



HAL
open science

Groupes arithmétiques et approximation diophantienne

Nicolas de Saxcé

► **To cite this version:**

| Nicolas de Saxcé. Groupes arithmétiques et approximation diophantienne. 2021. hal-03424971

HAL Id: hal-03424971

<https://hal.science/hal-03424971>

Preprint submitted on 10 Nov 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Groupes arithmétiques et approximation diophantienne

Arithmetic groups and diophantine approximation

Nicolas de Saxcé

CNRS – Université Sorbonne Paris Nord

GROUPES ARITHMÉTIQUES ET APPROXIMATION DIOPHANTINNE

Résumé

Nous développons une théorie de l'approximation diophantienne dans les variétés de drapeaux, obtenues comme quotient d'un groupe de Lie semi-simple défini sur \mathbb{Q} par un sous-groupe parabolique. En nous appuyant sur des résultats de la théorie des groupes arithmétiques, dûs entre autres à Borel et Harish-Chandra, et à Margulis et ses collaborateurs, nous démontrons dans ce cadre des généralisations des théorèmes classiques de l'approximation diophantienne.

Mots-clefs : groupes algébriques, dynamique homogène, approximation diophantienne

ARITHMETIC GROUPS AND DIOPHANTINE APPROXIMATION**Abstract**

We develop a theory of diophantine approximation on generalized flag varieties, varieties that can be obtained as a quotient of a semisimple algebraic \mathbb{Q} -group by a parabolic \mathbb{Q} -subgroup. Using methods from the theory of arithmetic groups, due in particular to Borel and Harish-Chandra, and to Margulis and his collaborators, we prove in this setting analogs of the classical theorems of diophantine approximation.

Keywords : algebraic groups, homogeneous dynamics, diophantine approximation

Remerciements

Ce mémoire a été écrit à l'occasion d'une habilitation à diriger des recherches, soutenue par l'auteur en juin 2021, à l'université Sorbonne Paris Nord. Je remercie vivement Julien Barral, Yves Benoist, Emmanuel Breuillard, Manfred Einsiedler, Frédéric Paulin, Jean-François Quint, et Olivier Wittenberg pour leurs commentaires sur une version antérieure du manuscrit, qui m'ont aidé à améliorer la présentation en de nombreux endroits.

Table des matières

1	Introduction	7
1.1	Résultats principaux	11
1.2	Une correspondance	16
1.3	Espaces de réseaux	18
2	Une correspondance	25
2.1	Hauteurs	25
2.2	Distance de Carnot-Carathéodory	26
2.3	L'espace des réseaux	30
2.4	L'exposant diophantien	31
2.5	Points mal approchables	37
2.6	Un cas particulier : la hauteur anti-canonique	39
3	Le théorème de Khintchine	43
3.1	Voisinages de l'infini	44
3.2	Théorème de Khintchine et flots diagonaux	49
3.3	Somme convergente	53
3.4	Somme divergente	56
4	Géométrie des espaces de réseaux	61
4.1	Théorie de la réduction	61
4.2	Représentations et ensembles fondamentaux	62
4.3	Drapeau partiel associé à un réseau	64
4.4	Une relation d'ordre sur \mathfrak{a}	68
5	Approximation des points algébriques	73
5.1	Orbites diagonales algébriques dans G/Γ	73
5.2	Flots semi-stables et extrémalité	77
5.3	L'exposant diophantien d'un point algébrique	79
6	Non divergence quantitative	85
6.1	Sous-ensembles de G/Γ	86
6.2	Fonctions régulières et non divergence	87
6.3	Non divergence pour une racine fixée	87
6.4	Non divergence globale	89
6.5	Drapeau partiel pour une mesure régulière	91

7	Flots diagonaux dans G/Γ	93
7.1	Mesures régulières	93
7.2	Adhérence de Zariski et hérédité	95
7.3	Encadrement du taux de fuite	96
7.4	Variétés algébriques définies sur $\overline{\mathbb{Q}}$	99
8	Approximation dans les sous-variétés	103
8.1	Variétés analytiques réelles	103
8.2	Un critère d'extrémalité	106
8.3	Sous-variétés algébriques définies sur $\overline{\mathbb{Q}}$	108
9	Quelques exemples	111
9.1	Espace projectif	111
9.2	Quadriques	113
9.3	Grassmannienne	114
9.4	Variété des drapeaux dans \mathbb{R}^d	118
10	Conclusion	121

Chapitre 1

Introduction

Tout nombre réel peut être approché par des rationnels, et l'on peut donc se demander à quelle vitesse une suite de nombres rationnels peut converger vers un point x donné sur la droite réelle. Naturellement, il s'agit alors de comparer la *hauteur*, i.e. le dénominateur, d'une approximation rationnelle $v = \frac{p}{q}$, à sa *distance* au point x . On s'intéresse donc à des inégalités de la forme $d(x, v) \leq \psi(H(v))$, où $d(x, v) = |x - v|$ désigne la distance de x à v , $H(v)$ la hauteur du point rationnel v , et $\psi : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ une fonction de limite nulle en l'infini. Ces problèmes sont apparus dès l'Antiquité Grecque, autour du Vème siècle avant J.-C., avec la découverte de l'existence des nombres irrationnels. Ainsi, Archimède proposait-il d'approcher le nombre π par la fraction $\frac{22}{7}$. À la Renaissance, ces questions furent redécouvertes en Europe occidentale, en particulier via les fractions continues, et sont depuis lors un sujet central des mathématiques. Les équations dont les inconnues sont des nombres entiers ou rationnels étaient dites « diophantiennes », en référence à Diophante d'Alexandrie, qui écrivit un mémoire à leur sujet vers le IIIème siècle après J.C., et Hermann Minkowski suggéra donc d'appeler « approximations diophantiennes » les solutions approchées à ces équations. Au cours du XXème siècle, cette expression s'est naturellement imposée pour désigner la théorie qui s'est développée autour de ces problèmes. Le résultat le plus connu du domaine est sans doute le théorème de Dirichlet, dont la démonstration est basée sur le célèbre « principe des tiroirs », et selon lequel, pour tout $x \in \mathbb{R}$, pour tout entier $Q \geq 1$, il existe $q \in \{0, \dots, Q\}$ tel que

$$\left| x - \frac{p}{q} \right| < \frac{1}{qQ}.$$

Entre autres résultats importants, on peut aussi citer le théorème de Khintchine [28] sur les approximations rationnelles à un point choisi aléatoirement suivant la mesure de Lebesgue, le théorème de Thue-Siegel-Roth [60, 57, 48] sur les approximations rationnelles des nombres algébriques, et les théorèmes de Baker sur les approximations de logarithmes de nombres rationnels [4]. Bien sûr, ces problèmes peuvent aussi être étudiés en dimension supérieure, et l'on étudie alors les approximations rationnelles des points d'un l'espace affine réel, ou mieux, d'un espace projectif $\mathbb{P}^n(\mathbb{R})$. Tous les résultats mentionnés ci-dessus s'adaptent à ce cadre. Par exemple, le théorème de Dirichlet a été généralisé par Minkowski [45], Khintchine lui-même [29] observa que la théorie métrique de l'approximation diophantienne qu'il développait pouvait se formuler en dimension arbitraire, et Schmidt [52] démontra

son fameux « théorème du sous-espace » pour étudier les approximations rationnelles des points de \mathbb{R}^n à coordonnées algébriques, généralisant ainsi les résultats de Roth. Avec le développement du domaine, il apparut qu'une grande part de la géométrie sous-jacente pouvait être convenablement décrite à l'aide des outils de la « géométrie des nombres ». Cette théorie, introduite par Minkowski, Mahler et Siegel [58], consiste en l'étude des *réseaux*, sous-groupes discrets de rang maximal de l'espace euclidien \mathbb{R}^d . La pertinence de l'espace des réseaux se fit plus frappante encore avec les travaux de Dani [13], qui montra que certains problèmes diophantiens pouvaient se formuler efficacement en termes de flots sur l'espace des réseaux, puis de Kleinbock et Margulis [31], qui se servirent des flots sur l'espace des réseaux pour résoudre une conjecture importante de Sprindzuk [59], à l'aide d'idées provenant des travaux de Margulis [44] sur les orbites unipotentes dans les espaces homogènes. Cela ouvrit la voie à l'étude de l'approximation diophantienne à l'aide de la dynamique homogène, ce qui non seulement permit d'obtenir de nouvelles démonstrations de résultats déjà connus, mais encore mena à beaucoup des progrès récents du domaine. Pour n'en citer que quelques-uns, mentionnons seulement la nouvelle démonstration du théorème de Khintchine par Kleinbock et Margulis [32], les travaux de Shah [56] sur les améliorations du théorème de Dirichlet et leurs généralisations par Yang [61], les résultats de Menny Aka, Emmanuel Breuillard, Lior Rosenzweig et l'auteur du présent mémoire [1, 2] sur les propriétés diophantiennes des groupes de Lie nilpotents, et tout récemment, la démonstration par Beresnevich et Yang [6, 5] d'une version du théorème de Khintchine pour des points choisis aléatoirement sur une sous-variété analytique. De façon intéressante, l'approche de Kleinbock et Margulis pour résoudre la conjecture de Sprindzuk a de nombreux points communs avec la démonstration de Schmidt de son théorème du sous-espace, et comme nous l'avons observé avec Emmanuel Breuillard [12], il est possible d'unifier ces deux résultats en un seul énoncé sur le comportement asymptotique de certaines orbites diagonales dans l'espace des réseaux.

Plus généralement, on peut considérer une variété algébrique X définie sur \mathbb{Q} arbitraire, sur laquelle les points rationnels sont denses, et étudier la qualité des approximations rationnelles $v \in X(\mathbb{Q})$ à un point donné $x \in X(\mathbb{R})$. On souhaite alors obtenir des résultats analogues aux théorèmes classiques de l'approximation diophantienne. Certains auteurs font référence à ce type de problème sous le terme « approximation diophantienne *intrinsèque* », pour souligner la différence avec l'approximation diophantienne sur les sous-variétés étudiée par Sprindzuk et ses successeurs, où l'on étudie simplement les approximations à un point choisi aléatoirement sur une sous-variété $M \subset \mathbb{P}^n(\mathbb{R})$ par des points rationnels quelconques dans $\mathbb{P}^n(\mathbb{R})$, et non nécessairement sur M . Dès 1965, dans un article de survol sur l'approximation diophantienne, Lang [39] suggérait plusieurs problèmes d'approximation diophantienne intrinsèque, mais ceux-ci ne semblent pas avoir suscité beaucoup d'intérêt jusqu'aux travaux récents de Ghosh, Gorodnik et Nevo sur le sujet [23, 24, 22]. Il y a quelques années, Kleinbock et Merrill [36] ont proposé une approche très élégante à l'approximation diophantienne intrinsèque sur les sphères, à l'aide de flots diagonaux sur l'espace G/Γ , où $G = \mathrm{SO}(1, n)$ est un groupe orthogonal de signature $(1, n)$, et $\Gamma = G(\mathbb{Z})$ un sous-groupe arithmétique. Ils ont ainsi pu démontrer les analogues de plusieurs résultats classiques, comme les théorèmes de Dirichlet ou de Khintchine. En collaboration avec Fishman et Simmons [20], ils ont d'ailleurs montré peu après que leurs méthodes s'appliquent aussi à l'étude de l'approximation diophantienne sur une quadrique rationnelle arbitraire. Dans un

autre article [19], les mêmes auteurs ont tenté d'initier une étude de l'approximation diophantienne intrinsèque sur des variétés quelconques, mais le cadre choisi était sans doute trop général pour que l'on y puisse obtenir des résultats optimaux.

Le présent mémoire a pour but de montrer que les *variétés de drapeaux*, obtenues comme quotient $X = P \backslash G$ d'un groupe algébrique semi-simple G défini sur \mathbb{Q} par un sous-groupe parabolique P , forment une classe naturelle de variétés pour étudier l'approximation diophantienne. Une fois munie X des notions de hauteur et de distance appropriées, nous verrons que les méthodes de la dynamique homogène s'appliquent et permettent d'obtenir une théorie satisfaisante de l'approximation diophantienne. Naturellement, dans ce cadre, l'espace $\mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$ des réseaux dans l'espace euclidien est remplacé par un quotient plus général G/Γ de G par un sous-groupe arithmétique Γ , et les flots sur cet espace seront étudiés grâce à la théorie de la réduction des groupes arithmétiques, développée par Borel et Harish-Chandra [9]. Notons cependant que même dans le cas où $G = \mathrm{SL}_d$ est le groupe spécial linéaire, notre approche nous permet d'obtenir plusieurs résultats nouveaux sur certains problèmes posés par Schmidt [51] au sujet des approximations rationnelles des sous-espaces linéaires de \mathbb{R}^d .

Beaucoup des méthodes que nous utilisons pour construire la théorie de l'approximation diophantienne sur les variétés de drapeaux avaient auparavant été utilisées seulement dans certains cas particuliers. Par conséquent, nous avons parfois dû modifier les énoncés disponibles dans la littérature, et souvent en donner de nouvelles démonstrations. Nous décrivons brièvement maintenant les principales idées nouvelles qui nous ont permis d'arriver à nos fins.

La correspondance

Le premier problème lorsqu'on étudie une variété de drapeau générale $X = P \backslash G$ est qu'il peut y avoir de nombreux choix de hauteur possible sur $X(\mathbb{Q})$. À équivalence près, toute hauteur sur $X(\mathbb{Q})$ provient d'un plongement de X dans l'espace projectif d'une représentation irréductible de G . L'approche qui s'est naturellement imposée pour nous a été de ne pas choisir une hauteur particulière sur X , ou plus précisément, de travailler avec une hauteur H_χ arbitraire, associée à un plongement $X \hookrightarrow \mathbb{P}(V_\chi)$ dans l'espace projectif associé à une représentation irréductible V_χ de G . Le second problème, peut-être plus surprenant, est que la distance appropriée sur $X(\mathbb{R})$ n'est pas en général une distance riemannienne. En effet, pour pouvoir traduire les propriétés diophantiennes d'un point en termes du comportement asymptotique d'une orbite dans G/Γ , il est nécessaire de disposer d'un sous-groupe à un paramètre (a_t) dans G qui dilate la métrique sur X ; cela est seulement possible pour la distance de Carnot-Carathéodory construite au chapitre 2. Ces distances sont très naturelles, et ont déjà fait l'objet d'études approfondies, en particulier par Gromov [25] et ses successeurs. Une fois définies la hauteur et la distance sur X , on pourrait espérer – c'est le cas lorsque $X = \mathbb{P}^n$ – que la correspondance relie simplement les meilleures approximations rationnelles à un point $x = Ps_x$ dans X aux petits vecteurs dans les réseaux de l'orbite $(a_t s_x V_\chi(\mathbb{Z}))_{t>0}$. Cela cependant n'est pas absolument vrai, car certains petits vecteurs dans l'orbite du réseau ne donnent pas lieu à une bonne approximation¹, et il faut en outre contrôler la di-

¹Il peut même arriver qu'un point correspondant à une orbite divergente dans l'espace des réseaux soit strictement moins bien approché par des rationnels qu'un point correspondant à une

rection des petits vecteurs dans l'orbite. L'énoncé précis de la correspondance est donné au chapitre 2, Proposition 2.4.4, et aussi, dans une version légèrement plus générale, au chapitre 3, Proposition 3.2.4, pour la démonstration du théorème de Khintchine sur X .

Orbites diagonales et théorie de la réduction

Afin d'étudier le comportement asymptotique des orbites diagonales dans l'espace des réseaux, il est commode de formuler les énoncés à l'aide des objets donnés par la théorie de la réduction, qui fournit une description précise du voisinage de l'infini dans l'espace G/Γ . Comme cela apparaissait déjà dans nos travaux en commun avec Menny Aka, Emmanuel Breuillard et Lior Rosenzweig [2] ou dans ceux de Pengyu Yang [61], ce sont les variétés de Schubert dans X qui permettent de formuler un critère pour la divergence d'une orbite diagonale. Nous poursuivons ici cette étude et, dans le cas d'un point à coordonnées algébriques, donnons une formule explicite pour le taux de fuite d'une orbite divergente, le théorème 5.1.1. Cette formule fait intervenir la projection orthogonale sur une chambre de Weyl. Notons que cette projection a déjà été étudiée par Aubert et Howe [3] et s'est avérée utile dans les travaux de Langlands [40] et Vogan [26] sur la classification des représentations irréductibles admissibles des groupes de Lie réductifs. En préliminaire à la démonstration de notre formule, nous étudions soigneusement au chapitre 4 les propriétés de cette projection sur la chambre de Weyl, et sa relation à l'ordre de Kostant [38].

Non divergence quantitative intrinsèque

L'ordre de Kostant et la projection sur la chambre de Weyl sont aussi des objets cruciaux pour énoncer et démontrer le théorème 6.2.1, version précise des inégalités de non divergence quantitative dans un groupe semi-simple G arbitraire, qui est le résultat principal du chapitre 6. Ces inégalités étaient auparavant seulement disponibles lorsque $G = \mathrm{SL}_d$. Bien entendu, il est toujours possible d'obtenir un énoncé de non divergence quantitative par plongement de G dans un groupe SL_d , mais le résultat alors obtenu n'est pas suffisamment précis pour les applications à l'étude des exposants diophantiens que nous avons en vue. La démonstration que nous proposons de ces inégalités est sensiblement différente de celle utilisée par Margulis et ses collaborateurs [44, 31, 42]; nous y utilisons de manière essentielle la théorie de la réduction et la théorie du plus haut poids pour les représentations de groupes semi-simples.

Un problème de Schmidt : l'approximation des sous-espaces vectoriels

Pour illustrer notre méthode, nous décrivons brièvement les résultats qu'elle permet d'obtenir en rapport avec un problème de Schmidt [51] sur les approximations rationnelles des sous-espaces vectoriels de \mathbb{R}^d . Dans son article, après avoir défini les notions de hauteur et de distance appropriées sur la variété grassmannienne $X = \mathrm{Grass}(\ell, d)$ des sous-espaces de dimension ℓ dans \mathbb{R}^d , Schmidt définit l'exposant diophantien d'un point $x \in X$ par la formule

$$\beta(x) = \inf\{\beta > 0 \mid \exists c > 0 : \forall v \in X(\mathbb{Q}), d(x, v) \geq cH(v)^{-\beta}\}$$

orbite bornée! Un tel exemple est donné à la fin du chapitre 9.

et pose le problème de déterminer la borne inférieure $\inf_{x \in X(\mathbb{R})} \beta(x)$. Dans sa conclusion, il observe que l'on peut minorer $\beta(x) \geq \frac{1}{\ell} + \frac{1}{d-\ell}$ pour presque tout sous-espace x de dimension ℓ , et suggère une étude plus approfondie des propriétés diophantiennes d'un point x choisi aléatoirement sur X . L'un de nos premiers résultats, le théorème 9.3.1, montre que pour presque tout x dans X , $\beta(x) = \frac{1}{\ell} + \frac{1}{d-\ell}$. On obtient d'ailleurs une description bien plus précise de la qualité des approximations rationnelles à un sous-espace aléatoire grâce au théorème 9.3.2, analogue du théorème de Khintchine pour les variétés grassmanniennes. Ce qui nous paraît plus intéressant encore, c'est une formule générale pour l'exposant diophantien de n'importe quel sous-espace de \mathbb{R}^d qui admette une base constituée de vecteurs à coordonnées algébriques. Notons que cette formule, donnée dans le théorème 9.3.4, et que l'on doit pouvoir deviner après avoir étudié suffisamment de cas particuliers, ne s'énonce simplement qu'une fois que l'on introduit le formalisme général des groupes semi-simples, et la projection sur la chambre de Weyl. Comme corollaire remarquable de cette formule, nous montrons que tout point algébrique $x \in X(\mathbb{Q})$ vérifie $\beta(x) \geq \frac{1}{\ell} + \frac{1}{d-\ell}$, et donnons une condition nécessaire et suffisante pour qu'une égalité ait lieu, cf. corollaire 9.3.5. En d'autres termes, $\inf_{x \in X(\overline{\mathbb{Q}})} \beta(x) = \frac{1}{\ell} + \frac{1}{d-\ell}$.

1.1 Résultats principaux

Ce mémoire a pour but d'exploiter les méthodes de la théorie des groupes arithmétiques pour étudier l'approximation diophantienne dans certaines variétés, obtenues comme quotient $X = P \backslash G$ d'un groupe algébrique semi-simple G défini sur \mathbb{Q} , par un sous-groupe parabolique défini sur \mathbb{Q} . Les variétés de cette forme sont communément appelées *variétés de drapeaux*. Les exemples les plus élémentaires de telles variétés sont les espaces projectifs \mathbb{P}^n , $n \geq 1$, les variétés grassmanniennes $\text{Grass}(\ell, d)$, $1 \leq \ell \leq d$, les quadriques projectives, et la variété des drapeaux d'un espace vectoriel.

Dans la suite, une variété de drapeaux $X = P \backslash G$ sera toujours munie d'une distance de Carnot-Carathéodory naturelle d , dont la construction est détaillée au paragraphe 2.2. Les hauteurs que nous considérerons sur $X(\mathbb{Q})$ seront obtenues par plongement de X dans un espace projectif. Rappelons que si V est un espace vectoriel défini sur \mathbb{Q} , le choix d'une base rationnelle $(u_i)_{1 \leq i \leq d}$ de V permet de définir une hauteur sur les points rationnels de $\mathbb{P}(V)$: ayant fixé une norme euclidienne sur V pour laquelle la base (u_i) est orthonormée, si $v \in \mathbb{P}(V)(\mathbb{Q})$ est représenté par un vecteur primitif \mathbf{v} dans le réseau $\oplus_i \mathbb{Z}u_i$, on pose

$$H(v) = \|\mathbf{v}\|.$$

Toutes les hauteurs sur $\mathbb{P}(V)$ construites de cette manière sont équivalentes, i.e. comparables à une constante multiplicative près. Ensuite, si V_χ est une représentation irréductible rationnelle de G engendrée par une unique droite $[e_\chi]$ de plus haut poids χ telle que $\text{Stab}_G[e_\chi] = P$, on obtient une hauteur H_χ sur X par restriction d'une hauteur sur $\mathbb{P}(V_\chi)$ en identifiant $X = P \backslash G$ à l'orbite $G[e_\chi]$ de la droite de plus haut poids dans $\mathbb{P}(V_\chi)$. L'approximation diophantienne sur X est l'étude de la qualité des approximations rationnelles d'un point $x \in X(\mathbb{R})$: pour un grand paramètre $T \geq 0$, on cherche à évaluer en fonction de T la distance minimale à x d'un point rationnel v de hauteur $H_\chi(v) \leq T$.

Les résultats que nous démontrons dans ce mémoire se divisent en trois catégories, suivant la manière de choisir le point x dans $X(\mathbb{R})$. Les premiers résultats concernent les propriétés diophantiennes d'un point x choisi aléatoirement suivant la mesure de Lebesgue sur $X(\mathbb{R})$, les seconds traitent d'un point $x \in X(\mathbb{Q})$, i.e. dont les coordonnées sont des nombres algébriques, et pour les derniers, le point x sera choisi aléatoirement sur une sous-variété analytique de $X(\mathbb{R})$.

Propriétés génériques des points de $X(\mathbb{R})$

Pour commencer, on définit l'*exposant diophantien* $\beta_\chi(x)$ d'un point $x \in X(\mathbb{R})$ par

$$\beta_\chi(x) = \inf\{\beta > 0 \mid \exists c > 0 : \forall v \in X(\mathbb{Q}), d(x, v) \geq cH_\chi(v)^{-\beta}\}.$$

Le premier résultat général que nous démontrerons est que la fonction β_χ est constante presque partout sur $X(\mathbb{R})$.

Théorème 1.1 (Valeur presque sûre de l'exposant). *Il existe une constante explicite $\beta_\chi(X) \in \mathbb{Q}$ strictement positive telle que pour presque tout $x \in X(\mathbb{R})$,*

$$\beta_\chi(x) = \beta_\chi(X).$$

Si l'on munit X de la hauteur anti-canonique, ce qui correspond à choisir χ égal à la somme des racines apparaissant dans le radical unipotent de P , un résultat de Franke [21] montre que le nombre de points rationnels $v \in X(\mathbb{Q})$ de hauteur au plus T satisfait, pour certaines constantes $c > 0$ et $b \in \mathbb{N}^*$,

$$N_X(T) \sim c \cdot T(\log T)^{b-1} \quad (T \rightarrow +\infty) \quad (1.1)$$

L'exposant diophantien presque sûr dans X prend alors la valeur naturelle

$$\beta_\chi(X) = \frac{1}{\dim_{cc} X},$$

où $\dim_{cc} X$ est la dimension de Carnot-Carathéodory de X , unique entier tel que le nombre de recouvrement de $X(\mathbb{R})$ par des boules de rayon $\delta > 0$ pour la métrique de Carnot-Carathéodory satisfasse $N(X, \delta) \asymp \delta^{-\dim_{cc} X}$ lorsque δ tend vers zéro. Mohammadi et Salehi Golsefidy [46, Theorem 4], ont généralisé le résultat de Franke et montré que pour toute hauteur H_χ , il existe des constantes $c, u_\chi > 0$ et $v_\chi \in \mathbb{N}^*$ pour lesquelles

$$N_X(T) \sim c \cdot T^{u_\chi} (\log T)^{v_\chi - 1} \quad (T \rightarrow +\infty). \quad (1.2)$$

Une application facile du lemme de Borel-Cantelli permet de montrer qu'on a toujours l'inégalité $\beta_\chi(X) \leq \frac{u_\chi}{\dim_{cc} X}$, quoique l'inégalité puisse être stricte en général.

