [(e_n, e_1^*)]$
- $a_h^+ = [(e_1 + 2e_2 + e_n, e_1^* + e_n^* - e_2^*)]$

On a bien montré le théorème 3.15 grâce à la proposition 3.16. □

3.3.3. Démonstration de la proposition 3.16. — Il faut donc maintenant démontrer la proposition 3.16. Nous aurons besoin pour cela de trois lemmes.

Voyons tout d'abord comment construire une partie infinie H-valuée de l'ensemble limite dans $\mathbb{Q}(V)$ à partir d'un triplet H-valué :

Lemme 3.18. — *Soient g un élément biproximal de $GL(k^n)$ et a appartenant à $\mathbb{Q}(V)$ tels que le triplet (a, a_g^+, a_g^-) soit transverse et H-valué. Alors il existe un entier $i > 1$ tel que l'ensemble $\{g^{im}.a \,/\, m \in \mathbb{Z}\}$ est transverse et H-valué.*

Démonstration. — On suppose - quitte à remplacer g par g^d - que g et g^{-1} sont H-proximaux.

On fait les choix des vecteurs v, f, $v_g^\pm$ et $f_g^\pm$ de telle sorte que pour tout couple (b,c) du triplet (a, a_g^+, a_g^-), on a $\eta_{bc} = f_b(v_c) = 1 \in G$. C'est possible car le triplet est transverse et H-valué.

Notons $v_m = g^m v$ et $f_m = g^m f$. Travaillons dans la H-sphère $\mathbb{S}(V)$ et pour x dans V notons $\tilde{x}$ sa projection dans $\mathbb{S}$. Alors, comme $f_g^-(v) = f_g^-(v_g^+)$, on sait que $\tilde{v}_n$ tend vers $\tilde{v}_g^+$ quand $n \to +\infty$. En effet $\tilde{v}_n$ tend vers $\alpha\tilde{v}_g^+$ pour un $\alpha \in S$, et la condition impose $\alpha = 1$. De même, $\tilde{v}_n$ tend vers $\tilde{v}_g^-$ quand $n \to -\infty$. L'ouverture de H nous garantit alors l'existence de i_0 tel que pour tout entier i avec $|i| \geq i_0$, $f(v_i) \in H$. Mais alors si i et j sont deux entiers tels que $|i - j| \geq i_0$, on a $f_j(v_i) \in H$. Donc la famille $\{g^{i_0 m}.a \,/\, m \in \mathbb{Z}\}$ est transverse et H-valuée. □

Il faut maintenant arriver à construire des sous-groupes Zariski-dense. C'est l'objet du second lemme.

Lemme 3.19. — *Soit Γ un sous-groupe fortement irréductible et proximal de $SL(n,k)$. Soient $m \geq 2$ et $a_1^\pm$, $a_2^\pm$, …, $a_m^\pm$ des éléments de $\Lambda_\Gamma^{\mathbb{Q}}$. Alors pour tout $\epsilon > 0$, on peut trouver des éléments g_1, …, g_m de Γ tels que :*

- *Pour tout $1 \leq i \leq m$, g_i est H-biproximal.*
- *Pour tout $1 \leq i \leq m$, $d(a_{g_i}^+, a_i^+) < \epsilon$ et $d(a_{g_i}^-, a_i^-) < \epsilon$.*
- *Pour tout $p \geq 1$, le sous-groupe Δ_p de Γ engendré par $(g_i^p)_{1 \leq i \leq m}$ est Zariski-dense dans Γ.*

Démonstration. — Nous renvoyons au lemme 7.2 de [2]. En effet, $SL(n,k)$ est un $\mathbb{Q}_p$-groupe semisimple. Il faut cependant prendre la précaution de remplacer dans cette preuve les g_j par g_j^d pour assurer qu'ils sont H-proximaux. □

Un dernier lemme permettra de vérifier que les groupes construits dans le lemme précédent sont composés d'éléments H-proximaux.

Lemme 3.20. — *Soit E une partie finie de $GL(V)$ formée d'éléments H-biproximaux et telle que l'inverse de tout élément de E est encore dans E. Supposons que l'ensemble $\Lambda_E^{\mathbb{Q}} = \{a_g^+ \,/\, g \in E\}$ de $\mathbb{Q}(V)$ est transverse. De plus, on suppose que pour tout $i \geq 1$ le sous groupe Δ_i de $GL(V)$ engendré par $\{g^i \,/\, g \in E\}$ agit irréductiblement sur V. Alors on peut trouver un entier $i_0 \geq 1$ tel que, pour tout $i \geq i_0$, on a :*
- *Tous les éléments de $\Delta_i - \{e\}$ sont proximaux.*
- *Δ_i est H-proximal si et seulement si $\Lambda_E^{\mathbb{Q}}$ est H-valué.*
- *$\Lambda_{\Delta_i}^{\mathbb{Q}}$ est H-valué si et seulement si $\Lambda_E^{\mathbb{Q}}$ est H-valué.*

Démonstration. — Soit ϵ un réel positif. Soit g un élément proximal, on dispose alors de x_g^+ et y_g^-, et on note Y_g^- le noyau de y_g^-. On définit alors $b_\epsilon(g) = \{x \in \mathbb{P}(V) \,/\, d(x, x_g^+) < \epsilon\}$ et $B_\epsilon(g) = \{x \in \mathbb{P}(V) \,/\, d(x, Y_g^-) > \epsilon\}$.

On dit alors que g est ϵ-proximal si on a : $b_\epsilon(g) \subset B_\epsilon(g)$, $g(B_\epsilon(g)) \subset b_\epsilon(g)$ et l'action de g restreinte à $B_\epsilon(g)$ est ϵ-lipschitzienne.

Fixons ϵ suffisamment petit tel que, pour tout g et h distincts de E avec $g \neq h^{-1}$, on a $b_\epsilon(h) \subset B_\epsilon(g)$. On peut trouver un entier i_0 tel que tous les g^{i_0} pour g un élément de E sont ϵ-proximaux. On note $E^i = \{g^i \,/\, g \in E\}$ pour tout entier i.

Soit $i \geq i_0$. Soit $h = h_l \dots h_1$ un élément de Δ_i, avec h_k dans E^i. On suppose (quitte à simplifier et à conjuguer) que pour tout $1 \leq k \leq l$, $h_k \neq h_{k+1}^{-1}$, avec la notation $h_1 = h_{l+1}$. Comme les h_k sont dans E^i, ils sont ϵ-proximaux.

Dans ces conditions, on vérifie que pour tout $1 \leq k \leq l$, on a les inclusions suivantes : $h_k \dots h_1(b_\epsilon(h_l)) \subset h_k \dots h_1(B_\epsilon(h_1)) \subset b_\epsilon(h_k)$. Donc on obtient que $h(b_\epsilon(h_l)) \subset b_\epsilon(h_l)$ et on voit que la restriction de h à $b_\epsilon(h_l)$ est ϵ-lipschitzienne. Donc h admet un point fixe attracteur dans $b_\epsilon(h_l)$ et est donc proximal.

Le premier point est donc démontré.

Pour le deuxième point, il va falloir à nouveau travailler dans la H-sphère. Pour tout g dans E, choisissons v_g^+ et f_g^- des relevés de x_g^+ et y_g^- dans respectivement V et V^* tels que $f_g^-(v_g^+) \in H$. Si x appartient à V, on note $\tilde{x}$ son projeté dans la H-sphère. Soit $a_\epsilon(g) = \{v \in \mathbb{S}(V) \,/\, D(v, \tilde{v}_g^+) < \epsilon\}$. Il est clair par construction que $a_\epsilon(g)$ se projette sur $b_\epsilon(g)$. Donc pour tout h et h' distincts de E^i avec $h' \neq h^{-1}$, on peut définir $\eta_{hh'}$ comme l'unique élément de S tel que on a $h(a_\epsilon(h')) \subset \eta_{hh'} a_\epsilon(h)$. On voit que $\eta_{hh'}$ est la classe de $f_h^-(v_{h'}^+)$.

Si maintenant, comme pour le point précédent, on a un mot $h = h_l \dots h_1$ réduit avec h_k dans E^i, on définit $\eta_h = \eta_{h_1 h_l} \dots \eta_{h_2 h_1}$. On a alors $h(a_\epsilon(h_l)) \subset \eta_h a_\epsilon(h_l)$.