Au vu du théorème 1.1 ci-dessus, il est naturel de s'intéresser à des propriétés diophantiennes plus fines. Par analogie avec le célèbre théorème de Khintchine [29], pour une fonction $\psi : \mathbb{R}^+ \rightarrow \mathbb{R}^+$, nous considérons l'inégalité

$$d(x, v) \leq H_\chi(v)^{-\beta_\chi(X)} \psi(H_\chi(v)) \quad (1.3)$$

et montrons le théorème suivant.

Théorème 1.2 (Théorème de Khintchine pour une variété de drapeaux). *Il existe des constantes explicites $a_\chi > 0$ et $b_\chi \in \mathbb{N}^*$ pour lesquelles l'énoncé suivant est vérifié. Soit $\psi : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ une fonction décroissante.*

- Si $\int_e^{+\infty} \psi(u)^{\frac{a_\chi}{\beta_\chi(X)}} (\log \log u)^{b_\chi-1} \frac{du}{u} < +\infty$, alors, pour presque tout $x \in X(\mathbb{R})$, l'inégalité (1.3) n'admet qu'un nombre fini de solutions $v \in X(\mathbb{Q})$.
- Si $\int_e^{+\infty} \psi(u)^{\frac{a_\chi}{\beta_\chi(X)}} (\log \log u)^{b_\chi-1} \frac{du}{u} = +\infty$, alors, pour presque tout $x \in X(\mathbb{R})$, l'inégalité (1.3) admet une infinité de solutions $v \in X(\mathbb{Q})$.

Dans le cas où $X = \mathbb{P}^n$ est un espace projectif, on retrouve le théorème démontré par Khintchine [29] en 1926. Le résultat était déjà connu aussi lorsque X est une quadrique projective, depuis les travaux remarquables de Kleinbock et Merrill [36] puis de Fishman, Kleinbock, Merrill et Simmons [20] sur le sujet. Les constantes a_χ et b_χ se calculent facilement à l'aide d'un système de racines associé à G , et proviennent d'un encadrement asymptotique de la mesure de certains voisinages de l'infini dans l'espace G/Γ , où Γ est un sous-groupe arithmétique de G . On renvoie à la proposition 1.13 ci-dessous pour un énoncé plus précis. Dans le cas particulier où X est munie de la hauteur anti-canonique, $a_\chi = 1$ et b_χ est égal au rang rationnel de la variété $X = P \backslash G$, i.e. $b_\chi = \text{rang } G - \text{rang } P$. Grâce à un principe de transfert dû à Beresnevich et Velani [7], cela permet aussi de calculer la dimension de Hausdorff, pour la métrique de Carnot-Carathéodory, des points de $X(\mathbb{R})$ tels que $\beta_\chi(x) = \beta$.

Théorème 1.3 (Théorème de Jarník pour une variété de drapeaux). *Soit X une variété de drapeaux rationnelle munie de sa métrique de Carnot-Carathéodory et de la hauteur anti-canonique H_χ . Pour tout $\beta \geq \frac{1}{\dim_{cc} X}$, l'ensemble*

$$E_\beta = \{x \in X(\mathbb{R}) \mid \beta(x) \geq \beta\}$$

vérifie

$$\dim_{H,cc} E_\beta = \frac{1}{\beta},$$

où $\dim_{H,cc}$ désigne la dimension de Hausdorff associée à la métrique de Carnot-Carathéodory sur X .

Approximation des points algébriques

Nous noterons $\overline{\mathbb{Q}}$ le sous-corps de \mathbb{R} constitué des éléments algébriques sur \mathbb{Q} . Un résultat majeur concernant l'approximation des éléments de $\overline{\mathbb{Q}}$ par des rationnels est le théorème de Roth [48], qui assure que si $x \in \overline{\mathbb{Q}}$ est irrationnel et $\varepsilon > 0$, alors l'inégalité

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{q^{2+\varepsilon}}, \quad p \in \mathbb{Z}, \quad q \in \mathbb{N}^*$$

n'admet qu'un nombre fini de solutions (p, q) . De manière équivalente, si \mathbb{P}^1 est muni de la distance et de la hauteur usuelles, le théorème de Roth affirme que tout élément $x \in \mathbb{P}^1(\overline{\mathbb{Q}}) \setminus \mathbb{P}^1(\mathbb{Q})$ vérifie $\beta(x) = 2$. Ce théorème a d'ailleurs été généralisé par Schmidt [52] : si $x \in \mathbb{P}^n(\overline{\mathbb{Q}})$ n'est inclus dans aucun sous-espace projectif rationnel propre, alors $\beta(x) = 1 + \frac{1}{n}$. Nous montrons que ces résultats sont encore valables dans une variété de drapeaux X arbitraire : hors de certaines contraintes

rationnelles, tous les points algébriques de X ont même exposant diophantien, égal à l'exposant presque sûr d'un point aléatoire de $X(\mathbb{R})$.

Rappelons que la variété $X = P \backslash G$ se décompose en cellules de Schubert : si $B \subset G$ désigne un \mathbb{Q} -sous-groupe parabolique minimal, W le groupe de Weyl associé, et $W_P = (W \cap P) \backslash W$, alors

$$X = \bigsqcup_{w \in W_P} PwB.$$

Notons $X_w = \overline{PwB}$ l'adhérence de la cellule de Schubert PwB . Une *variété de Schubert* dans X est une variété de la forme $X_w g$, pour $w \in W_P$ et $g \in G$. Si l'élément g peut être choisi dans $G(\mathbb{Q})$, nous dirons que la variété de Schubert est *rationnelle*.

Théorème 1.4 (Points algébriques extrémaux). *Si $x \in X(\overline{\mathbb{Q}})$ n'appartient à aucune sous-variété de Schubert rationnelle², alors $\beta_\chi(x) = \beta_\chi(X)$.*

Plus généralement, nous obtenons une formule pour l'exposant d'un point $x \in X(\overline{\mathbb{Q}})$, en termes d'une certaine variété de Schubert rationnelle le contenant. Mais l'énoncé précis de cette formule requiert l'introduction d'autres objets associés à X . Nous noterons T un \mathbb{Q} -tore déployé maximal de G inclus dans B , $A = T^0(\mathbb{R})$ la composante connexe des points réels de T , \mathfrak{a} l'algèbre de Lie de A et $\Pi \subset \mathfrak{a}^*$ la base du système de racines associé à G et T correspondant au parabolique minimal B . Ces objets sont définis plus précisément dans Borel [8, §11] et leur construction détaillée est donnée dans Borel et Tits [10, §5]. Insistons sur le fait que l'on s'intéresse ici aux racines de G par rapport au \mathbb{Q} -tore *déployé* maximal S ; on parle parfois du système des \mathbb{Q} -racines de G , dont la base Π est de cardinal égal au \mathbb{Q} -rang de G .

Si $\theta \subset \Pi$ est l'ensemble de racines simples associé à P – tel que les racines négatives apparaissant dans P se décomposent sur θ – on définit un unique élément Y dans \mathfrak{a} par

$$\alpha(Y) = \begin{cases} 0 & \text{si } \alpha \in \theta \\ -1 & \text{si } \alpha \in \Pi \setminus \theta \end{cases}$$

L'espace \mathfrak{a} étant muni d'une norme euclidienne invariante par l'action du groupe de Weyl, nous noterons $p_{\mathfrak{a}^-} : \mathfrak{a} \rightarrow \mathfrak{a}^-$ la projection au plus proche voisin sur la chambre de Weyl négative

$$\mathfrak{a}^- = \{u \in \mathfrak{a} \mid \forall \alpha \in \Pi, \alpha(u) \leq 0\}.$$

Enfin, l'action adjointe à droite du groupe de Weyl W sur \mathfrak{a} et \mathfrak{a}^* sera notée en exposant : pour $w \in W$, $Y^w = (\text{Ad } w)^{-1}Y$, et $\chi^w = \chi \circ (\text{Ad } w)$.

Théorème 1.5 (Exposant d'un point algébrique). *Pour chaque élément $x \in X(\overline{\mathbb{Q}})$, il existe $w \in W_P$ et $\gamma \in G(\mathbb{Q})$ tels que $x \in X_w \gamma$ et*

$$\beta_\chi(x) = \frac{1}{-\langle \chi, Y \rangle + \langle \chi^w, p_{\mathfrak{a}^-}(Y^w) \rangle}.$$

²Il suffit en fait que x ne soit dans aucune sous-variété de Schubert rationnelle *instable*. On renvoie au paragraphe 5.2 pour plus de détails sur ce sujet.

Dans le théorème ci-dessus, la variété de Schubert $X_w\gamma$ est en fait entièrement déterminée par x . On renvoie le lecteur au paragraphe 5.3 pour le détail de sa construction. Comme corollaire remarquable du théorème ci-dessus, on peut montrer que, dans certains cas, la valeur minimale de l'exposant $\beta_\chi(x)$, $x \in X(\mathbb{Q})$, est égale à $\beta_\chi(X)$.

Corollaire 1.6 (Minoration de l'exposant d'un point algébrique). *Si $X = P \backslash G$, avec P un sous-groupe parabolique maximal du \mathbb{Q} -groupe semi-simple G , alors*

$$\min_{x \in X(\mathbb{Q})} \beta_\chi(x) = \beta_\chi(X).$$

Ce corollaire s'applique en particulier lorsque $X = \text{Grass}(\ell, d)$ est la variété grassmannienne des sous-espaces de dimension ℓ dans \mathbb{R}^d , munie de la hauteur induite par le plongement de Plücker. On obtient ainsi une réponse partielle à un problème de Schmidt [51] :

Problème ouvert : Déterminer la quantité $\inf_{x \in \text{Grass}(\ell, d)} \beta_\chi(x)$.

Plus de détails à ce sujet sont donnés au chapitre 9, où nous décrivons quelques exemples de variétés de drapeaux. Nous verrons aussi dans ce chapitre que le corollaire ci-dessus est faux en général si le sous-groupe parabolique P n'est pas maximal. Il reste cependant valable dans un autre cas important : si $X = P \backslash G$ avec G déployé sur \mathbb{Q} , P un \mathbb{Q} -parabolique *minimal*, et H_χ la hauteur anti-canonique sur X .

Approximation dans les sous-variétés

Nous voulons maintenant décrire les propriétés diophantiennes presque sûres d'un point x choisi aléatoirement sur une sous-variété analytique $M \subset X(\mathbb{R})$. Si M est une variété analytique de dimension m , on considère une mesure λ_M sur M équivalente à la restriction à M de la mesure de Hausdorff de dimension m . Comme nos résultats ne dépendent de la mesure qu'à équivalence près, le choix précis de λ_M n'aura pas d'importance dans la suite.

Le premier résultat que nous établissons est que l'exposant diophantien d'un point de M est constant presque sûrement. Ce fait remarquable généralise un résultat de Kleinbock [33], valable lorsque X est un espace projectif.

Théorème 1.7 (Exposant d'une sous-variété analytique). *Soit M une sous-variété analytique connexe de X . Il existe une constante $\beta_\chi(M)$ telle que pour presque tout $x \in M$, $\beta_\chi(x) = \beta_\chi(M)$.*

Suivant la terminologie introduite par Sprindzuk [59], nous dirons qu'une sous-variété analytique $M \subset X$ est *extrémale* si $\beta_\chi(M) = \beta_\chi(X)$. Dans le cas où $X = \mathbb{P}^n$ est un espace projectif, une sous-variété analytique est dite *non dégénérée* si elle n'est incluse dans aucun sous-espace projectif strict. La conjecture de Sprindzuk, démontrée par Kleinbock et Margulis [31] en 1998, stipulait que toute sous-variété analytique non dégénérée dans \mathbb{P}^n était extrémale. Ici encore, ce résultat admet une généralisation naturelle au cadre des variétés de drapeaux. Nous dirons qu'une sous-variété analytique $M \subset X$ est *non dégénérée* si elle n'est incluse dans aucune sous-variété de Schubert propre. Cette terminologie est bien sûr compatible avec celle déjà utilisée dans le cas où X est un espace projectif.

Théorème 1.8 (Extrémalité des sous-variétés non dégénérées). *Toute sous-variété analytique connexe M non dégénérée³ dans X est extrémale.*

Notre dernier résultat mêle sous-variétés analytiques et nombres algébriques. En prenant pour variété un singleton $M = \{x\}$, avec $x \in X(\overline{\mathbb{Q}})$, on retrouvera d'ailleurs le théorème 1.5 énoncé ci-dessus. Nous reprenons les notations introduites juste avant le théorème 1.5.

Théorème 1.9 (Exposant d'une sous-variété définie sur $\overline{\mathbb{Q}}$). *Soit M une sous-variété analytique connexe de X dont l'adhérence de Zariski est définie sur $\overline{\mathbb{Q}}$. Il existe $w \in W_P$ et $\gamma \in G(\mathbb{Q})$ tels que $M \subset X_w\gamma$ et pour presque tout $x \in M$,*

$$\beta_\chi(x) = \frac{1}{-\langle \chi, Y \rangle + \langle \chi^w, p_{\mathfrak{a}^-}(Y^w) \rangle}.$$

On observe que les énoncés concernant l'approximation diophantienne sur les sous-variétés sont très voisins de ceux concernant les points algébriques. Cela s'explique par le fait que les contraintes géométriques qui apparaissent sont les mêmes dans les deux situations. Pour les mettre en évidence, nous utilisons une correspondance entre les propriétés diophantiennes d'un point $x \in X(\mathbb{R})$ et le comportement asymptotique de certaines orbites diagonales dans l'espace des réseaux d'un espace euclidien.

1.2 Une correspondance

Un *réseau* Δ dans un espace euclidien V est un sous-groupe discret de rang maximal. En d'autres termes, pour une base $(v_i)_{1 \leq i \leq d}$ de V , on peut écrire

$$\Delta = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_d.$$

Le groupe linéaire $GL(V)$ agit naturellement sur l'espace des réseaux de V . Les travaux de Minkowski [45] et Siegel [58] ont mis en évidence le fait que de nombreuses propriétés arithmétiques se comprennent simplement grâce à l'espace des réseaux. Cette approche de l'arithmétique, souvent appelée « géométrie des nombres », s'est aussi révélée particulièrement fructueuse pour l'approximation diophantienne. Elle est en particulier à la base de la démonstration de Schmidt de son théorème du sous-espace [53, Theorem 1F]. Mais commençons par un exemple simple, qui illustre bien l'intérêt de l'espace des réseaux pour l'étude de l'approximation diophantienne.

L'espace projectif

Nous avons défini plus haut l'exposant diophantien d'un point $x \in \mathbb{P}^n(\mathbb{R})$:

$$\beta(x) = \inf\{\beta > 0 \mid \exists c > 0 : \forall v \in \mathbb{P}^n(\mathbb{Q}), d(x, v) \geq cH(v)^{-\beta}\}.$$

Si $x \in \mathbb{P}^n(\mathbb{R})$ s'écrit en coordonnées homogènes $x = [1 : x_1 : \dots : x_n]$, nous lui associons un réseau Δ_x dans \mathbb{R}^d par la formule

$$\Delta_x = s_x \mathbb{Z}^d, \quad \text{où } s_x = \begin{pmatrix} 1 & 0 & \dots & 0 \\ -x_1 & 1 & \dots & 0 \\ \vdots & 0 & \ddots & 0 \\ -x_n & 0 & \dots & 1 \end{pmatrix}.$$

³Ici encore il suffit de supposer que M n'est incluse dans aucune sous-variété de Schubert instable, comme expliqué au paragraphe 8.2.

La *systole*, ou *premier minimum*, d'un réseau Δ est la longueur minimale d'un vecteur non nul dans Δ :

$$\lambda_1(\Delta) = \inf \{ \lambda > 0 \mid \Delta \cap B(0, \lambda) \neq \{0\} \}.$$

Nous considérons alors dans $\mathrm{GL}_d(\mathbb{R})$ le sous-groupe

$$a_t = \mathrm{diag}(e^{-t}, e^{t/n}, \dots, e^{t/n}),$$

et posons

$$\gamma(x) = \limsup_{t \rightarrow +\infty} \frac{-1}{t} \log \lambda_1(a_t \Delta_x).$$

La proposition élémentaire ci-dessous est tirée de Kleinbock et Margulis [32, Theorem 8.5], et généralise des résultats antérieurs de Dani [13].

Proposition 1.10 (Correspondance de Dani pour \mathbb{P}^n). *Pour tout $x \in \mathbb{P}^n(\mathbb{R})$,*

$$\beta(x) = \left(1 + \frac{1}{n}\right) \frac{1}{1 - \gamma(x)}.$$

Le point de départ de tous les résultats démontrés dans ce mémoire est une généralisation de cette proposition, dans laquelle l'espace projectif est remplacé par une variété de drapeaux X arbitraire.

Variétés de drapeaux

Rappelons que X peut s'écrire comme l'espace quotient $X = P \backslash G$ d'un \mathbb{Q} -groupe semi-simple G par un \mathbb{Q} -sous-groupe parabolique P , et que $X(\mathbb{R})$ est munie de la distance de Carnot-Carathéodory naturelle définie au paragraphe 2.2. Nous fixons aussi une représentation rationnelle irréductible de G sur un espace vectoriel V_χ engendré, comme G -module, par une unique droite rationnelle de plus haut poids e_χ . Nous supposons en outre que le stabilisateur dans G de la droite engendrée par e_χ est égal à P . Cela permet de plonger X dans l'espace projectif $\mathbb{P}(V_\chi)$; la hauteur sur $X(\mathbb{Q})$ obtenue par restriction de la hauteur usuelle sur $\mathbb{P}(V_\chi)$ est notée H_χ .

Pour étudier l'approximation diophantienne dans X , munie de la hauteur H_χ , nous utiliserons l'espace des réseaux de V_χ . Ayant fixé un réseau rationnel $V_\chi(\mathbb{Z})$ dans V_χ , nous associons à chaque élément x de $X(\mathbb{R})$ un réseau

$$\Delta_x = s_x V_\chi(\mathbb{Z}), \quad \text{où } s_x \in G \text{ est tel que } x = P s_x.$$

Nous utiliserons le sous-groupe à un paramètre (a_t) déjà mentionné ci-dessus :

$$a_t = e^{tY}, \quad \text{où } Y \in \mathfrak{a} \text{ est défini par } \alpha(Y) = \begin{cases} 0 & \text{si } \alpha \in \theta \\ -1 & \text{si } \alpha \notin \theta. \end{cases}$$

La correspondance qui relie l'exposant diophantien $\beta_\chi(x)$ au comportement asymptotique de l'orbite $(a_t \Delta_x)_{t>0}$ met en jeu une quantité un peu plus subtile à définir que la systole d'un réseau. Notons

$$\tilde{X} = G \cdot e_\chi \subset V_\chi$$

l'orbite de e_x dans V_x sous l'action de G . L'ensemble \tilde{X} est le cône dans V_x contenant toutes les droites du plongement de X dans $\mathbb{P}(V_x)$, privé du point 0. L'espace V_x se décompose en somme directe d'espaces de poids sous l'action du groupe abélien (a_t) , et nous notons

$$\pi^+ : V_x \rightarrow \mathbb{R}e_x$$

la projection sur e_x parallèlement à la somme de tous les autres espaces de poids. Pour tout réseau Δ dans V_x , nous posons

$$r_x(\Delta) = \inf \left\{ r > 0 \mid \exists v \in \Delta \cap B(0, r) : \begin{array}{l} v \in \tilde{X} \\ \|\pi^+(v)\| \geq \frac{\|v\|}{2} \end{array} \right\}.$$

Remarquons qu'on peut avoir $r_x(\Delta) = +\infty$, par exemple si Δ ne rencontre pas le cône \tilde{X} . Quoiqu'il en soit, on pose

$$\gamma_x(x) = \limsup_{t \rightarrow +\infty} \frac{-1}{t} \log r_x(a_t \Delta_x).$$

Il n'est pas difficile de se convaincre que cette quantité ne dépend pas du choix de l'élément s_x tel que $x = Ps_x$; cela est expliqué en détail au paragraphe 2.4. On peut alors relier les quantités $\beta_x(x)$ et $\gamma_x(x)$ grâce à la proposition suivante.

Proposition 1.11 (Correspondance drapeau-réseau). *Pour tout $x \in X(\mathbb{R})$,*

$$\beta_x(x) = \frac{1}{-\chi(Y) - \gamma_x(x)}.$$

La définition de la fonction r_x , et notamment la contrainte $\|\pi^+(v)\| \geq \frac{\|v\|}{2}$ sur le petit vecteur v , rend cette proposition un peu moins simple à appliquer que son analogue pour l'espace projectif. Elle nous sera néanmoins très utile.

1.3 Espaces de réseaux

Dans la correspondance décrite ci-dessus, les réseaux de V_x qui interviennent sont de la forme $gV_x(\mathbb{Z})$, avec $g \in G$. Si on note Γ le stabilisateur de $V_x(\mathbb{Z})$ dans G , l'orbite $G \cdot V_x(\mathbb{Z})$ s'identifie au quotient

$$\Omega = G/\Gamma.$$

Un tel quotient d'un groupe algébrique G semi-simple défini sur \mathbb{Q} par un sous-groupe arithmétique Γ sera appelé un *espace de réseaux*, car il s'identifie à une partie de l'espace des réseaux de l'espace euclidien V_x . La géométrie de ces espaces est décrite avec assez de précision par la théorie de la réduction, due à Borel et Harish-Chandra, et très clairement exposée dans le livre de Borel [8]. Il y est notamment démontré que l'espace Ω est de volume fini pour la mesure de Haar, unique mesure de Radon invariante sous l'action de G , à constante multiplicative près. Les résultats et les méthodes de [8] seront d'ailleurs un outil essentiel dans tout ce mémoire. À chacun des résultats d'approximation diophantienne dans la variété de drapeaux X correspond un théorème sur l'espace de réseaux Ω . Nous décrivons maintenant ces résultats, qui, à notre avis, ont leur intérêt propre.

Mélange exponentiel

Pour démontrer un théorème de Khintchine sur la variété de drapeaux X , nous suivons la méthode proposée par Kleinbock et Margulis [32] et utilisée aussi par Kleinbock et Merrill [36] et Fishman, Kleinbock, Merrill et Simmons [20] dans leur étude des quadriques. Cette méthode est basée sur un théorème de décroissance exponentielle des coefficients dans la représentation $L^2(\Omega)$. Nous admettrons ce résultat, dont la démonstration nous éloignerait trop de notre sujet d'étude, mais en donnons l'énoncé exact ici, puisqu'il sera essentiel dans la suite. L'énoncé général ci-dessous découle d'un article récent de Einsiedler, Margulis, Mohammadi et Venkatesh [18, §§4.1 et 4.3]; on renvoie aussi à Kleinbock et Margulis [32, §3.4] pour une version antérieure.

Théorème 1.12 (Décroissance exponentielle des coefficients dans $L^2(\Omega)$). *Soit G un \mathbb{Q} -groupe semi-simple simplement connexe, Γ un sous-groupe arithmétique, et $\Omega = G/\Gamma$. Soit T un \mathbb{Q} -tore déployé maximal de G , $A = T^0(\mathbb{R})$ et (a_t) un sous-groupe à un paramètre de A . On suppose que $\forall t > 0$, $a_t = e^{tY}$, avec $Y \in \mathfrak{a}$ tel que pour toute projection $p_i : \mathfrak{g} \rightarrow \mathfrak{g}_i$ sur un facteur \mathbb{Q} -simple, $p_i(Y) \neq 0$. Alors, il existe des constantes $\ell \in \mathbb{N}$ et $C, \tau > 0$ telles que pour toutes fonctions $f_1, f_2 \in C^\infty(\Omega)$ et tout $t > 0$,*

$$\left| \int_{\Omega} f_1(a_t \Delta) f_2(\Delta) m_{\Omega}(d\Delta) - m_{\Omega}(f_1) m_{\Omega}(f_2) \right| \leq C e^{-\tau t} \|\Upsilon^{\ell} f_1\|_2 \|\Upsilon^{\ell} f_2\|_2,$$

où Υ désigne l'opérateur différentiel $\Upsilon = 1 - \sum_i Y_i^2$, avec (Y_i) une base orthonormée de l'algèbre de Lie \mathfrak{k} d'un sous-groupe compact maximal de $G(\mathbb{R})$.

L'autre élément utile à la démonstration du théorème de Khintchine est un encadrement asymptotique du volume de l'ensemble Δ des éléments de Ω tels que $r_{\chi}(\Delta) \leq r$. Nous vérifierons cet encadrement à l'aide de la théorie de la réduction, qui décrit un domaine fondamental pour l'action de Γ par translation à droite sur G .