Donc Δ_i est H-proximal si et seulement si on a $\forall h \in \Delta_i \setminus \{e\}$, $\eta_h = 1$. D'après le lemme 3.12, on voit que c'est équivalent au fait que $\Lambda_E^{\mathbb{Q}}$ est H-valué.

Pour le troisième point, on remarque tout d'abord que $\Lambda_E^{\mathbb{Q}}$ est inclus dans $\Lambda_{\Delta_i}^{\mathbb{Q}}$. Il suffit donc de montrer que si $\Lambda_E^{\mathbb{Q}}$ est H-valué, alors $\Lambda_{\Delta_i}^{\mathbb{Q}}$ l'est aussi. Raisonnons par l'absurde. Si $\Lambda_E^{\mathbb{Q}}$ est H-valué, Δ_i est H-proximal. Mais si $\Lambda_{\Delta_p}^{\mathbb{Q}}$ n'est pas H-valué, on peut construire grâce aux deux premiers points de ce lemme et au lemme précédent un élément proximal non H-proximal de $\Delta_i \setminus \{e\}$. C'est la contradiction cherchée.

□

Nous pouvons maintenant démontrer l'équivalence de la proposition 3.16 :

Démonstration. — Le premier point implique clairement le second.

Avec le lemme 3.20 et sa démonstration, on voit que le deuxième point implique le troisième.

Du troisième point on en déduit facilement le quatrième : on dispose d'une partie infinie H-valuée, donc a fortiori un triplet.

Pour passer du quatrième point au cinquième, on utilise le lemme 3.18 : soit (a, a^+, a^-) un triplet transverse H-valué. D'après le lemme 3.10 on trouve un élément biproximal g tel que a_g^+ est très proche de a^+ et a_g^- de a^-. Donc on dispose du triplet (a, a_g^+, a_g^-) transverse et H-valué. Ce qui permet d'appliquer le lemme 3.18 pour avoir une partie infinie transverse H-valuée.

Enfin le cinquième implique le premier point : Soit une famille $a_1^\pm$, …, $a_m^\pm$ transverse H-valuée. On choisit un $\epsilon > 0$ suffisamment petit et g_1, …, g_m comme dans le lemme 3.19 de sorte que la famille $a_{g_1}^\pm$, …, $a_{g_m}^\pm$ est encore transverse et H-valuée. Soit Δ_i le groupe engendré par les g_j^i. D'après les lemmes 3.19 et 3.20, pour i suffisamment grand, Δ_i est Zariski-dense composé d'éléments H-proximaux. □

Nous avons donc compris le comportement de la première valeur propre. Avec le même genre d'idée, on peut traiter toutes les valeurs propres simultanément. Ainsi dans la prochaine partie, nous étudierons les conditions d'existence de sous-groupes H-loxodromiques de $SL(n, k)$.

3.4. Sous-groupes H-loxodromiques

3.4.1. La variété des drapeaux. — Le but de cette partie est de démontrer le théorème suivant :

Théorème 3.21. — *Soit k un corps local, H un sous-groupe ouvert d'indice fini de k^*.*

Alors les trois propositions suivantes sont équivalentes :

1. $SL(n,k)$ *contient un sous-groupe Zariski dense et dont tous les éléments sont H-loxodromiques.*
2. $SL(n,k)$ *contient un sous-groupe H-loxodromique et Zariski-dense.*
3. -1 *appartient à H, ou n n'est pas congru à 2 modulo 4.*

La démonstration sera parallèle à la démonstration du théorème 3.15. Il faudra cependant être un peu plus précis car nous travaillons maintenant avec toutes les valeurs propres simultanément. Il faudra pour cela utiliser un soupçon de théorie des représentations.

Pour le groupe $SL(n,k)$ on connait des représentations r_l dans $V_l = \Lambda^l k^n$ pour $1 \leq k \leq n-1$. On a vu que si un Γ est H-loxodromique, alors tous les $r_l(\Gamma)$ sont H-proximaux. On fixe une base $(e_1, \dots e_n)$ de V

Nous travaillons dans la variété des drapeaux $X \simeq SL(n,k)/T^+$ de V où T^+ est l'ensemble des matrices triangulaires supérieures. Il nous faut donc définir la notion de H-valuation pour une partie Λ de X.

Pour cela, définissons des fonctions φ_l de X dans $\mathbb{Q}(V_l)$ pour tout $1 \leq l \leq n-1$: soit $z = (E_0 = \{0\}, \dots, E_n = V)$ un drapeau de X. Alors on pose $\varphi_l(z)$ égal au point de V_l représentant l'espace vectoriel E_l.

De plus, pour tout $1 \leq l \leq n-1$, on note a_l l'image par φ_l du drapeau canonique.

On peut alors définir la notion de H-valuation dans la variété des drapeaux :

Définition 3.22. — Une partie Λ de X est H-valuée (resp H-valuée 3 à 3) si et seulement si, pour tout $1 \leq l \leq n-1$, son image $\varphi_l(\Lambda)$ dans $\mathbb{Q}(V_l)$ est H-valuée (resp H-valuée 3 à 3).

Une telle partie est H-antivaluée 3 à 3 si elle ne contient aucun triplet transverse H-valué.

On peut alors énoncer une proposition similaire à la proposition 3.16 :

Proposition 3.23. — *Considérons Γ un sous-groupe Zariski-dense et loxodromique de $SL(n,k)$. Alors on a l'équivalence suivante :*

1. Γ *contient un sous-groupe Zariski-dense dont tous les éléments sont H-loxodromiques.*
2. Γ *contient un sous-groupe Zariski-dense et H-loxodromique.*
3. *l'ensemble limite Λ_Γ^X contient un triplet transverse H-valué.*

La prochaine partie est consacrée à la démonstration de cette proposition.

3.4.2. H-valuation de l'ensemble limite. — La démonstration de la proposition 3.23 est très similaire à celle de la proposition 3.16. Nous énonçons donc trois lemmes analogues aux trois lemmes utilisés plus haut.

Lemme 3.24. — *Soient g un élément biproximal de $SL(k^n)$ et z appartenant à X tels que le triplet (z, z_g^+, z_g^-) soit H-valué. Alors il existe un entier $p > 1$ tel que l'ensemble $\{g^{pn}.z \,/\, n \in \mathbb{Z}\}$ est transverse et H-valué.*

Démonstration. — C'est une conséquence du lemme 3.18. □

Lemme 3.25. — *Soit Γ un sous-groupe Zariski-dense loxodromique de $SL(k^n)$. Soient $m \geq 2$ et $z_1^\pm$, $z_2^\pm$, …, $z_m^\pm$ des éléments de Λ_Γ^X. Alors pour tout $\epsilon > 0$, on peut trouver des éléments g_1, …, g_m de Γ tels que :*
- *Pour tout $1 \leq j \leq m$, g_j est H-loxodromique.*
- *Pour tout $1 \leq j \leq m$, $d(z_{g_j}^+, z_j^+) < \epsilon$ et $d(z_{g_j}^-, z_j^-) < \epsilon$.*
- *Pour tout $i \geq 1$, le sous-groupe Δ_i de Γ engendré par $(g_j^i)_{1 \leq j \leq m}$ est Zariski-dense dans Γ.*

Démonstration. — Nous renvoyons à nouveau au lemme 7.2 de [2]. □

Le troisième lemme se réénonce ainsi :

Lemme 3.26. — *Soit E une partie finie de $SL(V)$ formée d'éléments H-loxodromiques et telle que l'inverse de tout élément de E est encore dans E. Supposons que l'ensemble $\Lambda_E^X = \{z_g^+ \,/\, g \in E\}$ de X est transverse. De plus, on suppose que pour tout $i \geq 1$ le sous groupe Δ_i de $SL(V)$ engendré par $\{g^i \,/\, g \in E\}$ est Zariski-dense dans $SL(V)$. Alors on peut trouver un entier $i_0 \geq 1$ tel que, pour tout $i \geq i_0$, on a :*
- *Tous les éléments $\Delta_i - \{e\}$ sont loxodromiques.*
- *Δ_i est H-loxodromique si et seulement si Λ_E^X est H-valué.*

Démonstration. — C'est une conséquence du lemme 3.20. □

On montre alors la proposition 3.23 de la même manière que la proposition 3.16, en remplaçant les lemmes 3.18, 3.19 et 3.20 par les trois lemmes ci-dessus.