Proposition 1.13 (Mesure d'un voisinage de l'infini). *Il existe des constantes $a_{\chi} > 0$ et $b_{\chi} \in \mathbb{N}^*$ telles que, à une constante multiplicative près dépendant de G et Γ , pour tout $r < 1$,*

$$m_{\Omega}(\{\Delta \in \Omega \mid r_{\chi}(\Delta) \leq r\}) \asymp r^{a_{\chi}} |\log r|^{b_{\chi}-1}.$$

Position dans un espace de réseaux

Si $\Omega = G/\Gamma$ est le quotient d'un \mathbb{Q} -groupe algébrique semi-simple par un sous-groupe arithmétique, nous définissons maintenant une fonction $c : \Omega \rightarrow \mathfrak{a}^-$ qui décrit la position d'un point dans Ω , à une constante près. C'est l'étude du comportement de cette fonction le long des orbites diagonales dans Ω qui permettra de démontrer les résultats d'approximation diophantienne présentés ci-dessus. Dans la construction de la fonction c , l'idée sous-jacente est qu'un élément $g\Gamma$ dans Ω doit s'étudier simultanément dans chacune des représentations fondamentales de G . Cela nous est indiqué par les méthodes de la théorie de la réduction, et en particulier [8, §§14 et 16].

Notons T un \mathbb{Q} -tore déployé maximal dans G , $A = T^0(\mathbb{R})$ la composante connexe des points réels de T , et \mathfrak{a} l'algèbre de Lie de A . Le système de racines Σ

de G par rapport à T s'identifie à un système de racines dans l'espace dual \mathfrak{a}^* . Nous fixons une base de racines simples $\Pi = \{\alpha_1, \dots, \alpha_r\}$ dans Σ et notons $\varpi_1, \dots, \varpi_r$ les poids fondamentaux associés. Pour chaque i , on fixe une \mathbb{Q} -représentation V_i de G engendrée par une unique droite rationnelle de plus haut poids $\omega_i = b_i \varpi_i$, avec $b_i \in \mathbb{N}^*$ minimal, et $V_i(\mathbb{Z})$ un réseau rationnel dans V_i stable par l'action de Γ et contenant un vecteur de plus haut poids e_i . Suivant Borel et Tits [10, §12.13], nous dirons que les représentations V_i , $i = 1, \dots, r$, sont les représentations *fondamentales* de G . Dans l'espace vectoriel V_i , nous noterons $\tilde{X}_i = G \cdot e_i$ l'orbite du vecteur de plus haut poids e_i sous l'action de G .

Les *covolumes successifs* d'un élément $\bar{g} = g\Gamma$ de l'espace de réseaux Ω sont les quantités

$$\mu_i(g) = \min\{\|gv\| \mid v \in V_i(\mathbb{Z}) \cap \tilde{X}_i\}, \quad i = 1, \dots, r.$$

Comme les poids fondamentaux forment une base de \mathfrak{a}^* , il existe un unique élément $c_0(g) \in \mathfrak{a}$ tel que

$$\forall i \in [1, r], \quad \omega_i(c_0(g)) = \log \mu_i(g).$$

Rappelons que la chambre de Weyl négative \mathfrak{a}^- est la partie convexe fermée de \mathfrak{a} définie par

$$\mathfrak{a}^- = \{Y \in \mathfrak{a} \mid \forall \alpha \in \Pi, \alpha(Y) \leq 0\}.$$

L'espace \mathfrak{a} est muni d'une norme euclidienne invariante par l'action du groupe de Weyl, et cela permet de définir la projection $p_{\mathfrak{a}^-} : \mathfrak{a} \rightarrow \mathfrak{a}^-$, qui associe à Y_0 l'unique élément $Y \in \mathfrak{a}^-$ tel que $d(Y_0, \mathfrak{a}^-) = d(Y_0, Y)$. La fonction $c : \Omega \rightarrow \mathfrak{a}^-$ est alors définie par la formule

$$c(g) = p_{\mathfrak{a}^-}(c_0(g)).$$

C'est une fonction propre sur Ω que l'on peut comprendre de la façon suivante : si g_1 et g_2 sont dans la même pointe de Ω , la distance de g_1 à g_2 est comparable à $\|c(g_1) - c(g_2)\|$, à une constante additive près.

Le théorème du sous-espace

Avec les notations utilisées ci-dessus, nous considérons maintenant un sous-groupe à un paramètre (a_t) dans A . Les démonstrations des théorèmes 1.4 et 1.5 sont basées sur le théorème fort du sous-espace de Schmidt [53, Theorem 3A, page 163], grâce auquel nous déterminons un équivalent asymptotique, lorsque t tend vers l'infini, de la fonction $c(a_t s)$, si s appartient à $G(\overline{\mathbb{Q}})$. Pour énoncer ce résultat, il est commode d'introduire la relation d'ordre partiel sur \mathfrak{a} donnée par

$$Y_1 \prec Y_2 \iff \forall i \in [1, r], \quad \omega_i(Y_1) \leq \omega_i(Y_2).$$

Par exemple, si $(Y_j)_{j \in J}$ est une famille d'éléments de \mathfrak{a} , nous noterons $Y = \inf_{j \in J} Y_j$ le plus grand minorant de la famille $(Y_j)_{j \in J}$, défini par

$$\forall i \in [1, r], \quad \omega_i(Y) = \inf_{j \in J} \omega_i(Y_j).$$

Rappelons que pour $Y \in \mathfrak{a}$ et w dans le groupe de Weyl, on note $Y^w = (\text{Ad } w)^{-1}Y$.

Théorème 1.14 (Orbites diagonales des points algébriques dans Ω). *Soient $Y \in \mathfrak{a}^-$ un élément arbitraire, $(a_t) = (e^{tY})$ le sous-groupe à un paramètre associé, et P le sous-groupe parabolique associé à (a_t) :*

$$P = \{g \in G \mid \lim_{t \rightarrow +\infty} a_t g a_{-t} \text{ existe}\}.$$

Pour $w \in W_P$, nous notons $X_w = \overline{PwB}$ la variété de Bruhat standard correspondante. Étant donné $s \in G(\mathbb{Q})$ posons

$$c_\infty = \inf\{p_{\mathfrak{a}^-}(Y^w) ; w \in W_P : \exists \gamma \in G(\mathbb{Q}) : s \in X_w\gamma\} \in \mathfrak{a}^-.$$

Alors,

$$\lim_{t \rightarrow +\infty} \frac{1}{t} c(a_t s) = c_\infty$$

et il existe une variété de Bruhat⁴ rationnelle $X_w\gamma$, $w \in W_P$, $\gamma \in G(\mathbb{Q})$ contenant x et telle que $p_{\mathfrak{a}^-}(Y^w) = c_\infty$.

En fait, la démonstration de ce théorème permet aussi de contrôler partiellement l'élément $\gamma_t \in G(\mathbb{Q})$ qui apparaît pour $t > 0$ grand dans une décomposition de Siegel $a_t s = k_t b_t n_t \gamma_t$. Nous renvoyons au chapitre 5, théorème 5.1.1 pour un énoncé précis.

Non divergence quantitative

Le dernier résultat dont nous aurons besoin sur l'espace de réseaux Ω est un énoncé de non divergence quantitative : étant donnée une mesure borélienne μ sur G on cherche à contrôler la valeur de $c(g)$ lorsque l'élément g est choisi aléatoirement suivant la mesure μ . C'est pour étudier le comportement des flots unipotents dans l'espace $\mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z})$ que ce type de résultat a été introduit par Margulis [44]. Ensuite, les travaux de Dani [14], puis de Kleinbock et Margulis [31] ont permis d'aboutir à un énoncé quantitatif adapté à l'approximation diophantienne. Mais les théorèmes montrés par Kleinbock et Margulis, ou plus récemment par Lindentrauss, Margulis, Mohammadi et Shah [42] ne concernent que le groupe SL_d . Pour les applications que nous avons en vue, il est important d'avoir un résultat qui s'applique dans un \mathbb{Q} -groupe semi-simple arbitraire, et qui en respecte la géométrie. Ici encore, c'est la fonction $c : G \rightarrow \mathfrak{a}^-$ qui permet de formuler l'énoncé adéquat.

Nous aurons même besoin d'étendre la fonction c aux parties compactes de G . Si $S \subset G$ est une partie compacte, on pose donc, pour chaque $i \in [1, r]$,

$$\mu_i(S) = \min_{v \in V_i(\mathbb{Z}) \cap \tilde{X}_i} \max_{s \in S} \|sv\|.$$

Cela permet de définir un élément $c_0(S) \in \mathfrak{a}$ par

$$\forall i \in [1, r], \omega_i(c_0(S)) = \log \mu_i(S),$$

puis, comme précédemment,

$$c(S) = p_{\mathfrak{a}^-}(c_0(S)).$$

Dans toute la suite, le groupe G est muni d'une métrique riemannienne arbitraire. Si μ est une mesure borélienne sur G , U un ouvert de G , et $C, \alpha > 0$ deux constantes, nous dirons qu'une fonction mesurable $f : U \rightarrow \mathbb{R}$ est (C, α) -régulière sur U si pour toute boule $B = B(x, r) \cap U$ de U centrée en $x \in \mathrm{Supp} \mu$, et pour tout $\varepsilon > 0$,

$$\mu(\{g \in B \mid |f(g)| \leq \varepsilon \|f\|_{B, \mu}\}) \leq C \varepsilon^\alpha \mu(B),$$

⁴Une variété de la forme $X_w\gamma$ sera dite variété de Bruhat si elle est vue comme une partie de G , et variété de Schubert si elle est vue comme une partie de $X = P \backslash G$.

où l'on note

$$\|f\|_{B,\mu} = \sup\{|f(y)| ; y \in B \cap \text{Supp } \mu\}.$$

Nous montrerons le théorème suivant.

Théorème 1.15 (Non divergence quantitative dans G). *Étant données deux constantes $C_0, \alpha_0 > 0$, il existe $C, \alpha > 0$ tels qu'on ait la propriété suivante.*

Soit μ une mesure de Radon sur G et $B(x, \rho) \subset G$ une boule satisfaisant

$$\forall i \in [1, r], \forall v \in \tilde{X}_i \cap V_i(\mathbb{Z}), g \mapsto \|gv\| \text{ est } (C_0, \alpha_0)\text{-régulière sur } B(x, 5\rho) \text{ pour } \mu.$$

Alors, pour tout $\varepsilon > 0$, notant $S = \text{Supp } \mu \cap B(x, \rho)$,

$$\mu(\{g \in B(x, \rho) \mid \|c(g) - c(S)\| \geq -\log \varepsilon\}) \leq C\varepsilon^\alpha \mu(B(x, \rho)).$$

Pour l'approximation diophantienne dans les sous-variétés, ce théorème jouera un rôle analogue à celui du théorème du sous-espace de Schmidt pour l'approximation diophantienne des points algébriques, et nous permettra notamment de démontrer les deux résultats ci-dessous. Nous dirons qu'une mesure borélienne sur G est *localement régulière* en un point s_0 dans G s'il existe une boule ouverte $B = B(s_0, r)$ et des constantes $C, \alpha > 0$ telles que

$$\begin{aligned} \forall i \in [1, r], \forall v \in \tilde{X}_i \cap V_i(\mathbb{Z}), \forall g \in G, \\ s \mapsto \|gsv\| \text{ est } (C, \alpha)\text{-régulière sur } B \text{ pour } \mu. \end{aligned}$$

Théorème 1.16 (Orbites diagonales partant d'une mesure régulière). *Soit $(a_t)_{t>0}$ un sous-groupe à un paramètre dans A , et μ une mesure sur G localement régulière en s_0 . Il existe une boule ouverte B centrée en s_0 telle que pour μ -presque tout $s \in B$, notant $S = B \cap \text{Supp } \mu$,*

$$\lim_{t \rightarrow +\infty} \frac{1}{t} (c(a_t s) - c(a_t S)) = 0.$$

En d'autres termes, au voisinage de s_0 , du point de vue de la fonction c , presque toutes les orbites suivent le même comportement asymptotique, qui ne dépend que du support de μ au voisinage de s_0 . Si S est un ensemble algébrique irréductible de dimension m dans G , on le munit de sa mesure de Lebesgue μ , qui n'est autre que la restriction à S de la mesure de Hausdorff de dimension m . En tout point non singulier de S , la mesure μ est localement régulière, et cela permet d'appliquer le théorème ci-dessus. Dans le cas où l'ensemble algébrique S est défini sur $\overline{\mathbb{Q}}$, nous pourrions même montrer, à l'aide de nos résultats sur les nombres algébriques, que l'expression $\frac{1}{t}c(a_t S)$ converge lorsque t tend vers l'infini, et en déduire le résultat suivant.

Théorème 1.17 (Orbites diagonales et ensembles algébriques). *Soient $Y \in \mathfrak{a}^-$ un élément arbitraire, $(a_t) = (e^{tY})$ le sous-groupe à un paramètre associé, et P le sous-groupe parabolique associé à (a_t) :*

$$P = \{g \in G \mid \lim_{t \rightarrow +\infty} a_t g a_{-t} \text{ existe}\}.$$

Pour $w \in W_P$, nous notons $X_w = \overline{PwB}$ la variété de Bruhat standard correspondante. Étant donné un ensemble algébrique irréductible S dans G défini sur $\overline{\mathbb{Q}}$, posons

$$c_\infty = \inf\{p_{\mathfrak{a}^-}(Y^w) ; w \in W_P : \exists \gamma \in G(\overline{\mathbb{Q}}) : S \subset X_w \gamma\} \in \mathfrak{a}^-.$$

Alors, pour presque tout s dans S ,

$$\lim_{t \rightarrow +\infty} \frac{1}{t} c(a_t s) = c_\infty.$$

et il existe une variété de Bruhat rationnelle $X_w \gamma$, $w \in W_P$, $\gamma \in G(\mathbb{Q})$ contenant S et telle que $p_{\mathfrak{a}^-}(Y^w) = c_\infty$.

Ici encore, on renvoie au théorème 7.4.1 pour un énoncé plus précis. C'est à l'aide de ce dernier résultat que nous démontrerons le théorème 1.9.

Chapitre 2

Une correspondance

Dans tout ce chapitre, nous considérerons une variété de drapeaux X , obtenue comme un espace quotient $X = P \backslash G$ d'un \mathbb{Q} -groupe semi-simple G par un \mathbb{Q} -sous-groupe parabolique P . Après avoir défini des hauteurs et des distances sur X , nous définirons l'exposant diophantien d'un point de X , que nous mettrons en relation avec le comportement asymptotique de certaines orbites dans l'espace des réseaux d'une représentation rationnelle bien choisie de G .

2.1 Hauteurs

Quitte à remplacer G par son revêtement universel, nous pouvons supposer sans perte de généralité que le groupe G est simplement connexe. Fixons dans G un \mathbb{Q} -sous-groupe parabolique minimal $B \subset P$, et $T \subset B$ un sous-tore \mathbb{Q} -déployé maximal. Le choix de B induit un ordre sur le groupe $X^*(T)$ des caractères de T , et donc une base Π du système de racines associé à G et T . Pour la théorie générale des représentations rationnelles de G , on renvoie à Borel et Tits [10, §12].

Pour définir une hauteur sur $X = P \backslash G$, nous partirons d'une \mathbb{Q} -représentation linéaire à gauche

$$\rho : G \rightarrow \mathrm{GL}(V_\chi)$$

engendrée par un unique vecteur $e_\chi \in V_\chi(\mathbb{Q})$ de plus haut poids χ . On suppose en outre que si $[e_\chi] \in \mathbb{P}(V)$ est la direction engendrée par e_χ , alors

$$\mathrm{Stab}_G[e_\chi] = P.$$

La variété $X = P \backslash G$ s'identifie naturellement à l'orbite de la droite $[e_\chi]$ dans l'espace projectif $\mathbb{P}(V)$ via l'application

$$\begin{aligned} \iota : X &\rightarrow \mathbb{P}(V) \\ Pg &\mapsto g^{-1}[e_\chi], \end{aligned}$$

et comme cette identification préserve les points rationnels, cela permet de définir la hauteur H_χ sur X , par restriction. Plus précisément, ayant fixé une base rationnelle $(u_i)_{1 \leq i \leq d}$ de V et une norme euclidienne sur V pour laquelle cette base est orthonormée, on définit une hauteur sur $\mathbb{P}(V)$ par la formule

$$H(u) = \|\mathbf{u}\|,$$

où \mathbf{u} est un représentant primitif de u dans le réseau $\bigoplus_{1 \leq i \leq d} \mathbb{Z}u_i$, et la hauteur sur X est alors donnée par

$$H_\chi(v) = H(\iota_\chi(v)).$$

Pour les variétés de drapeaux munies d'une hauteur comme ci-dessus, on dispose d'un équivalent asymptotique pour le nombre de points de hauteur bornée. Cela a été observé en premier lieu par Schanuel [49] pour l'espace projectif, puis démontré par Franke [21] pour une variété de drapeaux X munie de la hauteur anti-canonique. La version générale que nous citons ici est due à Mohammadi et Salehi Golsefidy [46, Theorem 4].

Théorème 2.1.1 (Nombre de points rationnels de hauteur bornée). *Soit X une variété de drapeaux définie sur \mathbb{Q} , munie d'une hauteur H_χ associée au poids dominant χ . Il existe des constantes $c, u_\chi > 0$ et $v_\chi \in \mathbb{N}^*$ telles que la quantité*

$$N_\chi(T) = \text{card}\{v \in X(\mathbb{Q}) \mid H_\chi(v) \leq T\}$$

vérifie

$$N_\chi(T) \sim c \cdot T^{u_\chi} (\log T)^{v_\chi - 1} \quad \text{lorsque } T \text{ tend vers } +\infty.$$

Les constantes u_χ et v_χ sont facilement calculables à l'aide d'un système de racines associé à G , comme expliqué dans [46].

2.2 Distance de Carnot-Carathéodory

Nous fixons maintenant un point réel x de $X = P \backslash G$, et expliquons comment évaluer la distance à x d'une approximation v . La distance pour laquelle nous pourrions obtenir des résultats satisfaisants sur les exposants diophantiens est une distance de Carnot-Carathéodory, qui n'est pas riemannienne en général, sauf si le radical unipotent de P est abélien.

Soit T un sous-tore \mathbb{Q} -déployé maximal de G inclus dans P . L'algèbre de Lie \mathfrak{g} se décompose sous l'action de T en sous-espaces de racines :

$$\mathfrak{g} = \mathfrak{z} \oplus \left(\bigoplus_{\alpha \in \Sigma} \mathfrak{g}_\alpha \right),$$

où

$$\mathfrak{z} = \{u \in \mathfrak{g} \mid \forall t \in T, (\text{Ad } t)u = u\}$$

et

$$\mathfrak{g}_\alpha = \{u \in \mathfrak{g} \mid \forall t \in T, (\text{Ad } t)u = \alpha(t)u\}.$$

D'après [8, §11.7], si Π est une base du système de racines Σ , il existe une partie $\theta \subset \Pi$ telle que l'algèbre de Lie \mathfrak{p} du sous-groupe parabolique P s'écrive

$$\mathfrak{p} = \mathfrak{z} \oplus \left(\bigoplus_{\alpha \in \Sigma^+ \cup \langle \theta \rangle^-} \mathfrak{g}_\alpha \right),$$

où Σ^+ désigne l'ensemble des racines positives, et $\langle \theta \rangle^- \subset \Sigma$ l'ensemble des racines négatives qui s'écrivent

$$\alpha = - \sum_{\beta \in \theta} n_\beta \beta, \quad n_\beta \in \mathbb{N}.$$

L'algèbre de Lie \mathfrak{u}^- du sous-groupe unipotent U^- opposé à P se décompose en somme directe

$$\mathfrak{u}^- = \bigoplus_{i \geq 1} m_i,$$

où m_i est la somme de tous les espaces de racines \mathfrak{g}_α , où $-\alpha$ est une racine positive contenant exactement i éléments hors de θ dans sa décomposition en racines simples, avec multiplicité. La proposition suivante peut se vérifier au cas par cas pour chaque système de racines, en utilisant les tables de Bourbaki [11, planches I à IX]; la démonstration plus conceptuelle incluse ci-dessous provient de la thèse de doctorat de Sébastien Miquel, et nous a été communiquée par Yves Benoist.

Proposition 2.2.1 (Stratification de \mathfrak{u}^-). *La décomposition $\mathfrak{u}^- = \bigoplus_{i \geq 1} m_i$ est une stratification de \mathfrak{u}^- , i.e. pour chaque i ,*

$$[m_1, m_i] = m_{i+1}.$$

Démonstration. Si $X \in \mathfrak{g}_\alpha$ et $Y \in \mathfrak{g}_\beta$, alors $[X, Y] \in \mathfrak{g}_{\alpha+\beta}$, donc pour tout i , $[m_1, m_i] \subset m_{i+1}$. Pour l'inclusion réciproque, supposons tout d'abord que le groupe est déployé sur \mathbb{Q} , de sorte que si α, β sont deux racines telles que $\alpha + \beta \in \Sigma$ est non nulle, alors $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] = \mathfrak{g}_{\alpha+\beta}$. Soit $i \geq 2$ et β une racine contenant i racines simples hors de θ ; on veut voir que $\mathfrak{g}_\beta \subset [m_1, m_{i-1}]$. D'après [54, chapitre 5, §9, proposition 5, page 32] on peut décomposer β en somme de racines simples

$$\beta = \alpha_1 + \cdots + \alpha_k$$

de sorte que pour chaque i , $\alpha_1 + \cdots + \alpha_i$ soit une racine. Montrons par récurrence sur $k \geq i$ que

$$\mathfrak{g}_\beta \subset [m_1, m_{i-1}].$$

Le résultat est clair pour $k = i$, car alors pour tout $j \in [1, k]$, $\alpha_j \notin \theta$, et par suite $\mathfrak{g}_\beta = [\mathfrak{g}_{\alpha_1}, \mathfrak{g}_{\alpha_2 + \cdots + \alpha_k}] \subset [m_1, m_{i-1}]$. Supposons donc $k > i$. Si $\alpha_k \notin \theta$, on a ce qu'on veut : avec $\beta' = \alpha_1 + \cdots + \alpha_{k-1}$, on a $\beta = \beta' + \alpha_k$ et donc $\mathfrak{g}_\beta = [\mathfrak{g}_{\alpha_k}, \mathfrak{g}_{\beta'}] \subset [m_1, m_{i-1}]$. Si $\alpha_k \in \theta$, l'hypothèse de récurrence sur k permet d'écrire

$$\mathfrak{g}_{\beta'} \subset [m_1, m_{i-1}].$$

Par conséquent

$$\mathfrak{g}_\beta = [\mathfrak{g}_{\beta'}, \mathfrak{g}_{\alpha_k}] \subset [[m_1, m_{i-1}], \mathfrak{g}_{\alpha_k}] \subset [[m_1, \mathfrak{g}_{\alpha_k}], m_{i-1}] + [m_1, [m_{i-1}, \mathfrak{g}_{\alpha_k}]].$$

Comme $\alpha_k \in \theta$, $[m_1, \mathfrak{g}_{\alpha_k}] \subset m_1$ et $[m_{i-1}, \mathfrak{g}_{\alpha_k}] \subset m_{i-1}$ et donc

$$\mathfrak{g}_\beta \subset [m_1, m_{i-1}] + [m_1, m_{i-1}].$$

Si G n'est pas déployé sur \mathbb{Q} , on remplace \mathbb{Q} par le corps algébriquement clos \mathbb{C} , sur lequel G est déployé. Soit alors T' un tore maximal contenant T , et Σ' le système de racines associé à G et T' . Le système de racines Σ de G par rapport à T s'obtient à partir de Σ' par restriction à T . Fixons un ordre sur Σ' compatible avec l'ordre choisi sur Σ , i.e. tel que la projection d'une racine positive est positive, et notons Π' la base associée à cet ordre. D'après [10, proposition 6.8] les éléments de Π' sont envoyés par restriction à T sur $\Pi \cup \{0\}$. Soit $\theta' \subset \Pi'$ l'image réciproque de $\theta \cup \{0\}$. Sur \mathbb{C} , et pour le tore T' , le sous-groupe parabolique P est associé à la partie $\theta' \subset \Pi'$ et l'on vérifie facilement que la filtration de \mathfrak{u}^- est aussi construite comme ci-dessus, à partir de θ' . Le résultat découle donc du cas où G est déployé. \square

L'espace vectoriel $m_1 \leq \mathfrak{u}^-$ s'identifie naturellement à un sous-espace de l'espace tangent à $X = P \backslash G$ au point base P ; ce sous-espace est invariant par l'action du stabilisateur P du point base. Nous dirons qu'un chemin $\gamma : [0, 1] \rightarrow X$ est *horizontal* si pour tout t dans $[0, 1]$,

$$\gamma'(t) \cdot s(\gamma(t))^{-1} \in m_1,$$

où $s(x)$ désigne un élément de G tel que $x = Ps(x)$. Comme m_1 est invariant par P , cette notion ne dépend pas du choix de l'élément $s(x)$. Nous noterons \mathcal{H} l'ensemble des chemins horizontaux. Ayant fixé un sous-groupe compact maximal $K \subset G$ et une norme euclidienne sur m_1 invariante sous l'action de $K \cap P$, on définit la *longueur* d'un chemin horizontal γ par la formule

$$\ell(\gamma) = \int_0^1 \|\gamma'(t) \cdot s(\gamma(t))^{-1}\| dt,$$

où cette fois l'élément $s(\gamma(t))$ tel que $\gamma(t) = Ps(\gamma(t))$ est choisi dans K .

Définition 2.2.2 (Distance de Carnot-Carathéodory sur $P \backslash G$). On définit une distance sous-riemannienne sur X par la formule

$$d(x, y) = \inf\{\ell(\gamma) ; \gamma \in \mathcal{H} \text{ tel que } \gamma(0) = x \text{ et } \gamma(1) = y\}.$$

Remarque. La distance de Carnot-Carathéodory que nous avons construite dépend du choix du sous-groupe compact maximal K . Mais toutes les distances construites de cette manière sont équivalentes, et pour les problèmes d'approximation diophantienne que nous étudierons, ce choix n'aura donc pas d'importance.

D'après le théorème de Chow [25, Theorem 0.4] cette formule définit bien une distance sur X , et la topologie associée est équivalente à la topologie usuelle sur X . De plus, vue notre construction, cette distance est K -invariante. Remarquons aussi que tout élément g dans G agit sur X en préservant les chemins horizontaux; par conséquent, g induit une transformation bi-lipschitzienne de X , muni de la métrique de Carnot-Carathéodory. Pour comprendre la géométrie associée à la distance d , on peut s'aider de la carte locale

$$\begin{array}{ccc} U^- & \rightarrow & X \\ s & \mapsto & P \cdot s \end{array}$$

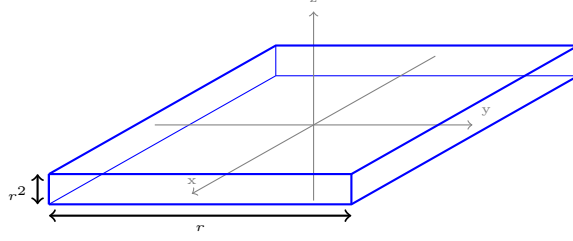
Si U^- est muni de la distance de Carnot-Carathéodory [41, §3.3, page 79] associée à la stratification $\mathfrak{u}^- = m_1 \oplus \dots \oplus m_r$, cette carte est localement bi-lipschitzienne. On définit ensuite une quasi-norme sur \mathfrak{u}^- par la formule

$$|x| = \max_{1 \leq i \leq r} \|x_i\|^{\frac{1}{i}},$$

où $x = \sum_i x_i$ est la décomposition de x suivant la stratification de \mathfrak{u}^- , et $\|\cdot\|$ désigne une norme arbitraire fixée sur \mathfrak{u}^- . Pour $r > 0$, nous noterons

$$B_{\mathfrak{u}^-}(0, r) = \{u \in \mathfrak{u}^- \mid |u| \leq r\}.$$

La figure ci-dessous représente la boule $B_{\mathfrak{u}^-}(0, r)$ pour $r > 0$ petit, lorsque U^- est le groupe de Heisenberg de dimension 3, identifié à l'espace \mathbb{R}^3 muni de l'opération $(x, y, z) * (x', y', z') = (x + x', y + y', z + z' + xy')$.

FIGURE 2.1 : Boule de rayon $r > 0$ pour $U^- = \text{Heisenberg}(3)$

La proposition ci-dessus permet de comparer les boules de rayon $r > 0$ pour la distance de Carnot-Carathéodory sur X à des boules pour la quasi-norme $|\cdot|$ associée à la stratification de \mathfrak{u}^- . En anglais, cet énoncé est souvent appelé « Ball-box Theorem » ce qui résume bien son contenu.

Proposition 2.2.3 (Ball-box Theorem). *Soit $x \in X$ et $s_x \in G$ tel que $x = Ps_x$. Il existe une constante $C > 0$ telle que pour tout $r > 0$ suffisamment petit,*

$$P \exp(B_{\mathfrak{u}^-}(0, \frac{r}{C})) \cdot s_x \subset B(x, r) \subset P \exp(B_{\mathfrak{u}^-}(0, Cr)) \cdot s_x.$$

Démonstration. Comme l'application $y \mapsto ys_x$ est bi-lipschitzienne sur X , il suffit de vérifier la proposition pour le point $x = P$. Vue l'équivalence locale des distances de Carnot-Carathéodory sur X et sur U^- , il suffit de démontrer le résultat analogue sur U^- . On définit une famille de dilatations $\delta_t : \mathfrak{u}^- \rightarrow \mathfrak{u}^-$ par $\delta_t(\sum x_i) = \sum t^i x_i$. C'est un sous-groupe à un paramètre d'automorphismes de \mathfrak{u}^- , qui induit donc un sous-groupe à un paramètre d'automorphismes de U^- , toujours noté δ_t . Comme δ_t préserve les chemins horizontaux et dilate la norme sur m_1 par un facteur t , on a pour tous x et y , $d(\delta_t(x), \delta_t(y)) = td(x, y)$. Par conséquent,

$$B(1, r) = \delta_r(B(1, 1)) = \exp(\delta_r(B_{\mathfrak{u}^-}(0, 1))) = \exp(B_{\mathfrak{u}^-}(0, r)).$$

□

Pour deviner par un argument heuristique la valeur presque sûre de l'exposant diophantien d'un point de X (cf. paragraphe suivant), il est utile de connaître le nombre de recouvrement de X par des boules de petit rayon $r > 0$ pour la métrique de Carnot-Carathéodory.

Proposition 2.2.4 (Dimension de Carnot-Carathéodory). *Le nombre de recouvrement de X à l'échelle $\delta > 0$ est*

$$N(X, \delta) \asymp \delta^{-\dim_{cc} X}.$$

où $\dim_{cc} X$ est la dimension de X pour la distance d , égale à

$$\dim_{cc} X = \sum_{i \geq 1} i \dim m_i.$$

Démonstration. Cette formule découle de la proposition précédente, qui décrit la forme des boules de rayon r pour la métrique d sur X . □

Remarque. Les méthodes développées dans ce mémoire permettent de traiter des quasi-distances un peu plus générales : on peut partir d'une quasi-norme sur $\mathfrak{p}\backslash\mathfrak{g}$ homogène pour un sous-groupe diagonal à un paramètre $a_t = e^{tY}$ dans P . Mais l'avantage de la métrique de Carnot-Carathéodory est que le drapeau associé dans $\mathfrak{p}\backslash\mathfrak{g}$ est invariant par P , ce qui fait que l'on obtient bien une distance sur $X = P\backslash G$. Dans le cadre de l'espace projectif, les quasi-distances sont utilisées dans [2] pour étudier l'approximation diophantienne dans les groupes nilpotents ; on obtient ainsi des résultats d'approximation diophantienne pour des quasi-normes dans \mathbb{R}^d .

2.3 L'espace des réseaux

Soit V un espace vectoriel euclidien, isomorphe à \mathbb{R}^d , $d \in \mathbb{N}^*$. Un *réseau* dans V est un sous-groupe discret de rang maximal, égal à $\dim V$. Pour décrire la forme d'un réseau Δ , on définit la suite de ses *minima successifs*

$$\lambda_1(\Delta) \leq \lambda_2(\Delta) \leq \dots \leq \lambda_d(\Delta)$$

par

$$\forall i \in [1, d], \quad \lambda_i(\Delta) = \inf\{\lambda > 0 \mid \text{rang}(B(0, \lambda) \cap \Delta) \geq i\},$$

où, pour $E \subset V$, on note $\text{rang}(E)$ le rang linéaire de E , i.e. le cardinal maximal d'une famille libre d'éléments de E . On définit aussi le *covolume* de Δ dans \mathbb{R}^d , noté $\text{covol}(\Delta)$, comme le volume d'un domaine fondamental de \mathbb{R}^d sous l'action de Δ . Le second théorème de Minkowski [45] relie les minima successifs d'un réseau et son covolume. Il sera d'une importance capitale dans la suite ce mémoire.

Théorème 2.3.1 (Second théorème de Minkowski). *Soit $d \in \mathbb{N}^*$ et Δ un réseau dans \mathbb{R}^d . Alors,*

$$\frac{2^d}{d!} \text{covol}(\Delta) \leq \lambda_1(\Delta) \dots \lambda_d(\Delta) \leq 2^d \text{covol}(\Delta).$$

Soit maintenant X une variété de drapeaux, obtenue comme un quotient $X = P\backslash G$ d'un \mathbb{Q} -groupe semi-simple G par un sous-groupe parabolique P . Nous fixons une \mathbb{Q} -représentation V_χ de G engendrée par un vecteur rationnel de plus haut poids e_χ tel que

$$\forall p \in P, \quad p \cdot e_\chi = \chi(p)e_\chi.$$

Cela permet en particulier de définir une hauteur H_χ comme expliqué au paragraphe 2.1. On munit aussi V_χ d'une norme euclidienne. Pour l'étude de l'approximation diophantienne dans X , en plus des minima successifs, nous devons définir une certaine fonction r_χ sur l'espace des réseaux de V_χ . Ayant fixé un sous-tore \mathbb{Q} -déployé maximal T dans P , l'espace V_χ se décompose en somme directe d'espaces de poids. Soit

$$\pi^+ : V_\chi \rightarrow \mathbb{R}e_\chi$$

la projection parallèlement à la somme des espaces de poids distincts de $\mathbb{R}e_\chi$. Notons aussi

$$\tilde{X} = G \cdot e_\chi$$

le cône dans V_χ engendré par $\iota(X)$, privé du point 0. Pour $r > 0$, on considère la partie suivante de V_χ :

$$C_r = \{\mathbf{v} \in \tilde{X} \mid \|\mathbf{v}\| \leq r \text{ et } \|\pi^+(\mathbf{v})\| > \frac{\|\mathbf{v}\|}{2}\}.$$

Remarque. Dans cette définition le choix de la constante $\frac{1}{2}$ dans l'inégalité $\|\pi^+(\mathbf{v})\| > \frac{\|\mathbf{v}\|}{2}$ est arbitraire. La correspondance que nous mettrons en évidence ci-dessous à la proposition 2.4.4 est encore valable si l'on remplace cette condition par $\|\pi^+(\mathbf{v})\| > c\|\mathbf{v}\|$, pour une constante $c > 0$ arbitraire.

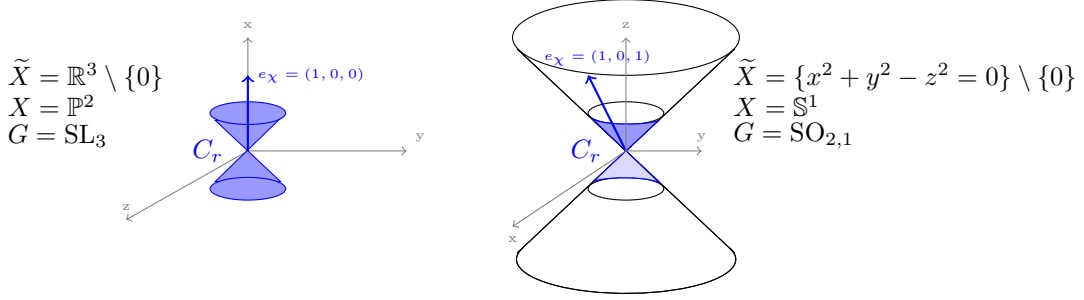


FIGURE 2.2 : L'ensemble C_r pour $X = \mathbb{P}^2$ et $X = \mathbb{S}^1$

Définition 2.3.2 (La fonction r_χ). Si Δ est un réseau de V_χ , on pose

$$r_\chi(\Delta) = \inf\{r > 0 \mid C_r \cap \Delta \neq \{0\}\} \in \mathbb{R} \cup \{+\infty\}.$$

Remarque. Attention! Les parties C_r ne sont pas convexes, et leur volume est nul en général, car $C_r \subset \tilde{X}$. Il n'est donc pas question d'appliquer ici le premier théorème de Minkowski, et il est d'ailleurs facile de construire un réseau Δ dans V_χ tel que $r_\chi(\Delta) = \infty$.

2.4 L'exposant diophantien

Pour chaque choix de hauteur H_χ sur la variété de drapeaux X , nous définissons un exposant diophantien β_χ sur X , que nous interprétons ensuite en termes d'orbites diagonales dans l'espace des réseaux de la représentation V_χ de plus haut poids χ .

Définition 2.4.1. L'exposant diophantien d'un point $x \in X$ pour la distance d de Carnot-Carathéodory est

$$\beta_\chi(x) = \inf\{\beta > 0 \mid \exists c > 0 : \forall v \in X(\mathbb{Q}), d(x, v) \geq c.H_\chi(v)^{-\beta}\}.$$

Exercice 1 (Minoration uniforme de l'exposant diophantien). Le but de cet exercice est de minorer l'exposant diophantien d'un point x arbitraire dans $X(\mathbb{R})$, grâce à la projection stéréographique $\begin{matrix} \mathfrak{u}^- & \rightarrow & X \\ u & \mapsto & Pe^u. \end{matrix}$ On fixe un réseau rationnel $\mathfrak{u}^-(\mathbb{Z})$ dans l'algèbre de Lie \mathfrak{u}^- .

1. Pour $u \in \mathfrak{u}^-$ irrationnel, montrer qu'il existe une infinité de rationnels $\frac{\mathbf{p}}{q} \in \mathfrak{u}^-(\mathbb{Q})$, où $\mathbf{p} \in \mathfrak{u}^-(\mathbb{Z})$ et $q \in \mathbb{N}^*$ tels que $\left|u - \frac{\mathbf{p}}{q}\right| \ll q^{-\frac{1+\dim X}{\dim_{cc} X}}$.
2. Si $x = e^u$, vérifier que $d(x, Pe^{\frac{\mathbf{p}}{q}}) \asymp d(P, e^{\frac{\mathbf{p}}{q}}e^{-u}) \ll \left|u - \frac{\mathbf{p}}{q}\right|$.

3. Justifier que l'application $u^- \rightarrow V_\chi$; $u \mapsto e^{-u}e_\chi$ est polynomiale; on note d_χ son degré.
4. Montrer que pour tout $x \in X(\mathbb{R})$, $\beta_\chi(x) \geq \frac{1+\dim X}{d_\chi \dim_{cc} X}$.
5. Si $X = \text{Grass}(\ell, d)$ est une variété grassmannienne, munie de la hauteur associée au plongement de Plücker $X \hookrightarrow \mathbb{P}(\wedge^\ell \mathbb{R}^d)$, montrer que pour tout $x \in X(\mathbb{R})$, $\beta_\chi(x) \geq \frac{1}{\ell} + \frac{1}{\ell(d-\ell) \min(\ell, d-\ell)}$.

Suivant la méthode introduite par Dani [13], et exploitée ensuite avec succès par divers auteurs, notamment Kleinbock et Margulis [31, 33], nous voulons traduire les propriétés diophantiennes d'un point $x \in X = P \backslash G$ en termes d'orbites diagonales dans l'espace des réseaux de V_χ . Pour cela, nous fixons dans V_χ un réseau rationnel $V_\chi(\mathbb{Z})$, et si $x = Ps_x$ est un élément de X , nous lui associons le réseau

$$\Delta_x = s_x V_\chi(\mathbb{Z}).$$

Par ailleurs, ayant fixé un sous-tore \mathbb{Q} -déployé maximal $T \subset P$, nous noterons $A = T^0(\mathbb{R})$ la composante neutre de ses points réels, et \mathfrak{a} l'algèbre de Lie de A . Rappelons que l'on note Π une base du système de racines de G pour T , et $\theta \subset \Pi$ la partie associée au sous-groupe parabolique P , telle que toutes les racines négatives de P se décomposent en éléments de θ . On définit alors un sous-groupe diagonal (a_t) à un paramètre dans G en posant

$$a_t = e^{tY} \quad \text{où } Y \in \mathfrak{a} \text{ est défini par } \alpha(Y) = \begin{cases} 0 & \text{si } \alpha \in \theta \\ -1 & \text{si } \alpha \notin \theta. \end{cases} \quad (2.1)$$

Ce flot est choisi de sorte que la quasi-norme sur u^- définie au paragraphe ci-dessus satisfasse la propriété d'homogénéité suivante.

Lemme 2.4.2. *Pour tout $t \in \mathbb{R}$ et tout $u \in u^-$,*

$$|(\text{Ad } a_t)u| = e^t |u|.$$

Démonstration. Écrivons $u = \sum_{i \geq 1} u_i$ suivant la décomposition en somme directe $u^- = m_1 \oplus \dots \oplus m_s$. Comme $\text{Ad } a_t = e^{t \text{ad } Y}$, cette décomposition est préservée par $\text{Ad } a_t$ et de plus, vue la définition de Y , pour chaque i , $(\text{Ad } a_t)u_i = e^{it}u_i$. Avec la formule $|u| = \max_{1 \leq i \leq s} \|u_i\|^{\frac{1}{i}}$, on trouve ce qu'on veut. \square

Définition 2.4.3 (Taux de fuite dans l'espace des réseaux de V_χ). *Le taux de fuite du réseau $\Delta_x = s_x V_\chi(\mathbb{Z})$ sous l'action de (a_t) est*

$$\gamma_\chi(x) = \liminf_{t \rightarrow \infty} \frac{-1}{t} \log r_\chi(a_t \Delta_x)$$

Remarque. Ce taux de fuite ne dépend pas du choix de l'élément s_x tel que $x = Ps_x$, car pour tout $p \in P$, l'élément $a_t p a_t^{-1}$ converge vers $p_\infty \in P$ lorsque t tend vers l'infini. En effet, $p_\infty e_\chi = \chi(p_\infty) e_\chi$, donc si $\|a_t \mathbf{v}\| \leq e^{-\gamma t}$ et $\|\pi^+(a_t \mathbf{v})\| \geq \frac{\|a_t \mathbf{v}\|}{2}$ alors $\|a_t p \mathbf{v}\| \leq C e^{-\gamma t}$ et $\|\pi^+(a_t p \mathbf{v})\| \geq \frac{\|a_t p \mathbf{v}\|}{2C}$, où C est une constante qui dépend de p_∞ . En suite, prenant $t' = t - C$, avec $C > 0$ suffisamment grand, comme la direction e_χ est plus contractée que les autres par un facteur exponentiel, on trouve $\|\pi^+(a_{t'} p \mathbf{v})\| \geq \frac{\|a_{t'} p \mathbf{v}\|}{2}$ et $\|a_{t'} p \mathbf{v}\| \leq C' e^{-\gamma t}$.

Remarque. Il existe une constante $c = c_x > 0$ telle que pour tout \mathbf{v} non nul dans Δ_x , $\|\mathbf{v}\| \geq c$. Par suite, pour tout $t > 0$, tout vecteur \mathbf{v} non nul de $a_t \Delta_x$ satisfait $\|\mathbf{v}\| \geq ce^{t\chi(Y)}$, ce qui montre que pour tout x , $\gamma_\chi(x) \leq -\chi(Y)$. Cette majoration est optimale, comme le montre le cas $s_x = 1$. Il semble beaucoup plus difficile de déterminer la borne inférieure optimale de γ_χ sur X . Toutefois, l'exercice 1 ci-dessus montre que pour tout x , $\beta_\chi(x) \geq \frac{1+\dim X}{d_x \dim_{cc} X} > 0$. Avec la proposition 2.4.4 ci-dessous, cela implique que $\gamma_\chi(x)$ est uniformément minorée sur X , ce qui n'était pas évident a priori.

Dans son article [13], Dani formule en termes dynamiques la correspondance entre les propriétés diophantiniennes d'un point x de l'espace projectif $\mathbb{P}^{d-1}(\mathbb{R})$ et le comportement d'une orbite diagonale $(a_t s_x \mathbb{Z}^d)_{t>0}$ dans l'espace des réseaux de \mathbb{R}^d : les bonnes approximations rationnelles de x correspondent aux petits vecteurs dans les réseaux de l'orbite. La proposition suivante généralise cette correspondance pour les variétés drapeaux. Une différence majeure apparaît cependant : s'il est toujours vrai qu'une bonne approximation rationnelle du point x permet de construire un petit vecteur dans un réseau $a_t s_x V_\chi(\mathbb{Z})$, pour $t > 0$ bien choisi, la réciproque n'est pas toujours vraie. Pour pouvoir construire une bonne approximation à partir d'un petit vecteur \mathbf{v} dans $a_t s_x V_\chi(\mathbb{Z})$, il est nécessaire d'imposer que ce vecteur appartienne à l'orbite \tilde{X} d'un vecteur de plus haut poids dans V_χ , et surtout, que sa projection dans la direction de plus haut poids soit comparable à sa norme.

Proposition 2.4.4 (Correspondance drapeau-réseau). *Soit G un \mathbb{Q} -groupe semi-simple, P un \mathbb{Q} -sous-groupe parabolique, et $X = P \backslash G$ la variété quotient. Fixons aussi une hauteur H_χ sur $X(\mathbb{Q})$, donnée par un poids dominant χ associé à P .*

Avec les notations ci-dessus, pour tout $x \in X(\mathbb{R})$,

$$\beta_\chi(x) = \frac{1}{-\chi(Y) - \gamma_\chi(x)}.$$

Démonstration. La hauteur H_χ sur $X(\mathbb{Q})$ est donnée par la formule

$$H_\chi(v) = \|\mathbf{v}\|,$$

où $\mathbf{v} \in V_\chi(\mathbb{Z})$ est un représentant primitif de $v \in X(\mathbb{Q})$.

Soit $\beta < \beta_\chi(x)$, de sorte qu'il existe un point rationnel $v \in X(\mathbb{Q})$ arbitrairement proche de x tel que $d(x, v) \leq H_\chi(v)^{-\beta}$. Écrivons

$$x = P s_x \quad \text{et} \quad v = P e^u s_x, \quad \text{avec } u \in \mathfrak{u}^-,$$

ce qui peut aussi s'écrire, en identifiant $X \simeq G \cdot [e_\chi]$,

$$x = s_x^{-1} \cdot [e_\chi] \quad \text{et} \quad v = s_x^{-1} e^{-u} \cdot [e_\chi].$$

Si \mathbf{v} est un représentant primitif de v dans $V_\chi(\mathbb{Z})$, le vecteur $s_x \mathbf{v}$ est porté par la direction $\mathbb{R} e^{-u} e_\chi$, et par conséquent, pour tout $t > 0$,

$$\begin{aligned} a_t s_x \mathbf{v} &\asymp H_\chi(v) a_t e^{-u} e_\chi \\ &= H_\chi(v) \chi(a_t) e^{-(\text{Ad } a_t)u} e_\chi \\ &= H_\chi(v) \chi(a_t) [e_\chi - ((\text{Ad } a_t)u) e_\chi + \frac{1}{2} ((\text{Ad } a_t)u)^2 e_\chi + \dots] \end{aligned}$$

Notons que dans la somme ci-dessus, seul le premier terme e_χ n'est pas dans le noyau de π^+ .