Il reste donc à démontrer le théorème 3.21. Pour cela, le point un peu délicat est de construire un triplet H-valué. Nous détaillons cette construction dans la partie suivante.

3.4.3. Construction d'un triplet H-valué. — Le but de cette partie est de construire un triplet H-valué de la variété des drapeaux. Quand on ne s'intéressait qu'à la première valeur propre, cette construction n'était qu'une formalité. Maintenant, il faut contrôler la H-valuation du triplet dans toutes les représentations simultanément. Pour cela, nous utilisons l'action d'un certain élément Y de $M(n, k)$.

Commençons par une définition et un lemme. On rappelle qu'on dispose de $(e_1, \ldots, e_n)$ une base de V.

Définition 3.27. — Soient Y appartenant à $GL(n, k)$ et $1 \leq l \leq n-1$. Alors on note $N_l(Y) = \inf\{k \in \mathbb{N} \,/\, f_l(Y^k.v_l) \neq 0\}$, où $v_l = e_1 \wedge \ldots \wedge e_l$ appartient à V_l et $f_l = (e_{n-l+1} \wedge \ldots \wedge e_n)^*$ appartient au dual V_l^* de V_l.

On remarque que v_l et f_l sont des vecteurs de plus haut poids restreint de V_l et V_l^* respectivement.

Le lemme suivant explique comment utiliser l'action d'un élément Y nilpotent bien choisi. Comme Yest supposé nilpotent, on peut passer à l'exponentielle.

Lemme 3.28. — *Soient Y dans $M(n,k)$ et $1 \leq l \leq n-1$. Alors on peut trouver t et t' dans H tels que pour tout l :*

1. *Si $N_l(Y) < \infty$, le triplet $(a_l, e^{tY}.a_l, e^{t'Y}.a_l)$ est transverse.*
2. *Si $N_l(Y)$ est pair, il est H-valué.*
3. *Si $N_l(Y)$ est impair, le triplet et H-valué si et seulement si -1 est dans H*

Démonstration. — Soit t_i une suite de points de H tendant vers 0. Soit maintenant t'_i une suite de points de H tels que pour tout i, $t'_i - t_i$ est élément de H (en particulier $t_i \neq t'_i$). C'est possible car H est ouvert.

Fixons un entier $1 \leq l \leq n-1$.

Soit $N = N_l(Y)$. Soit (v_l, f_l) un représentant de a_l. Calculons pour tout i :

$$\begin{aligned} c_{t_i t'_i} &= (e^{t_i Y} f_l)(e^{t'_i Y} v_l) \\ &= f_l(e^{(t'_i - t_i)Y} v_l) \\ &= \tfrac{(t'_i - t_i)^N}{N!} f_l(Y^N v_l) + o((t'_i - t_i)^N) \end{aligned}$$

Cette expression ne s'annule pour i grand car on a supposé que $t_i \neq t'_i$. Donc tous les triplets $(a_l, e^{t_i Y}.a_l, e^{t'_i Y}.a_l)$ sont transverses.

On peut supposer v_l et f_l choisis de telle sorte que $\frac{f_l(Y^N v_l)}{N!} \in H$. On sait alors que pour i suffisamment grand $c_{t_i t'_i}$, c_{0t} et $c_{0t'}$ sont dans H car H est ouvert. Il suffit donc de vérifier que $c_{t_i 0}$, $c_{t'_i 0}$ et $c_{t't}$ sont dans H. C'est bien le cas si N est pair, ou alors, si N est impair, il faut et il suffit que -1 soit dans H.

Donc pour un certain I, on sait que le triplet $(a_l, e^{t_I Y}.a_l, e^{t'_I Y}.a_l)$ vérifie les conditions du lemme. □

Dans le cas où n n'est pas congru à 2 modulo 4, nous construisons maintenant un élément Y de $M(n,k)$ tel que $N_l(Y)$ soit pair pour tout $1 \leq l \leq n-1$.