D'après la proposition 2.2.3, la distance $d(x, v)$ est comparable à la quasi-norme du vecteur u dans \mathfrak{u}^- :

$$d(x, v) \asymp |u| \leq H_\chi(v)^{-\beta}.$$

Soit alors $c > 0$ tel que pour tout $w \in \mathfrak{u}^-$ tel que $|w| \leq c$, on ait $\|w\| \leq \frac{1}{4}$, et $t > 0$ tel que $e^t = cH_\chi(v)^\beta$. Avec ce choix de t , par homogénéité de la quasi-norme $|\cdot|$ pour le flot $\text{Ad } a_t$,

$$|(\text{Ad } a_t)u| = e^t|u| \leq ce^t d(x, v) \leq c$$

et donc

$$\|(\text{Ad } a_t)u\| \leq \frac{1}{4},$$

Or, pour $\|w\| \leq 1/4$, l'inégalité $\|e^w - I\| \leq 1/2$ implique d'une part

$$\| -((\text{Ad } a_t)u)e_\chi + \frac{1}{2}((\text{Ad } a_t)u)^2 e_\chi + \dots \| = \|(e^{-(\text{Ad } a_t)u} - I)e_\chi\| \leq 1/2$$

d'où

$$\|e_\chi\| = 1 \geq \frac{1}{2}\|e_\chi - ((\text{Ad } a_t)u)e_\chi + \frac{1}{2}((\text{Ad } a_t)u)^2 e_\chi + \dots\|$$

puis

$$\|\pi^+(a_t s_x \mathbf{v})\| \geq \frac{1}{2}\|a_t s_x \mathbf{v}\|.$$

D'autre part

$$\|a_t s_x \mathbf{v}\| \leq 2H_\chi(v)\chi(a_t) = 2c^{-\beta}e^{t[\chi(Y) + \frac{1}{\beta}]}$$

Cela montre que $\gamma_\chi(x) \geq -\chi(Y) - \frac{1}{\beta}$, et donc

$$\beta_\chi(x) \leq \frac{1}{-\chi(Y) - \gamma_\chi(x)}.$$

Pour montrer l'inégalité réciproque, fixons $\gamma < \gamma_\chi(x)$. On peut donc trouver $t > 0$ arbitrairement grand, et $\mathbf{v} \in \tilde{X} \cap V_\chi(\mathbb{Z})$ tel que

$$\|a_t s_x \mathbf{v}\| \leq e^{-\gamma t} \tag{2.2}$$

et

$$\|\pi^+(a_t s_x \mathbf{v})\| \geq \frac{1}{2}\|a_t s_x \mathbf{v}\|. \tag{2.3}$$

Notons v l'image de \mathbf{v} dans X , et comme ci-dessus, soit $u \in \mathfrak{u}^-$ tel que $v = Pe^u s_x$. Grâce à l'expression de $a_t s_x \mathbf{v}$ déjà utilisée précédemment, nous avons $\pi^+(a_t s_x \mathbf{v}) \asymp H_\chi(v)\chi(a_t)e_\chi$, et donc, d'après (2.3),

$$\frac{1}{H_\chi(v)\chi(a_t)}\|a_t s_x \mathbf{v}\| \ll 1.$$

On utilise ensuite la stratification $\mathfrak{u}^- = m_1 \oplus \dots \oplus m_r$, et l'on décompose $u = \sum_i u_i$ suivant cette somme directe. Dans l'égalité

$$e_\chi - \frac{1}{H_\chi(v)\chi(a_t)}a_t s_x \mathbf{v} = \left(\sum_i ((\text{Ad } a_t)u_i)e_\chi \right) - \frac{1}{2}((\text{Ad } a_t)u)^2 e_\chi + \dots, \tag{2.4}$$

le terme $((\text{Ad } a_t)u_1)e_\chi$ est en somme directe avec tous les autres, et l'on peut donc majorer

$$\|(\text{Ad } a_t)u_1e_\chi\| \ll 1.$$

Comme $P = \text{Stab}[e_\chi]$, l'application $u \mapsto u \cdot e_\chi$ est un difféomorphisme local au voisinage de 0, et par conséquent,

$$\|(\text{Ad } a_t)u_1\| \ll 1.$$

Dans (3.6), on peut alors faire passer tous les termes du membre de droite de la forme $((\text{Ad } a_t)u_1)^i e_\chi$ dans le membre de gauche, et cela n'augmente pas significativement la norme de ce dernier. Le terme $((\text{Ad } a_t)u_2)e_\chi$ est alors en somme directe avec tous les autres termes du membre de droite, ce qui permet de voir que $\|((\text{Ad } a_t)u_2)e_\chi\| \ll 1$, puis

$$\|(\text{Ad } a_t)u_2\| \ll 1.$$

Ainsi de proche en proche, on montre que pour chaque i , $\|(\text{Ad } a_t)u_i\| \ll 1$, de sorte qu'à la fin $\|((\text{Ad } a_t)u)e_\chi\| \ll 1$, et donc aussi

$$|(\text{Ad } a_t)u| \ll 1.$$

Par suite,

$$d(x, v) \asymp |u| = e^{-t}|(\text{Ad } a_t)u| \ll e^{-t}.$$

Or, l'inégalité (2.2) implique $H_\chi(v)\chi(a_t) = H_\chi(v)e^{t\chi(Y)} \leq e^{-\gamma t}$, d'où l'on tire $e^{t(\chi(Y)+\gamma)} \leq H_\chi(v)^{-1}$, puis¹

$$d(x, v) \ll H_\chi(v)^{\frac{1}{\chi(Y)+\gamma}}.$$

Comme γ peut être choisi arbitrairement proche de $\gamma_\chi(x)$, on obtient bien

$$\beta_\chi(x) \geq \frac{1}{-\chi(Y) - \gamma_\chi(x)}.$$

□

Le premier résultat important impliqué par la proposition 2.4.4 est le théorème suivant, selon lequel la fonction β_χ est constante presque partout sur X .

Théorème 2.4.5 (Valeur presque sûre de l'exposant diophantien). *Soit G un \mathbb{Q} -groupe semi-simple, P un \mathbb{Q} -sous-groupe parabolique, $X = P \backslash G$ la variété quotient, et H_χ la hauteur sur $X(\mathbb{Q})$ associée au poids dominant χ . Il existe une constante $\beta_\chi(X) > 0$ telle que pour presque tout x dans $X(\mathbb{R})$,*

$$\beta_\chi(x) = \beta_\chi(X).$$

De plus, si Π est une base d'un système de racines de G et $\theta \subset \Pi$ est telle que $P = P_\theta$, alors

$$\beta_\chi(X) = \frac{-1}{\chi(Y)},$$

où $Y \in \mathfrak{a}$ est l'élément défini par

$$\alpha(Y) = \begin{cases} 0 & \text{si } \alpha \in \theta \\ -1 & \text{si } \alpha \in \Pi \setminus \theta. \end{cases}$$

¹Noter que $\chi(Y) + \gamma < 0$.

Remarque. La formule $\beta_\chi(X) = \frac{-1}{\chi(Y)}$ implique en particulier que $\beta_\chi(X)$ est rationnel. En effet, il existe un entier $\ell \geq 1$ tel que pour tout élément χ dans le réseau des poids, on ait $\chi(Y) \in \frac{1}{\ell}\mathbb{Z}$. Si le poids χ est choisi dans le réseau engendré par les racines, on a même $-\chi(Y) \in \mathbb{N}^*$.

Démonstration. D'après la proposition 2.4.4, il suffit de faire voir que pour presque tout x dans $X(\mathbb{R})$, $\gamma_\chi(x) = 0$. Notons Γ le sous-groupe arithmétique de G qui stabilise le réseau $V_\chi(\mathbb{Z})$. Tout d'abord, par ergodicité du flot (a_t) sur l'espace $\Omega = G/\Gamma$, pour presque tout $s \in G$,

$$\lim_{t \rightarrow \infty} \frac{1}{t} \log \lambda_1(a_t s V_\chi(\mathbb{Z})) = 0.$$

En effet, si $\lambda_1(a_t s V_\chi(\mathbb{Z})) \leq e^{-\tau t}$, alors pour tout $t' \in [(1-\tau/2)t, t]$, $\lambda_1(a_{t'} s V_\chi(\mathbb{Z})) \leq e^{-\tau t/2} \leq \varepsilon$, et par conséquent $\frac{1}{t} |\{t' \in [0, t] \mid \lambda_1(a_{t'} s V_\chi(\mathbb{Z})) \leq \varepsilon\}| \geq \tau/2$. Mais par ergodicité, le membre de gauche converge vers $m(\{\Delta \mid \lambda_1(\Delta) \leq \varepsilon\})$, qui tend vers zéro lorsque ε tend vers zéro. Noter que $g \mapsto \lambda_1(g V_\chi(\mathbb{Z}))$ définit bien une fonction sur G/Γ , car $V_\chi(\mathbb{Z})$ est stable par Γ . Or, cette limite ne dépend que de la classe Ps de s modulo P , et donc, pour presque tout $x = Ps_x$ dans $X(\mathbb{R})$,

$$\lim_{t \rightarrow \infty} \frac{1}{t} \log \lambda_1(a_t s_x V_\chi(\mathbb{Z})) = 0. \quad (2.5)$$

Comme $\lambda_1(a_t s_x V_\chi(\mathbb{Z})) \leq r_\chi(a_t s_x V_\chi(\mathbb{Z}))$, cela montre déjà, pour presque tout x dans $X(\mathbb{R})$, $\gamma_\chi(x) \leq 0$.

Pour l'inégalité réciproque, nous utiliserons le théorème 4.1.2, tiré de la théorie de la réduction des groupes arithmétiques, dont les résultats principaux sont rappelés au chapitre 4. Pour $t > 0$ grand, ce théorème nous donne une décomposition de Siegel de $a_t s_x$:

$$a_t s_x = kan\gamma \quad \text{avec } k \in K, a \in A_\tau, n \in \omega, \gamma \in C\Gamma,$$

où C est une partie finie de $G(\mathbb{Q})$, Γ le stabilisateur de $V_\chi(\mathbb{Z})$ dans G , et A_τ et ω sont définis au paragraphe 4.1. Comme $\lambda_1(a_t s_x V_\chi(\mathbb{Z})) = e^{o(t)}$, on a aussi

$$\|a\| = e^{o(t)}.$$

Soit (u_1, \dots, u_k) une base de $V_\chi(\mathbb{Q})$ constituée d'éléments de $\tilde{X} \cap V_\chi(\mathbb{Z})$. Le sous-réseau qu'elle engendre est d'indice fini dans $V_\chi(\mathbb{Z})$. Si $D \in \mathbb{N}^*$ est un dénominateur commun aux coefficients des éléments de C dans la représentation sur V_χ , la base $(Da_t s_x \gamma^{-1} u_1, \dots, Da_t s_x \gamma^{-1} u_k)$ est constituée d'éléments de norme $e^{o(t)}$ appartenant à $\tilde{X} \cap a_t s_x V_\chi(\mathbb{Z})$, et engendre un réseau de covolume borné indépendamment de t . Par conséquent, pour tout $\varepsilon > 0$, on peut trouver i tel que l'élément $\mathbf{v}_i = a_t s_x \gamma^{-1} u_i$ vérifie $\frac{\|\pi^+(\mathbf{v}_i)\|}{\|\mathbf{v}_i\|} \geq e^{-\varepsilon t}$, et quitte à diminuer un peu t , on aura même $\frac{\|\pi^+(\mathbf{v}_i)\|}{\|\mathbf{v}_i\|} \geq \frac{1}{2}$. Comme on a aussi $\|\mathbf{v}_i\| = e^{o(t)}$, avec $\varepsilon > 0$ arbitrairement petit, cela donne bien $\gamma_\chi(x) \geq 0$, ce qu'il fallait démontrer. \square

Notons que la démonstration ci-dessus se fonde implicitement sur le lemme suivant, qui découle de la proposition 2.4.4, et dont nous ferons encore usage dans les chapitres 5 et 8.

Lemme 2.4.6. *Soit G un \mathbb{Q} -groupe semi-simple, P un \mathbb{Q} -sous-groupe parabolique, et $X = P \backslash G$ la variété quotient. Fixons aussi une hauteur H_χ sur $X(\mathbb{Q})$, donnée par un poids dominant χ associé à P .*

Soit $x \in X(\mathbb{R})$ et $s_x \in G$ tel que $x = Ps_x$. Si $\lim_{t \rightarrow \infty} \frac{1}{t} \log \lambda_1(a_t s_x V_\chi(\mathbb{Z})) = 0$, alors

$$\beta_\chi(x) = \beta_\chi(X).$$

2.5 Points mal approchables

Par analogie avec la terminologie utilisée pour $\mathbb{P}^1(\mathbb{R})$, nous définissons l'ensemble BA_X des points *mal approchables* dans X par

$$BA_X = \{x \in X(\mathbb{R}) \mid \exists c > 0 : \forall v \in X(\mathbb{Q}), d(x, v) \geq cH_\chi(v)^{-\beta_\chi}\}.$$

Nous montrons ci-dessous que cet ensemble est non vide, et même que sa dimension de Hausdorff est maximale, ce qui généralise un résultat bien connu de Schmidt pour l'espace projectif [50]. Notre démonstration utilise une variante des jeux de Schmidt, similaire à celle utilisée dans un article en commun avec Dmitry Kleinbock [35] pour montrer la propriété dans le cas particulier où X est une quadrique projective. Insistons cependant sur le fait que la distance utilisée ci-dessous sur $X(\mathbb{R})$ est celle associée à la métrique de Carnot-Carathéodory introduite à la partie 2.2.

Commençons par expliquer la règle du jeu de Schmidt, qui dépend d'un paramètre fixe $\alpha \in]0, \frac{1}{3}[$. Le jeu se joue entre deux joueurs Alice et Bob. Pour commencer la partie, Alice choisit une boule $B_0 = B(x_0, \rho_0)$ dans $X(\mathbb{R})$. Bob peut alors ôter à B_0 un voisinage de taille au plus $\rho_1 = \alpha\rho_0$ d'une sous-variété linéaire stricte L , i.e. de l'intersection de $X(\mathbb{R})$, vue comme une partie de $V_\chi(\mathbb{R})$, avec un hyperplan de V_χ . Puis Alice doit choisir une boule B_1 de rayon ρ_1 dans la partie restante $B_0 \setminus L^{(\alpha\rho_0)}$. Ensuite, Bob peut supprimer de B_1 un voisinage de taille au plus $\rho_2 = \alpha\rho_1$ d'une sous-variété linéaire, et ainsi de suite. Comme la suite des rayons $(\rho_n)_{n \geq 0}$ converge vers 0, l'intersection décroissante $\bigcap_{n \geq 0} B_n$ est réduite à un singleton :

$$\bigcap_{n \geq 0} B_n = \{x_\infty\}.$$

Une partie $S \subset X(\mathbb{R})$ est dite α -gagnante si Bob peut toujours jouer de sorte que $x_\infty \in S$. Une partie S est dite *gagnante* si elle est α -gagnante pour $\alpha > 0$ arbitrairement proche de zéro. Deux propriétés importantes des ensembles gagnants sont données dans la proposition ci-dessous, qui se démontre avec des arguments très semblables à ceux utilisés par Schmidt dans son article fondateur [50], auquel on renvoie le lecteur pour plus de détails sur le sujet.

Proposition 2.5.1. *Soit X une variété de drapeaux munie de la distance de Carnot-Carathéodory naturelle et d'une hauteur associée à un poids dominant χ .*

1. *Si (S_i) est une famille dénombrable de parties gagnantes dans $X(\mathbb{R})$, alors $S = \bigcap_i S_i$ est aussi une partie gagnante.*
2. *Si S est une partie gagnante de $X(\mathbb{R})$, alors S est dense dans $X(\mathbb{R})$ et $\dim_H S = \dim X$.*

Démonstration. Pour le premier point, fixons $\alpha \in]0, 1/3[$. En suivant aux temps $1, 3, 5, \dots$ une stratégie α^2 -gagnante pour S_1 , Bob peut s'assurer que $x_\infty \subset B_0 \cap B_2 \cap B_4 \dots$ appartient à S_1 . Aux temps $2, 6, 10, \dots$ une stratégie α^4 -gagnante pour S_2 permet aussi de s'assurer que $x_\infty \subset B_1 \cap B_5 \cap \dots$ soit dans S_2 . Et ainsi de suite, pour chaque $k \geq 1$, Bob peut choisir une stratégie α^{2^k} gagnante pour S_k , qu'il joue aux temps $2^{k-1}(2n+1)$, $n \in \mathbb{N}$ pour avoir toujours $x_\infty \in S_k$. Cela donne bien $x_\infty \in S = \bigcap_i S_i$, et S est donc bien un ensemble gagnant.

Pour le second point, la propriété de S pour un petit paramètre $\alpha > 0$ permet de construire une suite décroissante de fermés $(K_n)_{n \geq 1}$ telle qu'à chaque étape, pour une constante $c > 0$ indépendante de n et α , la partie K_n soit réunion d'au moins $(c \cdot \alpha^{\dim_{cc} X})^n$ boules de rayon α^n , et telle que l'intersection $K = \bigcap_{n \geq 1} K_n$ soit incluse dans S . Pour la métrique de Carnot-Carathéodory, on vérifie sans peine que $\dim_{H,cc} K \geq \frac{(\dim_{cc} X)|\log \alpha| - |\log c|}{|\log \alpha|}$, d'où l'on tire, en faisant tendre α vers 0, $\dim_{H,cc} S = \dim_{cc} X$. Cela implique la même égalité pour la métrique riemannienne : $\dim_H S = \dim X$. \square

Remarque. Dans le premier point, la dimension de Hausdorff est celle associée à une métrique riemannienne sur $X(\mathbb{R})$, et $\dim X$ désigne la dimension de X au sens usuel du terme. Mais la démonstration de la proposition montre plutôt l'égalité analogue pour la métrique de Carnot-Carathéodory $\dim_{H,cc} S = \dim_{cc} X$, qui lui est en fait équivalente.

Théorème 2.5.2 (Propriété de Schmidt des points mal approchables). *Soit X une variété de drapeaux munie de la distance de Carnot-Carathéodory naturelle et d'une hauteur associée à un poids dominant χ . L'ensemble BA_X est un ensemble gagnant au sens défini ci-dessus. En particulier,*

$$\dim_H \text{BA}_X = \dim X.$$

Pour démontrer ce théorème, nous utiliserons le lemme suivant.

Lemme 2.5.3 (Lemme du simplexe). *Soit X une variété de drapeaux munie de la distance de Carnot-Carathéodory naturelle et d'une hauteur associée à un poids dominant χ . Il existe une constante $c > 0$ telle que pour toute boule $B(x, \rho) \subset X(\mathbb{R})$ de rayon $\rho \in]0, 1[$, l'ensemble*

$$E_{x,\rho} = B(x, \rho) \cap \{v \in X(\mathbb{Q}) \mid H(v) \leq c\rho^{-\frac{1}{\beta_X(X)}}\}$$

soit inclus dans une sous-variété linéaire stricte de X .

Démonstration. On reprend les notations utilisées dans la démonstration de la proposition 2.4.4. En particulier si $B_\rho = B(x, \rho)$, on note $s_x \in K$ un élément tel que $Ps_x = x$. Soit $v \in X(\mathbb{Q}) \cap B_\rho$ tel que $H(v) \leq c\rho^{-\frac{1}{\beta_X(X)}}$, et \mathbf{v} un représentant dans $V_\chi(\mathbb{Z})$.

Soit $t > 0$ tel que $e^{-t\chi(Y)} = \rho^{-\frac{1}{\beta_X(X)}}$. Si $c > 0$ est choisi suffisamment petit, le calcul utilisé dans la première partie de la démonstration de la proposition 2.4.4 montre que $\|a_t s_x \mathbf{v}\| < 1$. Comme le réseau $a_t s_x V_\chi(\mathbb{Z})$ est de covolume égal à 1, cela implique que tous les représentants \mathbf{v} des éléments $v \in E_{x,\rho}$ sont inclus dans un hyperplan de V_χ , i.e. que $E_{x,\rho}$ est inclus dans une sous-variété linéaire de X . \square

Démonstration du théorème 2.5.2. Notons pour simplifier $\beta = \beta_X(X)$, et fixons un petit paramètre $\alpha > 0$. Pour commencer, Alice choisit une boule $B_0 = B(x_0, \rho_0)$. D'après le lemme 2.5.3, il existe une constante $c > 0$ telle que tous les points rationnels $v \in X(\mathbb{Q})$ dans $2B_0$ tels que $H(v) \leq c\rho_0^{-\frac{1}{\beta}}$ soient inclus dans une sous-variété linéaire L_0 . Bob peut alors supprimer le voisinage $L_0^{(\alpha\rho_0)}$ de cette sous-variété. Et de même, dans toute la suite de la partie, chaque fois qu'Alice a choisi une boule $B_i = B(x_i, \rho_i)$, où $\rho_i = \rho_0\alpha^i$, les points rationnels $v \in 2B_i$ tels que $H(v) \leq c\rho_i^{-\frac{1}{\beta}}$ sont tous dans une sous-variété linéaire L_i , et Bob peut supprimer le petit voisinage $L_i^{(\alpha\rho_i)}$.

Cette stratégie implique que $x_\infty \in \text{BA}_X$. En effet, si $v \in X(\mathbb{Q})$, on peut choisir i tel que

$$c\rho_{i-1}^{-\frac{1}{\beta}} \leq H(v) \leq c\rho_i^{-\frac{1}{\beta}}. \quad (2.6)$$

Si $v \notin 2B_i$, alors, comme $x_\infty \in B_i$, on trouve

$$d(x_\infty, v) \geq \rho_i = \alpha\rho_{i-1} \geq \alpha c^\beta H(v)^{-\beta}$$

tandis que si $v \in 2B_i$, l'inégalité (2.6) implique $v \in L_i$, et comme $x_\infty \in B_{i+1}$,

$$d(x_\infty, v) \geq \alpha\rho_i = \alpha^2\rho_{i-1} \geq \alpha^2 c^\beta H(v)^{-\beta}.$$

Posant $c_0 = c^\beta \alpha^2$, on trouve

$$\forall v \in X(\mathbb{Q}), \quad d(x_\infty, v) \geq c_0 H(v)^{-1},$$

et donc $x_\infty \in \text{BA}_X$. □

2.6 Un cas particulier : la hauteur anti-canonique

D'après un résultat de Franke [21], lorsque la variété de drapeaux est munie de la hauteur anti-canonique, le nombre $N_X(T)$ de points rationnels de hauteur anti-canonique au plus T dans X vérifie, pour certaines constantes $c > 0$ et $b \in \mathbb{N}^*$,

$$N_X(T) \sim c \cdot T(\log T)^{b-1}, \quad (T \rightarrow \infty).$$

Si ces points sont bien répartis, on peut donc s'attendre à ce que la valeur presque sûre $\beta_X(X)$ de l'exposant diophantien soit donnée par $\frac{1}{\dim_{cc} X}$, où $\dim_{cc} X$ est la dimension de X pour la distance de Carnot-Carathéodory, donnée par l'équivalent asymptotique $N(X, \delta) \asymp \delta^{-\dim_{cc} X}$, où $N(X, \delta)$ désigne le nombre de boules de rayon $\delta > 0$ nécessaire pour recouvrir l'espace compact $X(\mathbb{R})$. Le théorème suivant confirme cet argument heuristique.

Théorème 2.6.1 (Exposant diophantien pour la hauteur anti-canonique). *Soit G un \mathbb{Q} -groupe semi-simple, P un \mathbb{Q} -sous-groupe parabolique, et $X = P \backslash G$ la variété quotient. On munit X de la hauteur anti-canonique H_X associée à la somme des racines apparaissant dans le radical unipotent de P . Alors*

$$\beta_X(X) = \frac{1}{\dim_{cc} X}$$

où $\dim_{cc} X$ est la dimension de Carnot-Carathéodory de X .

Démonstration. Il suffit de vérifier que la formule générale donnée par le théorème 2.4.5 donne la valeur souhaitée dans ce cas particulier.

Les racines qui apparaissent dans le radical unipotent de U sont exactement celles dont la décomposition en racines simples contient un élément hors de la partie θ associée à P . Soit $\chi = \sum_{\alpha \in \Sigma_U} \alpha$ la somme de ces racines. On décompose cette somme suivant le nombre d'éléments hors de θ contenus dans la racine α . Vue la définition de l'élément Y , et en utilisant aussi le fait que U est naturellement isomorphe au sous-groupe unipotent U^- opposé à P ,

$$\chi(Y) = - \sum_{i \geq 1} i \dim m_i = - \dim_{cc} X.$$

□

Cette valeur explicite de $\beta_\chi(X)$, combinée avec l'équivalent asymptotique de Franke $\log N_X(T) \sim \log T$ et un principe de transfert dû à Beresnevich et Velani [7] permet même de calculer la dimension de Hausdorff des points de $X(\mathbb{R})$ tels que $\beta_\chi(x) = \beta$.

Théorème 2.6.2 (Théorème de Jarník pour une variété de drapeaux). *Soit X une variété de drapeaux rationnelle munie de sa métrique de Carnot-Carathéodory et de la hauteur anti-canonique H_χ . Pour tout $\beta \geq \frac{1}{\dim_{cc} X}$, l'ensemble*

$$E_\beta = \{x \in X(\mathbb{R}) \mid \beta(x) \geq \beta\}$$

vérifie

$$\dim_{H,cc} E_\beta = \frac{1}{\beta}.$$

Démonstration. Soit $\beta \geq \frac{1}{\dim_{cc} X}$. Commençons par vérifier que si $s > \frac{1}{\beta}$, alors la mesure de Hausdorff de dimension s de E_β est nulle : $\mathcal{H}_{cc}^s(E_\beta) = 0$. Pour cela, on utilise le recouvrement de E_β par les boules $B(v, H(v)^{-\beta})$, $v \in X(\mathbb{Q})$:

$$E_\beta \subset \bigcup_{H(v) \geq 2^{n_0}} B(v, H(v)^{-\beta})$$

et on majore

$$\begin{aligned} \sum_{H(v) \geq 2^{n_0}} H(v)^{-\beta s} &\leq \sum_{n \geq n_0} 2^{-n\beta s} N_X(2^{n+1}) \\ &\leq C_\varepsilon \sum_{n \geq n_0} 2^{-n(\beta s - 1 - \varepsilon)}, \end{aligned}$$

où la deuxième inégalité provient de la majoration $N_X(T) \leq C_\varepsilon T^{1+\varepsilon}$, qui découle de l'équivalent asymptotique de Franke rappelé ci-dessus. Si $\varepsilon > 0$ est choisi assez proche de zéro pour que $\beta s - 1 - \varepsilon > 0$, la somme converge, et en faisant tendre n_0 vers l'infini, on trouve donc $\mathcal{H}_{cc}^s(E_\beta) = 0$. Cela montre déjà $\dim_{H,cc} E_\beta \leq \frac{1}{\beta}$.

Pour montrer l'inégalité réciproque, on utilise le principe de transfert de Beresnevich et Velani [7, Theorem 3]. Remarquons que la mesure de Lebesgue sur $X(\mathbb{R})$ est équivalente à la mesure de Hausdorff en dimension $\dim_{cc} X$ définie pour la métrique de Carnot-Carathéodory. Pour abrégé les notations, posons $g : x \mapsto x^{\dim_{cc} X}$

et notons \mathcal{H}_{cc}^g la mesure de Hausdorff associée à cette fonction, pour la métrique de Carnot-Carathéodory. Pour certaines constantes $c_1, C_2 > 0$, la mesure d'une boule de rayon $r \leq 1$ dans $X(\mathbb{R})$ est contrôlée par

$$c_1 g(r) \leq \mathcal{H}_{cc}^g(B(x, r)) \leq C_2 g(r).$$

Suivant les notations de [7], si $f : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ est une fonction croissante bijective, et $B = B(x, r)$ une boule dans X , on note

$$B^f = B(x, g^{-1}f(r)) = B(x, (f(r))^{\frac{1}{\dim_{cc} X}}).$$

En particulier, $B^g = B$. Fixons $\beta > \frac{1}{\dim_{cc} X}$, et notons $(B_i)_{i \in \mathbb{N}}$ la famille de boules

$$B(v, H(v)^{-\beta}), \quad v \in X(\mathbb{Q})$$

de sorte que

$$E_\beta \supset \limsup_i B_i^g.$$

Soit $\varepsilon > 0$ et $f : x \mapsto x^{\frac{1}{\beta + \varepsilon}}$. D'après le théorème 2.6.1 l'ensemble $\limsup_i B_i^f$ est de mesure pleine :

$$\forall B \subset X(\mathbb{R}), \quad \mathcal{H}^g(B \cap \limsup_i B_i^f) = \mathcal{H}^g(B).$$

D'après [7, Theorem 3], cela implique

$$\forall B \subset X(\mathbb{R}), \quad \mathcal{H}^f(B \cap \limsup_i B_i^g) = \mathcal{H}^f(B)$$

et donc

$$\dim_{H,cc} E_\beta \geq \frac{1}{\beta + \varepsilon}.$$

□

Remarque. Lorsque X n'est pas munie de la hauteur anti-canonique, on peut toujours utiliser l'équivalent de Mohammadi et Salehi Golsefidy [46]

$$N_X(T) \sim cT^{u_X} (\log T)^{v_X}$$

et le lemme de Borel-Cantelli pour montrer que $\beta_X(X) \leq \frac{u_X}{\dim_{cc} X}$. Mais cette inégalité peut être stricte.

De même, la première partie de la démonstration du théorème 2.6.2 ci-dessus permet de voir que

$$\forall \beta \geq \frac{u_X}{\dim_{cc} X}, \quad \dim_{H,cc} E_\beta \leq \frac{u_X}{\beta}$$

tandis que le principe de transfert de Beresnevich et Velani implique que

$$\forall \beta \geq \beta_X(X), \quad \dim_{H,cc} E_\beta \geq \frac{\beta_X(X) \dim_{cc} X}{\beta}.$$

Mais ces deux bornes ne coïncident pas en général.

Chapitre 3

Le théorème de Khintchine

Comme précédemment, X désigne une variété de drapeaux, donnée sous la forme $X = P \backslash G$, où G est un \mathbb{Q} -groupe semi-simple, et P un \mathbb{Q} -sous-groupe parabolique. La hauteur H_χ sur $X(\mathbb{Q})$ est donnée par le choix d'un poids dominant χ de G associé à P , et la distance est celle associée à la métrique de Carnot-Carathéodory usuelle sur X . Cela permet de définir l'exposant diophantien $\beta_\chi(x)$ d'un point x dans $X(\mathbb{R})$. Nous avons vu à la partie précédente que cet exposant diophantien est constant presque partout sur $X(\mathbb{R})$: il existe une constante $\beta_\chi(X)$ telle que pour presque tout x dans $X(\mathbb{R})$, l'inégalité

$$d(x, v) \leq H(v)^{-\beta},$$

admet une infinité de solutions $v \in X(\mathbb{Q})$ si $\beta < \beta_\chi(X)$, et un nombre fini de solutions si $\beta > \beta_\chi(X)$. Pour étudier plus précisément les propriétés diophantiennes d'un point aléatoire de $X(\mathbb{R})$, nous nous intéressons donc à l'inégalité

$$d(x, v) \leq H(v)^{-\beta_\chi(X)} \psi(H(v)), \quad (3.1)$$

où $\psi : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ est une fonction décroissante. Le théorème 3.2.1 ci-dessous, analogue du célèbre théorème de Khintchine [29], donne une condition nécessaire et suffisante sur ψ pour que (3.1) ait une infinité de solutions pour presque tout x dans $X(\mathbb{R})$.

Pour sa démonstration, nous suivons l'approche développée par Kleinbock et Margulis [32, 30] pour démontrer le théorème de Khintchine dans l'espace projectif : nous ramenons ce théorème à un énoncé sur le comportement asymptotique de certaines orbites diagonales dans l'espace de réseaux $\Omega = G/\Gamma$, et utilisons la propriété de mélange exponentiel du flot (a_t) sur Ω . Dans le cas où X est une sphère projective, le théorème 3.2.1 est dû à Kleinbock et Merrill [36], qui ont ensuite généralisé leur résultat à une quadrique projective arbitraire, dans un travail en commun avec Fishman et Simmons [20]. Quelques complications interviennent dans notre situation, notamment parce que les ensembles à atteindre ne sont plus à proprement parler des voisinages de l'infini dans Ω . Nous commençons la démonstration par un paragraphe un peu calculatoire, sur le volume de certaines parties de Ω , parce que cela fera apparaître les paramètres utiles à l'énoncé précis du théorème de Khintchine.

3.1 Voisinages de l'infini

Ce paragraphe a pour but la proposition 3.1.1 ci-dessous, qui décrit le comportement asymptotique du volume de certaines portions de voisinages de l'infini dans G/Γ . Dans tout le paragraphe, G désigne un \mathbb{Q} -groupe semi-simple. Étant donnée une \mathbb{Q} -représentation linéaire V_χ de G engendrée par une unique droite rationnelle $\mathbb{R}e_\chi$ de plus haut poids χ , on note

$$P = \text{Stab}_G \mathbb{R}e_\chi$$

le stabilisateur dans G de la direction engendrée par e_χ , et

$$\tilde{X} = G \cdot e_\chi$$

l'orbite du vecteur de plus haut poids sous l'action de G . On considère un réseau rationnel $V_\chi(\mathbb{Z})$ dans V_χ , et le stabilisateur de $V_\chi(\mathbb{Z})$ dans G est noté Γ ; c'est un sous-groupe arithmétique de G .

Notons enfin $\Omega = G/\Gamma$, que nous identifierons naturellement à une partie de l'espace des réseaux de V_χ , via l'application $g\Gamma \mapsto gV_\chi(\mathbb{Z})$. Rappelons que sur cet espace de réseaux, la fonction r_χ est définie par

$$r_\chi(\Delta) = \inf\{r > 0 \mid \exists \mathbf{v} \in \Delta \cap \tilde{X} : \|\mathbf{v}\| \leq r \text{ et } \|\pi^+(\mathbf{v})\| \geq \frac{\|\mathbf{v}\|}{2}\},$$

où $\pi^+ : V_\chi \rightarrow V_\chi$ désigne la projection sur e_χ parallèlement aux autres espaces de poids.

Proposition 3.1.1 (Volume des voisinages de l'infini). *Pour $r > 0$, on considère le voisinage de l'infini dans Ω défini par*

$$\Omega_r = \{\Delta \in \Omega \mid \min_{\mathbf{v} \in \Delta \cap \tilde{X}} \|\mathbf{v}\| \leq r\},$$

et la sous-partie

$$\Omega'_r = \{\Delta \in \Omega \mid r_\chi(\Delta) \leq r\}.$$

Il existe des constantes $C, a_\chi, b_\chi > 0$ telles que pour tout r suffisamment petit,

$$\frac{1}{C} r^{a_\chi} |\log r|^{b_\chi - 1} \leq m_\Omega(\Omega'_r) \leq m_\Omega(\Omega_r) \leq C r^{a_\chi} |\log r|^{b_\chi - 1}.$$

Si $(Y_i)_{1 \leq i \leq r}$ désigne la base duale de la base des racines simples, et ρ la somme des racines positives comptées avec multiplicité, alors

$$a_\chi = \min_{1 \leq i \leq r} \frac{\rho(Y_i)}{\chi(Y_i)} \quad \text{et} \quad b_\chi = \text{card}\{i \in [1, r] \mid \frac{\rho(Y_i)}{\chi(Y_i)} = a_\chi\}.$$

La démonstration de cette proposition est basée sur la théorie de la réduction, telle qu'elle est exposée dans Borel [8, §§15 et 16]. Nous aurons en particulier besoin de la notion d'ensemble de Siegel. Notons B un \mathbb{Q} -sous-groupe parabolique minimal de G inclus dans P , T un tore \mathbb{Q} -déployé maximal dans B , $A = T^0(\mathbb{R})$ la composante connexe des points réels de T , N le radical unipotent de B , et M le \mathbb{Q} -sous-groupe anisotrope maximal du centralisateur $Z(T)^0$ de T dans G^0 . Le lecteur

est renvoyé à Borel [8, §11] et Borel et Tits [10] pour les résultats fondamentaux concernant la structure des \mathbb{Q} -sous-groupes paraboliques de G .

Soit \mathfrak{a} l'algèbre de Lie de A . Le système de racines Σ de G par rapport à T s'identifie à un système de racines dans l'espace dual \mathfrak{a}^* . On fixe un système de racines simples $\Pi = \{\alpha_1, \dots, \alpha_r\}$ pour un ordre associé à B . Pour $\tau \geq 0$, on définit un voisinage \mathfrak{a}_τ^- de \mathfrak{a}^- par

$$\mathfrak{a}_\tau^- = \{Y \in \mathfrak{a} \mid \forall \alpha \in \Pi, \alpha(Y) \leq \tau\},$$

et

$$A_\tau = \exp \mathfrak{a}_\tau^- \subset A.$$

Un ensemble de Siegel \mathfrak{S} de G sur \mathbb{Q} est un ensemble de la forme

$$\mathfrak{S} = KA_\tau\omega,$$

où K désigne un sous-groupe compact maximal de G , et ω un voisinage compact de l'identité dans les points réels de MN .

Démonstration de la proposition 3.1.1. Nous supposons dans cette démonstration que la norme sur V_χ est invariante par le sous-groupe compact maximal K ; on peut toujours se ramener à ce cas, par équivalence des normes en dimension finie. Soit $C \subset G(\mathbb{Q})$ un ensemble de représentants des classes de $P(\mathbb{Q}) \backslash G(\mathbb{Q}) / \Gamma$. D'après Borel [8, proposition 15.6], l'ensemble C est fini. Soit

$$\tilde{\Omega}_r = \{g\Gamma \in \Omega \mid \exists \gamma \in \Gamma, c \in C : \|g\gamma^{-1}c^{-1}e_\chi\| \leq r\}.$$

Comme C est fini, il existe une constante $C_0 > 0$ telle que pour tout $r > 0$,

$$\Omega_{r/C_0} \subset \tilde{\Omega}_r \subset \Omega_{C_0 r}.$$

De même, avec

$$\tilde{\Omega}'_r = \{g\Gamma \in \Omega \mid \exists \gamma \in \Gamma, c \in C : \|g\gamma^{-1}c^{-1}e_\chi\| \leq r \text{ et } \frac{\|\pi^+(g\gamma^{-1}c^{-1}e_\chi)\|}{\|g\gamma^{-1}c^{-1}e_\chi\|} \geq \frac{1}{2}\},$$

on a

$$\Omega'_{r/C_0} \subset \tilde{\Omega}'_r \subset \Omega'_{C_0 r}.$$

Il suffit donc de démontrer la proposition pour les ensembles $\tilde{\Omega}_r$ et $\tilde{\Omega}'_r$.

Fixons maintenant un ensemble de Siegel \mathfrak{S} qui satisfasse la conclusion de [8, Théorème 16.9] pour la fonction de type (P, χ) définie par $\Phi(g) = \|ge_\chi\|$. Soit $\tilde{\phi}$ la fonction sur G définie par

$$\tilde{\phi}(g) = \sum_{c \in C} \mathbb{1}_{\{gc^{-1} \in \mathfrak{S} \text{ et } \|gc^{-1}e_\chi\| \leq r\}}.$$

La projection de $\tilde{\phi}$ sur G/Γ est donnée par

$$\begin{aligned} \phi(g\Gamma) &= \sum_{\gamma \in \Gamma} \sum_{c \in C} \mathbb{1}_{\{g\gamma c^{-1} \in \mathfrak{S} \text{ et } \|g\gamma c^{-1}e_\chi\| \leq r\}} \\ &\geq \mathbb{1}_{\{\exists \gamma, c : g\gamma c^{-1} \in \mathfrak{S} \text{ et } \|g\gamma c^{-1}e_\chi\| \leq r\}} \\ &= \mathbb{1}_{\{\exists \gamma, c : \|g\gamma c^{-1}e_\chi\| \leq r\}} \\ &= \mathbb{1}_{\tilde{\Omega}_r}(g\Gamma), \end{aligned}$$

où l'avant-dernière égalité découle du choix de \mathfrak{S} , suivant [8, Théorème 16.9]. Par suite,

$$\begin{aligned} m_{G/\Gamma}(\tilde{\Omega}_r) &\leq m_{G/\Gamma}(\phi) \\ &= m_G(\tilde{\phi}) \\ &= \sum_{c \in C} m_G(\{g \mid gc^{-1} \in \mathfrak{S} \text{ et } \|gc^{-1}e_\chi\| \leq r\}) \\ &= |C| \cdot m_G(\{g \in \mathfrak{S} \mid \|ge_\chi\| \leq r\}). \end{aligned}$$

Pour évaluer le dernier terme, on utilise la définition de \mathfrak{S} et on décompose la mesure de Haar sur G suivant la décomposition $g = kman$. D'après [37, Proposition 8.32], pour les mesures de Haar à gauche sur G , K et MAN , notant $\Delta_{MAN} : MAN \rightarrow \mathbb{R}_+^*$ la fonction modulaire de MAN ,

$$dg = \Delta_{MAN}(man) dk d(man) = \Delta_{MAN}(m) \rho(a) dk d(man),$$

où ρ est le caractère de A associé à la somme des racines restreintes positives, comptées avec multiplicité. Toujours grâce à [37, Proposition 8.32], on peut encore décomposer

$$d(man) = dm d(an) = dm da dn,$$

et donc

$$\begin{aligned} m_G(\{g \in \mathfrak{S} \mid \|ge_\chi\| \leq r\}) &\asymp \int_{A^-} \mathbb{1}_{\{\chi(a) \leq r\}} \rho(a) da \\ &= \int_{\mathfrak{a}^-} \mathbb{1}_{\{\chi(h) \leq \log r\}} e^{\rho(h)} dh. \end{aligned}$$

Cette dernière intégrale est l'intégrale d'une fonction exponentielle sur un polytope convexe de \mathfrak{a} , et est donc comparable au maximum de la fonction sur cet ensemble, multiplié par un facteur correspondant à la dimension de la face sur laquelle ce maximum est réalisé. Naturellement, ce maximum est réalisé en l'un des sommets du convexe, qui sont les points $A_i = \frac{\log r}{\chi(Y_i)} Y_i$, $i = 1, \dots, r$. On trouve donc

$$\int_{\mathfrak{a}^-} \mathbb{1}_{\{\chi(h) \leq \log r\}} e^{\rho(h)} dh \asymp r^{a_\chi} (\log 1/r)^{b_\chi - 1}$$

où

$$a_\chi = \min_{1 \leq i \leq r} \frac{\rho(Y_i)}{\chi(Y_i)} \quad \text{et} \quad b_\chi = \text{card}\{i \in [1, r] \mid \frac{\rho(Y_i)}{\chi(Y_i)} = a_\chi\}.$$

Cela montre déjà une partie des inégalités souhaitées :

$$m_\Omega(\Omega'_r) \leq m_\Omega(\Omega_r) \ll r^{a_\chi} |\log r|^{b_\chi - 1}.$$

Le calcul pour minorer $m_\Omega(\Omega'_r) \asymp m_\Omega(\tilde{\Omega}'_r)$ est similaire : ayant fixé un ensemble de Siegel \mathfrak{S} , on utilise la fonction

$$\tilde{\psi}(g) = \mathbb{1}_{\{g \in \mathfrak{S} \text{ et } \|ge_\chi\| \leq r \text{ et } \|\pi^+(ge_\chi)\| \geq \frac{1}{2} \|ge_\chi\|\}}.$$

Par la propriété de Siegel pour le domaine \mathfrak{S} , i.e. la dernière assertion de [8, théorème 15.5], la projection de $\tilde{\psi}$ sur G/Γ vérifie, pour une certaine constante C_1 ,

$$\begin{aligned} \psi(g\Gamma) &= \sum_{\gamma \in \Gamma} \mathbb{1}_{\{g\gamma \in \mathfrak{S} \text{ et } \|g\gamma e_\chi\| \leq r \text{ et } \|\pi^+(g\gamma e_\chi)\| \geq \frac{1}{2}\|g\gamma e_\chi\|\}} \\ &\leq C_1 \mathbb{1}_{\{\exists \gamma \in \Gamma : \|g\gamma e_\chi\| \leq r \text{ et } \|\pi^+(g\gamma e_\chi)\| \geq \frac{1}{2}\|g\gamma e_\chi\|\}} \\ &= C_1 \mathbb{1}_{\tilde{\Omega}'_r}(g\Gamma). \end{aligned}$$

Par conséquent,

$$\begin{aligned} m_{G/\Gamma}(\tilde{\Omega}'_r) &\gg m_{G/\Gamma}(\psi) \\ &= m_G(\tilde{\psi}) \\ &= m_G(\{g \in \mathfrak{S} \mid \|ge_\chi\| \leq r \text{ et } \|\pi^+(ge_\chi)\| \geq \frac{1}{2}\|ge_\chi\|\}). \end{aligned}$$

Comme précédemment, pour évaluer le dernier terme, on utilise la décomposition de la mesure de Haar sur G suivant la décomposition $g = kman$. Soit $\omega \subset MN$ un voisinage compact de l'identité tel que

$$\mathfrak{S} \supset K(\exp \mathfrak{a}^-)\omega$$

et $V_K \subset K$ un voisinage de l'identité tel que

$$\forall k \in V_K, \quad \|\pi^+(ke_\chi)\| \geq \frac{1}{2}\|ke_\chi\| = \frac{1}{2}\|e_\chi\|.$$

Alors, pour tout h dans la chambre de Weyl \mathfrak{a}^- et tout $u \in MN$,

$$\|\pi^+(ke^h ue_\chi)\| = e^{\chi(h)} \|\pi^+(ke_\chi)\| \geq \frac{1}{2} e^{\chi(h)} \|e_\chi\| = \frac{1}{2} \|ke^h ue_\chi\|,$$

et l'on peut donc minorer

$$\begin{aligned} &m_G(\{g \in \mathfrak{S} \mid \|ge_\chi\| \leq r \text{ et } \|\pi^+(ge_\chi)\| \geq \frac{1}{2}\|ge_\chi\|\}) \\ &\geq \iint_{V_K \times \omega} \int_{\mathfrak{a}^-} \mathbb{1}_{\{\|ke^h ue_\chi\| \leq r \text{ et } \|\pi^+(ke^h ue_\chi)\| \geq \frac{1}{2}\|ke^h ue_\chi\|\}} e^{\rho(h)} dh dk du \\ &\geq \iint_{V_K \times \omega} \int_{\mathfrak{a}^-} \mathbb{1}_{\{\chi(h) \leq \log r\}} e^{\rho(h)} dh dk du \\ &\gg \int_{\mathfrak{a}^-} \mathbb{1}_{\{\chi(h) \leq \log r\}} e^{\rho(h)} dh \\ &\gg r^{a_\chi} |\log r|^{b_\chi - 1} \end{aligned}$$

par le calcul déjà expliqué dans la première partie de la démonstration. \square

Remarque. Les coefficients u_χ et v_χ qui apparaissent dans le théorème de Mohammadi et Salehi Golsefidy [46, Theorem 4], énoncé comme théorème 2.1.1 ci-dessus, ne sont pas égaux à a_χ et b_χ en général. L'équivalent asymptotique du nombre de points rationnels de X de hauteur au plus T est donné par

$$N_\chi(T) \sim c \cdot T^{u_\chi} (\log T)^{v_\chi - 1}.$$

Dans [46], ces coefficients sont définis de la façon suivante. On note $\mathfrak{b}^+ = \{\phi \in \mathfrak{a}^* \mid \forall i, \phi(\alpha_i) \geq 0\}$ et ρ_X la somme des racines associées à l'unipotent de P , et on pose

$$u_\chi = \inf\{u \mid u\chi - \rho_X \in \mathfrak{b}^+\} = \max_i \frac{\langle \rho_X, \alpha_i \rangle}{\langle \chi, \alpha_i \rangle},$$

tandis que v_χ est la codimension de la face de \mathfrak{b}^+ contenant $u_\chi\chi - \rho$. Dans le cas particulier où X est munie de la hauteur anti-canonique, $\rho_X = \chi$ et donc $u_\chi = a_\chi = 1$ et $v_\chi = b_\chi = \text{rang } G - \text{rang } P$. En effet, dans ce cas, $a_\chi = \min_i \frac{\rho(Y_i)}{\rho_X(Y_i)}$ est atteint pour tout i correspondant à une racine simple hors de la partie θ associée à P .

Notons $\varpi_1, \dots, \varpi_r$ les poids fondamentaux associés à la base de racines simples $\Pi = \{\alpha_1, \dots, \alpha_r\}$. Pour chaque i , on fixe une \mathbb{Q} -représentation V_i de G engendrée par une unique droite rationnelle de plus haut poids $\omega_i = b_i\varpi_i$, avec $b_i \in \mathbb{N}^*$ minimal. Suivant Borel et Tits [10, §12.13], nous dirons que les représentations V_i , $i = 1, \dots, r$, sont les représentations *fondamentales* de G . Lorsque $V_\chi = V_j$ est une représentation fondamentale de G , on peut déterminer quel indice réalise le minimum définissant a_χ ; c'est le contenu du lemme ci-dessous.

Lemme 3.1.2. *Soit $V_\chi = V_j$ une représentation fondamentale de G et P le sous-groupe parabolique maximal associé, stabilisateur de la droite de plus haut poids. Il existe $r_j \in \mathbb{Q}$ tel que la somme des racines du radical unipotent U de P , comptées avec multiplicité, vérifie*

$$\sum_{\alpha \in \Sigma_j^+} m_\alpha \alpha = r_j \omega_j,$$

et alors, les quantités a_χ et b_χ de la proposition précédente sont données par

$$a_\chi = r_j \quad \text{et} \quad b_\chi = 1.$$

Démonstration. Soit P le parabolique maximal correspondant à $\chi = \omega_j$. Le radical unipotent U de P correspond à l'ensemble Σ_j^+ des racines positives contenant α_j dans leur décomposition en racines simples. D'après [46, Lemma 5], la somme ρ_j de ces racines, comptées avec multiplicité, est proportionnelle à ω_j :

$$r_j \omega_j = \sum_{\alpha \in \Sigma_j^+} m_\alpha \alpha = \rho_j.$$

Par conséquent, il suffit de comprendre pour quel i la quantité $\frac{\rho(Y_i)}{\rho_j(Y_i)}$ est minimale. Naturellement, comme Y_j est orthogonal à toutes les racines qui ne contiennent pas α_j , on trouve

$$\frac{\rho(Y_j)}{\rho_j(Y_j)} = 1,$$

tandis que si $i \neq j$,

$$\frac{\rho(Y_i)}{\rho_j(Y_i)} = 1 + \frac{\rho'_j(Y_i)}{\rho_j(Y_i)} > 1,$$

où ρ'_j désigne la somme des racines positives qui ne contiennent pas α_j . Ainsi, $b_\chi = 1$ et

$$a_\chi = \frac{\rho(Y_j)}{\omega_j(Y_j)} = \frac{\rho_j(Y_j)}{\omega_j(Y_j)} = r_j.$$

□

Ce lemme et sa démonstration se généralisent de la façon suivante.