Cas n1 : n est impair

Posons $Y_0 \in M(n,k)$ défini par : $Y_0 e_i = e_{i+1}$ pour tout $1 \leq i \leq n$, avec $e_{n+1} = 0$. On peut alors calculer $N_l(Y_0)$ pour tout l : on a $N_l(Y_0) = l(n-l)$. Comme n est impair, cet entier est pair pour tout $1 \leq l \leq n-1$.

Cas n2 : $n = 2q$ avec q pair

On définit cette fois Y_1 par $Y_1 e_i = e_{i+1} + \delta_{i,q-1} e_{q+1}$ pour tout $1 \leq i \leq n$. On peut calculer, pour $1 \leq l < q$, $N_l(Y_1) = N_{n-l}(Y_1) = l(n-l-1)$. Ces entiers sont pairs.

Il reste le problème de la parité de $N_q(Y_1)$. Montrons dans un premier temps que cet entier est fini : il suffit de constater que $f_q(Y_1^{q^2}.e_1 \wedge \ldots \wedge e_q) \neq 0$. Donc $N_q(Y_1)$ est bien fini.

On remarque alors que la représentation r_q est orthogonale. C'est à dire que, d'après le lemme 3.17, la famille $(a_q, e^{t_I Y}.a_q, e^{t'_I Y}.a_q)$ est H-valuée, et ce pour tout H sous-groupe d'indice fini de k^*. Or il y a des tels H qui ne contiennent pas -1. Donc, d'après le lemme 3.28, $N_q(Y_1)$ ne peut pas être impair. Comme il est fini, c'est donc qu'il est pair.

Tous les $N_l(Y_1)$ sont donc pairs pour $1 \leq l \leq n-1$.

Grâce à ces éléments Y_0 et Y_1, nous pouvons maintenant démontrer le théorème 3.21.

Preuve du théorème 3.21. — L'équivalence entre le premier point et le deuxième est déjà prouvée dans la proposition. Il reste à montrer que $SL(n,k)$ contient un sous-groupe Zariski-dense et H-loxodromique si et seulement si -1 est dans H ou n n'est pas congru à 2 modulo 4

Or on remarque que la condition n non congru à 2 modulo 4 est équivalente au fait qu'aucun des r_l ne préserve une forme symplectique.

Ainsi, d'après le lemme 3.17, on voit que si -1 n'appartient pas à H et $n = 2a$ est congru à 2 modulo 4, alors $SL(n,k)$ ne contient pas de sous-groupes Zariski-denses H-loxodromiques. En effet, la représentation r_a est symplectique, donc $r_a(SL(n,k))$ ne contient pas de sous-groupe Zariski-dense H-proximal, donc $SL(n,k)$ ne contient pas de sous-groupe Zariski-dense H-loxodromique. Donc le premier point implique le deuxième.

Il suffit maintenant de montrer que dans les autres cas, on peut trouver des sous-groupes Zariski-denses dont tous les éléments sont H-loxodromiques. Il faut donc construire un triplet transverse et H-valué de la variété des drapeaux.

Pour cela, on sait que le drapeau canonique z_0 associé à la base $(e_1, \ldots, e_n)$ est dans $\Lambda^X_{SL(n,k)}$. De plus, dans tous les cas considérés, le lemme 3.28 nous donne t et t' tels que le triplet $(z_0, e^{tY}z_0, e^{t'Y}z_0)$ est transverse et H-valué car son image dans toutes les représentations r_l l'est (ici Y désigne Y_0 si n est impair et Y_1 si n est pair).

On en déduit l'existence d'un sous-groupe de $SL(n,k)$ Zariski-dense dont tous les éléments sont H-loxodromiques d'après la proposition 3.23. Ainsi le deuxi'eme point implique le premier. □

Le théorème 3.21 est donc bien démontré.

Pour en déduire le théorème 3.1, il suffit de remarquer que grâce au théorème 3.3 et à l'équivalence entre les deux premiers points du théorème 3.21, on a l'équivalence entre l'existence d'un sous-groupe Zariski-dense et H-loxodromique, et l'existence d'un sous-groupe Zariski-dense dont toutes les matrices ont leur spectre dans H.