Lemme 3.1.3. *Soit θ une partie de la base du système de racines de G , et P_θ le sous-groupe parabolique associé. Si $\chi = \sum_{\alpha \in \Sigma_\theta^+} m_\alpha \alpha$, est la somme des racines du radical unipotent de P_θ , comptées avec multiplicité, alors*

$$a_\chi = 1 \quad \text{et} \quad b_\chi = \text{rang}_{\mathbb{Q}} G - |\theta|.$$

Démonstration. Pour chaque i , on observe que

$$\rho(Y_i) = \sum_{\alpha \in \Sigma_i^+} m_\alpha \alpha(Y_i),$$

où Σ_i^+ désigne l'ensemble des racines positives contenant α_i . Comme par ailleurs Σ_θ^+ est l'ensemble des racines positives qui contiennent un élément hors de θ , on calcule

$$\chi(Y_i) = \sum_{\alpha \in \Sigma_i^+ \cap \Sigma_\theta^+} m_\alpha \alpha(Y_i) \begin{cases} = \sum_{\alpha \in \Sigma_i^+} m_\alpha \alpha(Y_i) & \text{si } i \notin \theta \\ < \sum_{\alpha \in \Sigma_i^+} m_\alpha \alpha(Y_i) & \text{si } i \in \theta, \end{cases}$$

cela montre ce qu'on veut. \square

3.2 Théorème de Khintchine et flots diagonaux

Comme précédemment, G désigne un \mathbb{Q} -groupe semi-simple, P un \mathbb{Q} -sous-groupe parabolique, et $X = P \backslash G$ la variété quotient. On fixe un poids dominant χ associé au sous-groupe parabolique P . D'après la proposition 3.1.1, il existe des constantes $a_\chi > 0$ et $b_\chi \in \mathbb{N}^*$ telles que pour $r > 0$ petit, le voisinage Ω_r de l'infini dans Ω défini par

$$\Omega_r = \{g\Gamma \mid \min_{v \in \tilde{X} \cap V_\chi(\mathbb{Z})} \|gv\| \leq r\}$$

vérifie

$$m_\Omega(\Omega_r) \asymp r^{a_\chi} |\log r|^{b_\chi - 1}.$$

Avec ces notations, le théorème de Khintchine sur la variété projective X , munie de la hauteur H_χ associée à χ et de la distance de Carnot-Carathéodory usuelle, s'énonce comme suit.

Théorème 3.2.1 (Théorème de Khintchine sur X). *Notons $\beta_\chi = \beta_\chi(X)$ l'exposant donné par le théorème 2.4.5. Soit $\psi : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ une fonction décroissante. Pour x dans X , on s'intéresse à l'inégalité*

$$d(x, v) \leq H_\chi(v)^{-\beta_\chi} \psi(H_\chi(v)). \quad (3.2)$$

- Si $\int_e^{+\infty} \psi(u)^{\frac{a_\chi}{\beta_\chi}} (\log \log u)^{b_\chi - 1} \frac{du}{u} < +\infty$, alors, pour presque tout x dans X , l'inégalité (3.2) n'a qu'un nombre fini de solutions.
- Si $\int_e^{+\infty} \psi(u)^{\frac{a_\chi}{\beta_\chi}} (\log \log u)^{b_\chi - 1} \frac{du}{u} = +\infty$, alors, pour presque tout x dans X , l'inégalité (3.2) admet une infinité de solutions.

Rappelons qu'un point $x \in X(\mathbb{R})$ est dit *mal approchable* dans X s'il existe une constante $c > 0$ telle que pour tout v dans $X(\mathbb{Q})$, $d(x, v) \geq cH_\chi(v)^{-\beta_x}$. Nous avons vu au chapitre 2 que l'ensemble BA_X des points mal approchables dans X est de dimension de Hausdorff maximale. Le théorème de Khintchine permet de montrer qu'il est toutefois négligeable au sens de la mesure de Lebesgue.

Corollaire 3.2.2 (Points mal approchables sur X). *L'ensemble BA_X des points mal approchables dans X est de mesure de Lebesgue nulle.*

Démonstration. Pour la fonction constante définie par $\psi(u) = c > 0$ pour tout $u \in \mathbb{R}^+$, l'intégrale est divergente. Le résultat découle donc de la seconde partie du théorème. \square

On peut aussi étudier les inégalités obtenues à partir de fonctions élémentaires, et montrer le résultat suivant.

Corollaire 3.2.3. 1. *L'inégalité $d(x, v) \leq H_\chi(v)^{-\beta_x} (\log H_\chi(v))^{-\gamma}$ admet une infinité de solutions $v \in X(\mathbb{Q})$ pour presque tout $x \in X(\mathbb{R})$, si et seulement si $\gamma \leq \frac{\beta_x}{a_x}$.*

2. *L'inégalité $d(x, v) \leq H_\chi(v)^{-\beta_x} (\log H_\chi(v))^{-\frac{\beta_x}{a_x}} (\log \log H_\chi(v))^{-\delta}$ admet une infinité de solutions $v \in X(\mathbb{Q})$ pour presque tout $x \in X(\mathbb{R})$, si et seulement si $\delta \leq \frac{b_x \beta_x}{a_x}$.*

Démonstration. D'après le théorème 3.2.1, il suffit pour la première partie d'étudier l'intégrabilité au voisinage de l'infini de la fonction ϕ définie par

$$\phi(u) = \frac{(\log \log u)^{b_x - 1}}{u(\log u)^{\frac{a_x \gamma}{\beta_x}}}.$$

L'intégrale diverge si et seulement si $\gamma \leq \frac{\beta_x}{a_x}$. La démonstration de la seconde assertion est analogue, une fois observé que l'intégrale

$$\int_e^{+\infty} \frac{du}{u(\log u)(\log \log u)^{\frac{a_x \delta}{\beta_x} - b_x + 1}}$$

diverge si et seulement si $\delta \leq \frac{b_x \beta_x}{a_x}$. \square

Pour traduire le théorème 3.2.1 en termes d'orbites diagonales dans l'espace des réseaux, nous aurons besoin d'une version un peu plus précise de la correspondance démontrée au chapitre 2, que nous énonçons maintenant. Rappelons que l'on définit un sous-groupe à un paramètre (a_t) dans le groupe A des points réels du tore \mathbb{Q} -déployé maximal T en posant

$$a_t = e^{tY} \quad \text{où } Y \in \mathfrak{a} \text{ est défini par } \alpha(Y) = \begin{cases} 0 & \text{si } \alpha \in \theta \\ -1 & \text{si } \alpha \notin \theta, \end{cases} \quad (3.3)$$

où $\theta \subset \Pi$ est l'ensemble de racines simples associé au sous-groupe parabolique P , tel que toutes les racines négatives de P se décomposent en éléments de θ . Enfin, si Δ est un réseau dans V_χ , nous avons défini ci-dessus

$$r_\chi(\Delta) = \inf\{r > 0 \mid \exists v \in \tilde{X} \cap B(0, r) : \|\pi^+(v)\| \geq \frac{1}{2}\|v\|\},$$

où $\pi^+ : V_\chi \rightarrow V_\chi$ désigne la projection sur $\mathbb{R}e_\chi$ parallèlement aux autres espaces de poids de a_t .

Proposition 3.2.4 (Correspondance drapeau-réseau). *Fixons $x \in X(\mathbb{R})$ et choisissons $s_x \in G$ tel que $x = Ps_x$. On note $\beta_\chi = \beta_\chi(X)$ l'exposant diophantien donné par la proposition 2.4.5. Il existe une constante $C > 0$ telle que les énoncés suivants soient vérifiés.*

Soit $\psi : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ une fonction décroissante, et $\Psi : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ la fonction définie par

$$\Psi(u) = Cu^{-\beta_\chi}\psi(u).$$

- *Si l'inégalité $d(x, v) \leq H_\chi(v)^{-\beta_\chi}\psi(H_\chi(v))$ admet une infinité de solutions $v \in X(\mathbb{Q})$, alors il existe $t > 0$ arbitrairement grand tel que*

$$r_\chi(a_t s_x V_\chi(\mathbb{Z})) \leq 2e^{-\frac{t}{\beta_\chi}} \Psi^{-1}(e^{-t}).$$

- *Si on a pour $t > 0$ arbitrairement grand $r_\chi(a_t s_x V_\chi(\mathbb{Z})) \leq e^{-\frac{t}{\beta_\chi}} \Psi^{-1}(e^{-t})$, alors l'inégalité*

$$d(x, v) \leq C^2 H_\chi(v)^{-\beta_\chi} \psi(H_\chi(v))$$

admet une infinité de solutions $v \in X(\mathbb{Q})$.

Démonstration. La démonstration est identique à celle de la proposition 2.4.4. Soit $v \in X(\mathbb{Q})$ arbitrairement proche de x tel que $d(x, v) \leq H_\chi(v)^{-\beta_\chi}\psi(H_\chi(v))$. Écrivons

$$x = Ps_x \quad v = Pe^u s_x, \quad u \in \mathfrak{u}^-,$$

de sorte que

$$d(x, v) \asymp |u| \leq H_\chi(v)^{-\beta_\chi}\psi(H_\chi(v)).$$

Soit $C > 0$ tel que pour tout $w \in \mathfrak{u}^-$ tel que $C|w| \leq 1$, on ait $\|w\| \leq \frac{1}{4}$. On choisit $t > 0$ tel que

$$e^{-t} = \Psi(H_\chi(v)) = CH_\chi(v)^{-\beta_\chi}\psi(H_\chi(v)).$$

Cela implique $C|(\text{Ad } a_t)u| = Ce^t|u| \leq 1$ et donc

$$\|(\text{Ad } a_t)u\| \leq \frac{1}{4}.$$

Soit maintenant \mathbf{v} un représentant primitif de v dans $V_\chi(\mathbb{Z})$. Le vecteur $s_x \mathbf{v}$ est porté par la direction $\mathbb{R}e^{-u}e_\chi$, et par conséquent, pour tout $t > 0$,

$$\begin{aligned} a_t s_x \mathbf{v} &= H_\chi(v) a_t e^{-u} e_\chi \\ &= H_\chi(v) e^{t\chi(Y)} [\exp(-(\text{Ad } a_t)u)] e_\chi \\ &= H_\chi(v) e^{t\chi(Y)} [e_\chi - (\text{Ad } a_t)u e_\chi + ((\text{Ad } a_t)u)^2 e_\chi - \dots] \end{aligned}$$

L'inégalité $\|e^w - I\| \leq 2\|w\|$ appliquée à $w = (\text{Ad } a_t)u$ donne d'une part

$$\|\pi^+(a_t s_x \mathbf{v})\| \geq \frac{1}{2} \|a_t s_x \mathbf{v}\|,$$

et d'autre part

$$\|a_t s_x \mathbf{v}\| \leq 2H_\chi(v) e^{t\chi(Y)}.$$

Comme $H_\chi(v) = \Psi^{-1}(e^{-t})$ et $\beta_\chi = \frac{-1}{\chi(Y)}$, cela montre que

$$r_\chi(a_t s_x \mathbf{v}) \leq 2H_\chi(v) e^{t\chi(Y)} \leq 2e^{-\frac{t}{\beta_\chi}} \Psi^{-1}(e^{-t}).$$

Montrons l'inégalité réciproque. Pour $t > 0$ arbitrairement grand, soit $\mathbf{v} \in \tilde{X} \cap V_\chi(\mathbb{Z})$ tel que

$$\|a_t s_x \mathbf{v}\| \leq e^{-\frac{t}{\beta_\chi}} \Psi^{-1}(e^{-t}) \quad (3.4)$$

et

$$\|\pi^+(a_t s_x \mathbf{v})\| \geq \frac{1}{2} \|a_t s_x \mathbf{v}\|. \quad (3.5)$$

Notons v l'image de \mathbf{v} dans X . Grâce à l'expression de $a_t s_x \mathbf{v}$ utilisée ci-dessus, nous avons

$$\pi^+(a_t s_x \mathbf{v}) = e^{t\chi(Y)} H_\chi(v) e_\chi$$

et donc, d'après (3.5),

$$H_\chi(v)^{-1} e^{-t\chi(Y)} \|a_t s_x \mathbf{v}\| \leq 2.$$

On utilise ensuite la stratification $\mathfrak{u}^- = m_1 \oplus \dots \oplus m_k$, et l'on décompose $u = \sum_i u_i$ suivant cette somme directe. Dans l'égalité

$$e_\chi - e^{-t\chi(Y)} H_\chi(v)^{-1} a_t s_x \mathbf{v} = \sum_i ((\text{Ad } a_t) u_i) e_\chi - \frac{1}{2} ((\text{Ad } a_t) u)^2 e_\chi + \dots, \quad (3.6)$$

le terme $((\text{Ad } a_t) u_1) e_\chi$ est en somme directe avec tous les autres, et l'on peut donc majorer

$$\|(\text{Ad } a_t) u_1 e_\chi\| \leq 3.$$

Comme $P = \text{Stab}[e_\chi]$, l'application $u \mapsto u \cdot e_\chi$ est un difféomorphisme local au voisinage de 0, et par conséquent,

$$\|(\text{Ad } a_t) u_1\| \ll 1.$$

Dans (3.6), on peut alors faire passer tous les termes du membre de droite de la forme $((\text{Ad } a_t) u_1)^i e_\chi$ dans le membre de gauche, et cela n'augmente pas significativement la norme de ce dernier. Le terme $((\text{Ad } a_t) u_2) e_\chi$ est alors en somme directe avec tous les autres termes du membre de droite, ce qui permet de voir que $\|((\text{Ad } a_t) u_2) e_\chi\| \ll 1$, puis

$$\|(\text{Ad } a_t) u_2\| \ll 1.$$

Ainsi de proche en proche, on montre que pour chaque i , $\|(\text{Ad } a_t) u_i\| \ll 1$, de sorte qu'à la fin $\|((\text{Ad } a_t) u) e_\chi\| \ll 1$, et donc aussi

$$|(\text{Ad } a_t) u| \ll 1.$$

Par suite,

$$d(x, v) = |u| = e^{-t} |(\text{Ad } a_t) u| \ll e^{-t}.$$

Or, l'inégalité (3.4) et la relation $\beta_\chi = -\frac{1}{\chi(Y)}$ impliquent

$$e^{t\chi(Y)} H_\chi(v) = \|\pi^+(a_t s_x v)\| \leq \|a_t s_x v\| \leq e^{t\chi(Y)} \Psi^{-1}(e^{-t}),$$

d'où l'on tire $e^{-t} \leq \Psi(H_\chi(v))$, ce qui permet de conclure

$$d(x, v) \ll \Psi(H_\chi(v)) \ll H_\chi(v)^{-\beta_\chi} \psi(H_\chi(v)).$$

□

3.3 Somme convergente

Nous donnons ici la démonstration de la première partie du théorème de Khintchine pour X . L'énoncé correspondant concernant le comportement asymptotique des orbites diagonales dans l'espace $\Omega = G/\Gamma$ est une simple application du lemme de Borel-Cantelli. Rappelons que l'espace Ω s'identifie à un ensemble de réseaux de l'espace euclidien V_χ associé à la représentation de plus haut poids χ , via l'application $g\Gamma \mapsto gV_\chi(\mathbb{Z})$. Avec cette identification, notant aussi $\tilde{X} = G \cdot e_\chi$ l'orbite du vecteur de plus haut poids dans V , on pose, pour $r > 0$,

$$\Omega_r = \{\Delta \in \Omega \mid \exists v \in \Delta \cap \tilde{X} : \|v\| \leq r\}.$$

Enfin, la mesure de Haar sur $\Omega = G/\Gamma$ est notée m_Ω .

Proposition 3.3.1. *Soit $(a_t)_{t \in \mathbb{N}}$ une suite d'éléments de G et $(r_t)_{t \in \mathbb{N}}$ une suite de réels positifs telle que $\sum_{t \geq 1} m_\Omega(\Omega_{r_t}) < \infty$. Pour presque tout $\Delta \in \Omega$, pour tout $t \in \mathbb{N}$ suffisamment grand,*

$$a_t \Delta \notin \Omega_{r_t}.$$

Par conséquent, pour presque tout $x = P s_x$ dans X , pour tout $t \in \mathbb{N}$ suffisamment grand,

$$r_\chi(a_t s_x V_\chi(\mathbb{Z})) \geq r_t.$$

Démonstration. Comme chaque élément a_t préserve la mesure de Haar sur Ω ,

$$m_\Omega(\{\Delta \mid a_t \Delta \in \Omega_{r_t}\}) = m_\Omega(\Omega_{r_t}),$$

est le terme général d'une série convergente, et le lemme de Borel-Cantelli montre donc que pour presque tout Δ , pour tout t suffisamment grand, $a_t \Delta \notin \Omega_{r_t}$. La seconde partie découle de la première, car

$$r_\chi(a_t s_x \Gamma) \geq \min\{\|v\| \mid v \in a_t s_x V_\chi(\mathbb{Z}) \cap \tilde{X}\},$$

et ce deuxième terme ne dépend pas du choix de s_x , à une constante multiplicative près. En appliquant la première partie à une suite (r'_t) telle que $\sum_{t \in \mathbb{N}} m_\Omega(\Omega_{r'_t}) < +\infty$ et $r_t = o(r'_t)$ on fait disparaître cette constante multiplicative. \square

Nous aurons besoin du lemme suivant, qui permet de supposer dans la démonstration du théorème 3.2.1 que la fonction ψ est majorée par une fonction de la forme $t \mapsto (\log t)^{-c}$. Le dessin ci-dessous explique le calcul effectué pour la démonstration.

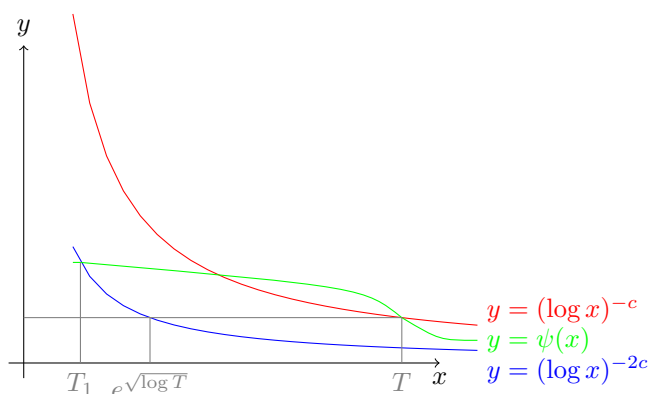


FIGURE 3.1 : Graphes des fonctions ψ , $x \mapsto (\log x)^{-c}$ et $x \mapsto (\log x)^{-2c}$.

Lemme 3.3.2. Soient $a, \beta > 0$ et $b \in \mathbb{N}^*$. Il existe $c > 0$ tel que pour toute fonction $\psi : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ décroissante telle que

$$I(\psi) = \int_e^\infty \psi(u)^{\frac{a}{\beta}} (\log \log u)^{b-1} \frac{du}{u} < +\infty,$$

pour tout $u > 0$ suffisamment grand, $\psi(u) \leq (\log u)^{-c}$.

Démonstration. Posons $c = \frac{\beta}{2a}$ et supposons que pour $T > 0$ arbitrairement grand, $\psi(T) \geq (\log T)^{-c}$. Soit

$$T_1 = \sup\{u \in [0, T] \mid \psi(u) \leq (\log u)^{-2c}\}.$$

Comme ψ est décroissante,

$$(\log T_1)^{-2c} \geq \psi(T_1) \geq \psi(T) \geq (\log T)^{-c},$$

et donc $(\log T_1) \leq (\log T)^{1/2}$. Par suite,

$$\begin{aligned} \int_{T_1}^T \psi(u)^{\frac{a}{\beta}} (\log \log u)^{b-1} \frac{du}{u} &\geq \int_{T_1}^T \frac{du}{u \log u} \\ &= \log \log T - \log \log T_1 \\ &\geq \frac{1}{2} \log \log T. \end{aligned}$$

Cela montre que l'intégrale $I(\psi)$ est divergente, et le lemme s'en déduit, par contraposée. \square

Nous pouvons maintenant démontrer la première partie du théorème 3.2.1.

Démonstration du théorème 3.2.1, cas convergent. Soit $\psi : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ décroissante telle que

$$\int_e^\infty \psi(u)^{\frac{ax}{\beta x}} (\log \log u)^{bx-1} \frac{du}{u} < \infty.$$

Quitte à remplacer $\psi(u)$ par $\psi(u) + (\log u)^{-C}$, avec $C > \frac{\beta_x}{a_x}$, on peut toujours supposer que $\psi(u) \geq (\log u)^{-C}$. D'autre part, le lemme 3.3.2 montre que pour tout $u > 0$ suffisamment grand, $\psi(u) \leq (\log u)^{-c}$. Ainsi,

$$\forall u \geq 0, \quad (\log u)^{-C} \leq \psi(u) \leq (\log u)^{-c}. \quad (3.7)$$

Posant

$$\Psi(u) = u^{-\beta_x} \psi(u) \quad \text{et} \quad r_t = 2e^{-\frac{t}{\beta_x}} \Psi^{-1}(e^{-t}),$$

les propositions 3.2.4 et 3.3.1 montrent qu'il suffit de démontrer que la somme $\sum_{t \geq 1} m_\Omega(\Omega_{r_t})$ converge, ce qui équivaut, d'après la proposition 3.1.1, à

$$\sum_{t \geq 1} r_t^{a_x} |\log r_t|^{b_x - 1} < +\infty.$$

L'encadrement (3.7) ci-dessus se réécrit

$$u^{-\beta_x} (\log u)^{-C} \leq \Psi(u) \leq u^{-\beta_x} (\log u)^{-c}, \quad (3.8)$$

ce qui implique

$$s^{-\frac{1}{\beta_x}} |\log s|^{-\frac{C}{\beta_x}} \ll \Psi^{-1}(s) \ll s^{-\frac{1}{\beta_x}} |\log s|^{-\frac{c}{\beta_x}}.$$

En effet, si $\Phi_-(u) = u^{-\beta_x} (\log u)^{-C}$ et $\Phi_+(u) = u^{-\beta_x} (\log u)^{-c}$, on a $\Phi_-^{-1}(s) \leq \Psi^{-1}(s) \leq \Phi_+^{-1}(s)$, et il suffit donc de vérifier que

$$s^{-1/\beta} |\log s|^{-\frac{C}{\beta}} \ll \Phi_-^{-1}(s) \leq \Phi_+^{-1}(s) \ll s^{-1/\beta} |\log s|^{-\frac{c}{\beta}}.$$

Comme Φ_- et Φ_+ sont décroissantes, cela est équivalent au fait que pour certains $C_0, c_0 > 0$,

$$\begin{aligned} \Phi_-(c_0 s^{-1/\beta} |\log s|^{-\frac{C}{\beta}}) &\geq s \geq \Phi_+(C_0 s^{-1/\beta} |\log s|^{-\frac{c}{\beta}}) \\ c_0^{-\beta} s |\log s|^C \left[\frac{-1}{\beta} \log s - \frac{C}{\beta} \log |\log s| \right]^{-C} &\geq s \geq C_0^{-\beta} s |\log s|^c \left[\frac{-1}{\beta} \log s - \frac{c}{\beta} \log |\log s| \right]^{-c} \\ c_0^{-\beta} s \left[\frac{1}{\beta} - o(1) \right]^{-C} &\geq s \geq C_0^{-\beta} s \left[\frac{1}{\beta} - o(1) \right]^{-c}, \end{aligned}$$

et le résultat s'ensuit, si C_0, c_0 sont choisis de sorte que $c_0^{-\beta} \beta^C > 1 > C_0^{-\beta} \beta^c$. Avec la borne supérieure de cet encadrement, on trouve

$$r_t = 2e^{-\frac{t}{\beta_x}} \Psi^{-1}(e^{-t}) \ll t^{-\frac{c}{\beta_x}},$$

d'où

$$|\log r_t| \ll \log t.$$

Par suite, il suffit de vérifier que

$$\sum_{t \geq 1} r_t^{a_x} (\log t)^{b_x - 1} < +\infty.$$

Pour cela, majorons

$$\Psi^{-1}(s) = s^{-\frac{1}{\beta_x}} \psi(\Psi^{-1}(s)) \leq s^{-\frac{1}{\beta_x}} \psi(c_0 s^{-\frac{1}{\beta_x}} |\log s|^{-\frac{C}{\beta_x}}),$$

et donc

$$r_t = 2e^{-\frac{t}{\beta_x}} \Psi^{-1}(e^{-t}) \leq 2\psi(c_0 e^{\frac{t}{\beta_x}} t^{-\frac{C}{\beta_x}}).$$

Cela donne

$$\begin{aligned} \sum_{t \geq 1} r_t^{a_x} (\log t)^{b_x - 1} &\leq 2 \sum_{t \geq 1} \psi(c_0 e^{\frac{t}{\beta_x}} t^{-\frac{C}{\beta_x}})^{a_x} (\log t)^{b_x - 1} \\ &\leq 2 \int_e^\infty \psi(c_0 e^{\frac{t}{\beta_x}} t^{-\frac{C}{\beta_x}})^{a_x} (\log t)^{b_x - 1} dt \end{aligned}$$

et avec le changement de variable $u = c_0 e^{\frac{t}{\beta_x}} t^{-\frac{C}{\beta_x}}$, $\frac{du}{u} = (\frac{1}{\beta_x} + o(1))dt$,

$$\sum_{t \geq 1} r_t^{a_x} (\log t)^{b_x - 1} \ll \int_1^\infty \psi(u)^{a_x} (\log \log u)^{b_x - 1} \frac{du}{u} < +\infty.$$

□

3.4 Somme divergente

Ici encore, on se ramène à un énoncé sur les orbites diagonales dans l'espace $\Omega = G/\Gamma$. La démonstration de la proposition suivante occupe la majeure partie de la fin de la démonstration du théorème 3.2.1; la traduction en termes d'approximation diophantienne sur X se fera facilement, par un calcul analogue à celui que nous avons donné ci-dessus dans le cas où la somme est convergente.