Concluons en donnant deux applications du théorème 3.1 :

Corollaire 3.29. — *On peut trouver dans $SL_n(\mathbb{Q}_p)$ un sous-groupe Zariski-dense dont toutes les valeurs propres sont des carrés si et seulement si ($n \not\equiv 2\,[4]$ ou $p \equiv 1\,[4]$).*

Corollaire 3.30. — *Pour tout entier n, pour tout k corps local de caractéristique 0, on peut trouver un sous-groupe Zariski-dense de $SL(n,k)$ dont toutes les valeurs propres sont des cubes.*

BIBLIOGRAPHIE

[1] H. Abels, G. Margulis & G. Soifer – « Semigroups containing proximal linear maps », *Isr. Jour. Math* **91** (1995), p. 1–30.

[2] Y. Benoist – « Actions propres sur les espaces homogènes réductifs », *Annals of Math.* **144** (1996), p. 315–347.

[3] ______, « Propriétés asymptotiques des groupes linéaires », *Geom. Funct. Anal.* **7** (1997), p. 1–47.

[4] ______, « Sous-groupes discrets des groupes de Lie », *Notes de cours* (1997).

[5] ______, « Automorphismes des cônes convexes », *Inventiones mathematicae* **141** (2000).

[6] Y. Benoist & F. Labourie – « Sur les difféomorphismes d'Anosov affines à feuilletages stable et instable différentiables », *Inventiones mathematicae* **111** (1993), p. 285–308.

[7] A. Borel – *Linear algebraic groups*, Mathematics Lecture Note Series, New York, 1969.

[8] A. Borel & J. Tits – « Groupes réductifs », *Inst. Hautes Etudes Sci. Publ. Math.* **27** (1965), p. 55–150.

[9] N. Bourbaki – *Groupes et algèbres de lie, chap. i*, Hermann, Paris, 1960.

[10] W. Casselman – *Introduction to the theory of admissible representation of p-adic reductive groups*, 1995.

[11] J. Cassels – *Rational quadratic forms*, Academic Press, London, New York, San Francisco, 1978.

[12] L. Clozel – « Démonstration de la conjecture τ », *Invent. Math.* **151** (2003), p. 297–328.

[13] L. Clozel, H. Oh & E. Ullmo – « Hecke operators and equidistribution of Hecke points », *Invent. Math.* **144** (2001), p. 327–351.

[14] S. Dani & J. Smillie – « Uniform distribution of horocycle orbits for fuchsian groups », *Duke Math. J.* **51** (1984), p. 185–194.

[15] W. Duke – « Some old problems and new results about quadratic forms », *Notices A.M.S* **44** (1997), p. 190–196.

[16] W. Duke & R. Schulze-Pillot – « Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids », *Invent Math* **99** (1990), p. 49–57.

[17] J. Ellenberg & A. Venkatesh – « Local-global principles for representations of quadratic forms », *Prépublication ; arxiv :math.NT/0604232* (2006).

[18] A. Eskin & C. McMullen – « Mixing, counting and equidistribution in Lie groups », *Duke Math. J.* **71** (1993), p. 181–209.

[19] A. Eskin & H. Oh – « Ergodic theoretic proof of equidistribution of Hecke points », *Erg. The. and Dyn. Sys.* (To appear).

[20] A. Gorodnik, F. Maucourant & H. Oh – « Manin's conjecture on rational points of bounded height and adelic mixing », *Prépublication* (2005).

[21] A. Gorodnik & B. Weiss – « Distribution of lattice orbits on homogeneous varieties », *à paraitre dans Geometric and functional analysis* (2004).

[22] B. Gross – « On the Satake isomorphism », *Galois Representations in Arithmetic Algebraic Geometry* (R. T. A.J. Scholl, éd.), Cambridge University Press, 1998, p. 223–237.

[23] S. Lang – *Algebra, 3rd ed.*, Addison-Wesley, 1993.

[24] F. Ledrappier – « Distribution des orbites des réseaux sur le plan réel », *C. R. Acad. Sci* **329** (1999), p. 61–64.

[25] F. Ledrappier & M. Pollicott – « Distribution results for lattices in $SL(2,\mathbb{Q}_p)$ », *Bull. Braz. Math. Soc.* **36(2)** (2005), p. 143–176.

[26] G. Margulis – « Formes quadratiques indéfinies et flots unipotents sur les espaces homogènes », *Compte Rendus de l'Académie des Sciences Série 1* **304** (1987), p. 249–253.

[27] G. Margulis & G. Tomanov – « Invariant measures for actions of unipotent groups over local fields on homogeneous spaces », *Invent. Math.* **116** (1994), p. 347–392.

[28] V. Platonov & A. Rapinchuk – *Algebraic groups and number theory*, Academic Press, Boston MA, London, Sydney, 1994.

[29] C. Pommerenke – « Über die Gleichverteilung von Gitterpunkten auf m-dimensionalen Ellipsoiden », *Acta Arithmetica* **5** (1959), p. 227–257.

[30] J. Quint – « Sous-groupes discrets des groupes de Lie semi-simples réels et p-adiques », Thèse, Université Paris 7 Denis Diderot, 2001.

[31] D. Serre – *Les matrices*, Dunod, 2001.

[32] J. Serre – *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1995.

[33] N. Shah – « Limit distributions of expanding translates of certain orbits on homogeneous spaces », *Proc. Indian Acad. Sci. (Math. Sci.)* **106 no 2** (1996), p. 105–125.

[34] W. Tartakowsky – « La détermination de la totalité des nombres représentables par une forme quadratique positive quaternaire », *Compte Rendus de l'Académie des Sciences* **186** (1928), p. 1684–1987.

[35] J. Tits – « Reductive groups over local fields », *Proceedings of Symposia in Pure Mathematics* **33** (1979), p. 20–70.

[36] G. Tomanov – « Orbits on homogeneous spaces of arithmetic origin and approximations », *Adv. Stud. Pure Math.* **26** (2000), p. 265–297.

Résumé : Cette thèse étudie quelques propriétés de répartition d'orbites de réseaux dans des variétés homogènes. Nous étudions principalement deux techniques :

– d'abord nous exploitons des résultats de mélange adélique pour étudier certains ensembles de matrices rationnelles dans un groupe réel compact. On montre par exemple l'équirépartition dans des groupes unitaires d'ensembles de matrices rationnelles définies par des conditions sur les dénominateurs des coefficients. Cela mène à des résultats d'existence de type passage local-global pour ces matrices.
– Ensuite, nous étudions la théorie des dynamiques polynomiales, issue du théorème de Ratner. Cela nous permet de montrer des résultats d'équirépartition d'orbites de réseaux de $SL(n, k)$ (k est un corps local non-archimédien de caractéristique nulle) dans un certain espace homogène sous ce groupe. Puis, nous montrons un analogue S-arithmétique d'un résultat d'équirépartition dû à Shah dans le cas réel.

Dans un troisième temps, nous abordons un problème un peu différent : étant donnés un corps local k de caractéristique nulle, et H un sous-groupe d'indice fini des inversibles de k, nous montrons que le groupe $SL(n, k)$ admet un sous-groupe Zariski-dense dont toutes les matrices ont leur spectre inclus dans H si et seulement si -1 est dans H ou bien n n'est pas congru à 2 modulo 4.

Mots clés : Groupes de Lie, groupes algébriques, groupes discrets, réseaux, groupes unipotents, espaces homogènes, équirépartition, mélange, adèles, théorème de Ratner.

Abstract : In this work, we study some properties of repartition of sets in homogeneous spaces. We use two different techniques :

– first we apply adelic mixing in order to study repartition of sets of rational matrices in a compact real group. We get equirepartition results in an unitary group for sets of rational matrices defined by conditions on denominators of coefficients. This yields a local-global principle for the existence of these matrices.
– Second we use some properties of polynomial dynamic, such as Ratner rigidity theorem. This yields equidistribution results for orbits of a lattice of the special linear group on a local field of characteristic 0 in an homogeneous space under this group. We also get an S-arithmetic analogue of a theorem due to Shah in the real case.

Third, we focus on a different problem : given a local field k of characteristic 0, and H a finite index subgroup of k^*, can we find a Zariski-dense subgroup in $SL(n, k)$ such that all the elements have their whole spectrum inside H ? We are able to answer this question : a sufficient and necessary condition is that either -1 belong to H or n is not congruent to 2 modulo 4.

Keywords : Lie groups, algebraic groups, discrete groups, lattices, unipotent groups, homogeneous spaces, equirepartition, mixing, adele, Ratner's theorem.