Proposition 3.4.1. *Soit (r_t) une suite de réels positifs telle que $\sum_{t \geq 1} m_\Omega(\Omega_{r_t}) = +\infty$. Alors, pour presque tout $\Delta \in \Omega$, il existe $t \in \mathbb{N}$ arbitrairement grand tel que*

$$r_\chi(a_t \Delta) \leq r_t.$$

En particulier, pour presque tout $x = Ps_x \in X$, pour $t \in \mathbb{N}$ arbitrairement grand,

$$r_\chi(a_t s_x V(\mathbb{Z})) \leq r_t.$$

Naturellement, la démonstration de cette proposition est basée sur une version du lemme de Borel-Cantelli dans le cas où la somme des probabilités des événements considérés est divergente, avec une hypothèse supplémentaire d'indépendance. Plus précisément, nous utiliserons le lemme élémentaire ci-dessous.

Lemme 3.4.2 (Une version du lemme de Borel-Cantelli). *Soit (X, m) un espace de probabilité, et $(h_t)_{t \in \mathbb{N}}$ une suite de fonctions intégrables à valeurs positives sur X satisfaisant :*

1. $\sum_{t \geq 1} m(h_t) = +\infty$;
2. $\exists C \geq 0 : \forall N \geq 1, \int_X (\sum_{t=1}^N h_t(x) - m(h_t))^2 m(dx) \leq C \cdot \sum_{t=1}^N m(h_t)$.

Alors pour presque tout x , l'ensemble $I(x) = \{t \in \mathbb{N} \mid h_t(x) > 0\}$ est infini.

Démonstration. Posons

$$\phi_N(x) = \frac{1}{\sum_{t=1}^N m(h_t)} \cdot \sum_{t=1}^N h_t(x).$$

Par hypothèse,

$$\left\| \sum_{t=1}^N h_t - m(h_t) \right\|_2^2 \leq C \cdot \sum_{t=1}^N m(h_t)$$

et donc

$$\|\phi_N - 1\|_2^2 \leq \frac{1}{\sum_{t=1}^N m(h_t)} \rightarrow_{N \rightarrow \infty} 0.$$

Par suite, on peut extraire de (ϕ_N) une sous-suite (ϕ_{N_k}) convergeant pour presque tout x vers 1. Alors, presque sûrement,

$$\sum_{t=1}^{N_k} h_t(x) \sim_{k \rightarrow \infty} \sum_{t=1}^{N_k} m(h_t) \rightarrow +\infty,$$

ce qui montre en particulier que l'ensemble $I(x)$ est presque sûrement infini. \square

Pour démontrer la deuxième partie du théorème 3.2.1, on souhaiterait appliquer le lemme 3.4.2 à la famille de fonctions $h_t = \mathbb{1}_{a_t^{-1}\Omega'_{r_t}}$, où

$$\Omega'_{r_t} = \{\Delta \in \Omega \mid r_\chi(\Delta) \leq r_t\}.$$

Cependant, la seconde condition du lemme n'est pas évidente à vérifier. Pour cela, nous nous ramenons à une suite de fonctions lisses h_t qui approchent $\mathbb{1}_{a_t^{-1}\Omega'_{r_t}}$ et dont on contrôle les normes de Sobolev.

Lemme 3.4.3. *Soit Υ l'opérateur $\Upsilon = 1 - \sum_i Y_i^2$, où (Y_i) est une base orthonormée de l'algèbre de Lie \mathfrak{k} d'un sous-groupe compact maximal de $G(\mathbb{R})$. Il existe des constantes $C, c > 0$ et une famille de fonctions $\eta_r : \Omega \rightarrow [0, 1]$, $r \in]0, 1]$ telles que*

1. $\eta_r(\Delta) > 0 \Rightarrow r_\chi(\Delta) \leq r$;
2. $\int_\Omega \eta_r(\Delta) m_\Omega(d\Delta) \geq cr^{a_\chi} |\log r|^{b_\chi - 1}$;
3. $\|\Upsilon^\ell(\eta_r)\|_2 \leq C\|\eta_r\|_2$.

Démonstration. Pour $\varepsilon > 0$ fixé suffisamment petit, on fixe une fonction positive $P \in C_c^\infty(G)$ telle que $\int_G P = 1$, $P(g) = P(g^{-1})$, et $\text{Supp } P \subset B_G(1, \varepsilon)$. Ensuite, pour tout $r > 0$, on pose

$$\eta_r = P * \mathbb{1}_{\Omega''_r},$$

où

$$\Omega''_r = \{\Delta \in \Omega \mid \exists v \in \Delta \cap \tilde{X} : \|v\| \leq \frac{r}{2} \text{ et } \frac{\|\pi^+(v)\|}{\|v\|} \geq \frac{3}{4}\}.$$

Vérifions que ces fonctions satisfont les conditions requises.

1. Si $\eta_r(\Delta) = \int_G P(g) \mathbb{1}_{\Omega''_r}(g\Delta) du > 0$, il existe $g \in \text{Supp } P \subset B_G(1, \varepsilon)$ tel que $g\Delta \in \Omega''_r$. En d'autres termes, pour un certain vecteur $v \in \Delta \cap \tilde{X}$ et $g \in B_G(1, \varepsilon)$,

$$\|\pi^+(gv)\| \geq \frac{3}{4}\|gv\| \quad \text{et} \quad \|gv\| \leq \frac{r}{2}.$$

Si $\varepsilon > 0$ est suffisamment petit, alors $\|g - 1\| \leq 1/10$, $\|g^{-1} - 1\| \leq 1/5$, et par conséquent, d'une part

$$\|v\| \leq \|g^{-1}\| \|gv\| \leq r,$$

et d'autre part

$$\begin{aligned} \|\pi^+(v)\| &\geq \|\pi^+(gv)\| - \|\pi^+(gv - v)\| \\ &\geq \frac{3}{4}\|gv\| - \frac{1}{10}\|v\| \\ &\geq \frac{3\|v\|}{4\|g^{-1}\|} - \frac{\|v\|}{10} \geq \frac{\|v\|}{2}. \end{aligned}$$

Cela montre bien que $\Delta \in \Omega'_r$.

2. Il suffit d'appliquer la proposition 3.1.1 pour obtenir

$$\int_{\Omega} \eta_r(\Delta) m_{\Omega}(d\Delta) = m_{\Omega}(\Omega''_r) \geq cr^{a_x} |\log r|^{b_x - 1},$$

pour un certain $c > 0$.

3. On contrôle $\|\Upsilon^\ell \eta_r\|_2$ grâce à l'inégalité de Young :

$$\|\Upsilon^\ell \eta_r\|_2 = \|\Upsilon^\ell P * \mathbb{1}_{\Omega''_r}\|_2 \leq \|\Upsilon P\|_2 \|\mathbb{1}_{\Omega''_r}\|_1 \leq C m_{\Omega}(\Omega''_r) = C \|\eta_r\|_1.$$

□

Enfin, nous aurons besoin du théorème suivant, qui découle des résultats de [32, §3.4] et [18, §4.1]. Malheureusement, la démonstration de ce théorème est trop longue pour être incluse dans ce mémoire ; plusieurs résultats intermédiaires importants ont permis d'y aboutir, et l'on renvoie à [18, §§ 4.2 et 4.3] pour plus de détails sur ce sujet.

Théorème 3.4.4 (Décroissance exponentielle des coefficients dans $L^2(\Omega)$). *Soit G un \mathbb{Q} -groupe semi-simple simplement connexe, Γ un sous-groupe arithmétique, et $\Omega = G/\Gamma$. Soit T un \mathbb{Q} -tore déployé maximal de G , $A = T^0(\mathbb{R})$ et (a_t) un sous-groupe à un paramètre de A . On suppose que $\forall t > 0$, $a_t = e^{tY}$, avec $Y \in \mathfrak{a}$ tel que pour toute projection $p_i : \mathfrak{g} \rightarrow \mathfrak{g}_i$ sur un facteur \mathbb{Q} -simple, $p_i(Y) \neq 0$. Il existe des constantes $\ell \in \mathbb{N}$ et $C, \tau > 0$ telles que pour toutes fonctions $f_1, f_2 \in C^\infty(\Omega)$ et tout $t > 0$,*

$$\left| \int_{\Omega} f_1(a_t \Delta) f_2(\Delta) m_{\Omega}(d\Delta) - m_{\Omega}(f_1) m_{\Omega}(f_2) \right| \leq C e^{-\tau t} \|\Upsilon^\ell f_1\|_2 \|\Upsilon^\ell f_2\|_2,$$

où Υ désigne l'opérateur différentiel $\Upsilon = 1 - \sum_i Y_i^2$, où (Y_i) est une base ortho-normée de l'algèbre de Lie \mathfrak{k} d'un sous-groupe compact maximal de $G(\mathbb{R})$.

Remarque. L'inégalité démontrée dans [18] est plus générale : pour tout g dans $G(\mathbb{R})$, $|\langle g f_1, f_2 \rangle - m_{\Omega}(f_1) m_{\Omega}(f_2)| \leq C \|g\|^{-\tau} \|\Upsilon^\ell f_1\|_2 \|\Upsilon^\ell f_2\|_2$, et la constante τ ne dépend pas de G . Le résultat est même encore valable sur les adèles.

Nous pouvons enfin conclure la démonstration de la proposition 3.4.1.

Démonstration de la proposition 3.4.1. On considère la suite de fonctions définies par $h_t(\Delta) = \eta_{r_t}(a_t \Delta)$. On peut supposer que le \mathbb{Q} -groupe semi-simple G est simplement connexe, et que le sous-groupe parabolique P ne contient aucun \mathbb{Q} -facteur de G . Dans ce cas, vu la définition de l'élément Y , pour toute projection $p_i : \mathfrak{g} \rightarrow \mathfrak{g}_i$ sur un facteur simple, $p_i(Y) \neq 0$, et l'on peut appliquer le théorème 3.4.4 :

$$\begin{aligned} \int_X \left(\sum_{t=1}^N h_t(\Delta) - m_\Omega(h_t) \right)^2 m_\Omega(d\Delta) &= \sum_{1 \leq t_1, t_2 \leq N} \int_X h_{t_1}(\Delta) h_{t_2}(\Delta) m_\Omega(d\Delta) - m_\Omega(h_{t_1}) m_\Omega(h_{t_2}) \\ &\ll \sum_{1 \leq t_1, t_2 \leq N} e^{-\tau|t_1 - t_2|} \|\Upsilon^\ell \eta_{r_{t_1}}\|_2 \|\Upsilon^\ell \eta_{r_{t_2}}\|_2 \\ &\ll \sum_{1 \leq t_1, t_2 \leq N} e^{-\tau|t_1 - t_2|} \|h_{t_1}\|_1 \|h_{t_2}\|_1 \\ &\ll \sum_{t=1}^N m_\Omega(h_t). \end{aligned}$$

Par ailleurs,

$$m_\Omega(h_t) = m_\Omega(\eta_{r_t}) \geq cr_t^{a_x} |\log r_t|^{b_x - 1} \gg m_\Omega(\Omega_{r_t})$$

et donc

$$\sum_{t \in \mathbb{N}} m_\Omega(h_t) \gg \sum_{t \in \mathbb{N}} m_\Omega(\Omega_{r_t}) = +\infty.$$

Ainsi, le lemme 3.4.2 s'applique à la suite de fonctions (h_t) , et montre que pour presque tout Δ , l'ensemble $I(\Delta) = \{t \in \mathbb{N} \mid h_t(\Delta) > 0\}$ est infini. Cela implique que pour presque tout $\Delta \in \Omega$, il existe t arbitrairement grand tel que $a_t \Delta \in \Omega'_{r_t}$. C'est ce qu'on voulait. \square

Nous pouvons enfin conclure cette partie avec la fin de la démonstration du théorème de Khintchine pour la variété de drapeaux $X = P \backslash G$.

Démonstration du théorème 3.2.1, cas divergent. Soit $C > \frac{\beta_x}{a_x}$. Quitte à remplacer ψ par la fonction $\tilde{\psi}$ définie par $\tilde{\psi}(u) = \max(\psi(u), (\log u)^{-C})$, on peut supposer que

$$\forall t > 0, \quad \psi(u) \geq (\log u)^{-C}. \quad (3.9)$$

En effet, comme $\int_e^{+\infty} (\log u)^{-\frac{C a_x}{\beta_x}} (\log \log u)^{b_x - 1} \frac{du}{u} < +\infty$ la première partie du théorème montre que l'inégalité $d(x, v) \leq H_\chi(v)^{-\beta_x} (\log H_\chi(v))^{-C}$ n'a qu'un nombre fini de solutions. Par suite, si $d(x, v) \leq H_\chi(v)^{-\beta} \tilde{\psi}(H_\chi(v))$ a une infinité de solutions, alors c'est aussi le cas pour l'inégalité $d(x, v) \leq H_\chi(v)^{-\beta} \psi(H_\chi(v))$.

Rappelons qu'étant donnée une fonction $\psi : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ décroissante, nous posons, pour $t > 0$,

$$\Psi(u) = u^{-\beta_x} \psi(u) \quad \text{et} \quad r_t = e^{-\frac{t}{\beta_x}} \Psi^{-1}(e^{-t}).$$

La proposition 3.2.4 montre qu'il suffit de montrer pour presque tout $x = Ps_x$ dans $X(\mathbb{R})$, pour $t > 0$ arbitrairement grand,

$$r_\chi(a_t s_x V_\chi(\mathbb{Z})) \leq r_t.$$

Cela découlera de la proposition 3.4.1, si nous pouvons montrer que $\sum_{t \geq 1} m_\Omega(\Omega_{r_t}) = +\infty$. Sous l'hypothèse (3.9), $\Psi(u) \geq u^{-\beta_x} (\log u)^{-C}$ donc $\Psi^{-1}(s) \gg s^{-\frac{1}{\beta_x}} |\log s|^{-\frac{C}{\beta_x}}$ puis

$$r_t = e^{-\frac{t}{\beta_x}} \Psi^{-1}(e^{-t}) \geq t^{-\frac{C}{\beta_x}}.$$

D'autre part, comme ψ est décroissante, pour tout $u \geq 1$, $\Psi(u) \leq u^{-\beta_x} \psi(1)$, donc $\Psi^{-1}(s) \ll s^{-\frac{1}{\beta_x}}$, et

$$\Psi^{-1}(s) = s^{-\frac{1}{\beta_x}} \psi(\Psi^{-1}(s))^{\frac{1}{\beta_x}} \gg s^{-\frac{1}{\beta_x}} \psi(C_0 s^{-\frac{1}{\beta_x}})^{\frac{1}{\beta_x}}.$$

Par suite,

$$\begin{aligned} \sum_{t \geq 1} r_t^{a_x} |\log r_t|^{b_x-1} &\gg \sum_{t \geq 1} r_t^{a_x} (\log t)^{b_x-1} \\ &= \sum_{t \geq 1} e^{-\frac{t a_x}{\beta_x}} \Psi^{-1}(e^{-t})^{a_x} (\log t)^{b_x-1} \\ &\geq \sum_{t \geq 1} \psi(C_0 e^{\frac{t}{\beta_x}})^{\frac{a_x}{\beta_x}} (\log t)^{b_x-1} \\ &\gg \int_1^\infty \psi(C_0 e^{\frac{t}{\beta_x}})^{\frac{a_x}{\beta_x}} (\log t)^{b_x-1} dt \\ &\gg \int_e^\infty \psi(u)^{\frac{a_x}{\beta_x}} (\log \log u)^{b_x-1} \frac{du}{u}, \end{aligned}$$

où la dernière inégalité découle du changement de variable

$$u = C_0 e^{\frac{t}{\beta_x}}, \quad \frac{du}{u} = \frac{dt}{\beta_x}.$$

Ainsi, $\sum_{t \geq 1} m_\Omega(\Omega_{r_t}) = +\infty$, et le théorème est démontré. \square

Chapitre 4

Géométrie des espaces de réseaux

Nous rappelons dans cette partie les résultats principaux de la théorie de la réduction, due à Borel et Harish-Chandra [9], et exposée très clairement dans Borel [8]. Cette théorie – que nous avons déjà utilisée dans la partie précédente pour évaluer le volume de certaines parties de Ω – décrit quels paramètres sont nécessaires pour situer un élément Δ dans l'espace de réseaux $\Omega = G/\Gamma$. Plus tard, nous étudierons le comportement asymptotique de ces paramètres le long de certaines orbites diagonales dans Ω , pour l'appliquer à nos problèmes d'approximation diophantienne.

4.1 Théorie de la réduction

Soit G un \mathbb{Q} -groupe semi-simple et $\Gamma = G(\mathbb{Z})$ un sous-groupe arithmétique de G . Nous notons B un \mathbb{Q} -sous-groupe parabolique minimal de G , U le radical unipotent de B , T un \mathbb{Q} -tore déployé maximal dans B , M le \mathbb{Q} -sous-groupe anisotrope maximal du centralisateur $Z(T)^0$ de T dans G^0 , et $A = T^0(\mathbb{R})$ la composante connexe des points réels de T .

Soit \mathfrak{a} l'algèbre de Lie de A . Le système de racines Σ de G par rapport à T s'identifie à un système de racines dans l'espace dual \mathfrak{a}^* . Fixons un système de racines simples $\Pi = \{\alpha_1, \dots, \alpha_r\}$ pour un ordre associé à B et notons \mathfrak{a}^- la chambre de Weyl opposée dans \mathfrak{a} , définie par

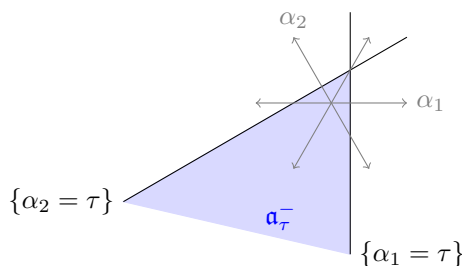
$$\mathfrak{a}^- = \{Y \in \mathfrak{a} \mid \forall \alpha \in \Pi, \alpha(Y) \leq 0\}.$$

Plus généralement, pour $\tau \geq 0$, on définit un voisinage \mathfrak{a}_τ^- de \mathfrak{a}^- par

$$\mathfrak{a}_\tau^- = \{Y \in \mathfrak{a} \mid \forall \alpha \in \Pi, \alpha(Y) \leq \tau\},$$

et

$$A_\tau = \exp \mathfrak{a}_\tau^- \subset A.$$

FIGURE 4.1 : Dessin de \mathfrak{a}_τ^- pour SL_3

Définition 4.1.1 (Ensemble de Siegel). Un *ensemble de Siegel* \mathfrak{S} de G sur \mathbb{Q} est un ensemble de la forme

$$\mathfrak{S} = KA_\tau\omega,$$

où K désigne un sous-groupe compact maximal de G , et ω un voisinage compact de l'identité dans les points réels de MU . En outre, on supposera toujours que K contient un ensemble de représentants du groupe de Weyl relatif $W = N(A)/A$ de G sur \mathbb{Q} , où $N(A)$ est égal au normalisateur de A dans G . Cela est possible d'après Borel et Tits [10, §5].

La théorie de la réduction pour les groupes arithmétiques [8, Théorème 15.5] nous assure qu'il existe un ensemble de Siegel dans G qui est à peu près un domaine fondamental pour l'action de Γ sur G .

Théorème 4.1.2 (Domaine fondamental du second type). *Il existe un ensemble de Siegel \mathfrak{S} sur \mathbb{Q} de G et une partie finie C de $G(\mathbb{Q})$ tels que $G = \mathfrak{S}C\Gamma$.*

Dans la suite, nous fixons une partie finie C de $G(\mathbb{Q})$ et un ensemble de Siegel $\mathfrak{S} = KA_\tau\omega$ qui satisfont la conclusion du théorème ci-dessus. Pour g dans G , nous dirons que l'expression

$$g = kanc\gamma, \quad \text{avec } k \in K, a \in A_\tau, n \in \omega, c \in C, \text{ et } \gamma \in \Gamma$$

est une *décomposition de Siegel* de g . Une telle décomposition n'est pas unique, mais nous verrons plus tard que certains de ses éléments sont essentiellement indépendants du choix de la décomposition. En général, le théorème ci-dessus [8, théorème 15.4] nous assure qu'il n'existe qu'un nombre fini de décompositions de Siegel d'un élément g de G .

Théorème 4.1.3 (Propriété de Siegel). *Soit \mathfrak{S} un ensemble de Siegel dans G . Pour toute partie finie $F \subset G(\mathbb{Q})$, l'ensemble $\Gamma \cap (\mathfrak{S}F)(\mathfrak{S}F)^{-1}$ est fini.*

4.2 Représentations et ensembles fondamentaux

Ayant fixé un \mathbb{Q} -tore déployé maximal T dans G , nous choisisons une base $\Pi = \{\alpha_1, \dots, \alpha_r\}$ du système de racines Σ associé à T , et notons $\varpi_1, \dots, \varpi_r$ les poids fondamentaux associés. Pour chaque i , on fixe une \mathbb{Q} -représentation V_i de G engendrée par une unique droite rationnelle de plus haut poids $\omega_i = b_i\varpi_i$, avec $b_i \in \mathbb{N}^*$

minimal, et $V_i(\mathbb{Z})$ un réseau rationnel dans V_i stable par l'action de Γ et contenant un vecteur de plus haut poids e_i . Suivant Borel et Tits [10, §12.13], nous dirons que les représentations V_i , $i = 1, \dots, r$, sont les représentations *fondamentales* de G . Dans chaque V_i , on fixe aussi un réseau rationnel $V_i(\mathbb{Z})$ stable par l'action de Γ et contenant un vecteur de plus haut poids e_i . Dans l'espace vectoriel V_i , nous noterons $\tilde{X}_i = G \cdot e_i$ l'orbite du vecteur de plus haut poids e_i sous l'action de G .

Définition 4.2.1 (Covolumes successifs). Pour g dans G , on définit les *covolumes successifs* $\mu_1(g), \dots, \mu_r(g)$ de $g\Gamma$ par

$$\mu_i(g) = \min\{\|gv\| ; v \in V_i(\mathbb{Z}) \cap \tilde{X}_i\}.$$

Remarque. Les quantités $\mu_i(g)$ ne dépendent en fait que de la projection de g dans G/Γ , car l'ensemble $V_i(\mathbb{Z}) \cap \tilde{X}_i$ est stable par l'action de Γ . Si $\bar{g} = g\Gamma$ est un élément de G/Γ , nous écrirons indifféremment $\mu_i(\bar{g})$ ou $\mu_i(g)$ pour ses covolumes successifs.

Remarque. Le choix d'une autre norme sur V_i change μ_i en une fonction comparable, à une constante multiplicative près. En fait, c'est souvent à cette constante multiplicative près qu'il faut comprendre μ_i . Par exemple, comme l'ensemble $P \backslash G(\mathbb{Q})/\Gamma$ est fini, il existe une partie finie C dans $G(\mathbb{Q})$ telle que pour tout g ,

$$\mu_i(g) \asymp \min\{\|g\gamma c e_i\| ; c \in C, \gamma \in \Gamma\}.$$

Les plus hauts poids $\omega_1, \dots, \omega_r$ des représentations fondamentales s'identifient naturellement à une base de \mathfrak{a}^* , et il existe donc un unique élément $c_0(g) \in \mathfrak{a}$ tel que

$$\forall i \in [1, r], \quad \omega_i(c_0(g)) = \log \mu_i(g).$$

La théorie de la réduction permet de montrer que l'application c_0 que nous venons de définir est essentiellement à valeurs dans \mathfrak{a}^- . Ci-dessous, et dans toute la suite, on munit \mathfrak{a} d'une structure euclidienne invariante par l'action du groupe de Weyl.

Proposition 4.2.2 (Covolumes successifs et chambre de Weyl). *Il existe $C_0 \geq 0$ tel que pour tout g dans G , $d(c_0(g), \mathfrak{a}^-) \leq C_0$.*

Démonstration. Soient $\mathfrak{S} = KA_\tau\omega$ et $C \subset G(\mathbb{Q})$ l'ensemble de Siegel et la partie finie donnés par le théorème 4.1.2. Pour tout g dans G , il existe une décomposition de Siegel

$$g = kanc\gamma, \quad \text{avec } k \in K, n \in \omega, c \in C, \gamma \in \Gamma \text{ et } a = e^Y, Y \in \mathfrak{a}_t^-.$$

Alors, pour chaque i , $\mu_i(g) = \mu_i(anc) \asymp \mu_i(an)$, car l'ensemble $cV_i(\mathbb{Z}) \cap \tilde{X}_i$ est commensurable à $V_i(\mathbb{Z}) \cap \tilde{X}_i$: si D est un dénominateur commun des coefficients des éléments de C et de leurs inverses dans la représentation V_i ,

$$DV_i(\mathbb{Z}) \cap \tilde{X}_i \subset cV_i(\mathbb{Z}) \cap \tilde{X}_i \subset \frac{1}{D}V_i(\mathbb{Z}) \cap \tilde{X}_i.$$

Ensuite, on remarque que ana^{-1} est un élément borné dans G lorsque a varie dans A_τ et n dans ω , de sorte que pour tout $v \in V_i(\mathbb{Z}) \setminus \{0\}$,

$$\|anv\| \asymp \|av\| \gg e^{\omega_i(Y)},$$

car $e^{\omega_i(Y)}$ est essentiellement la plus petite valeur propre de a dans V_i . Cela montre que $\mu_i(g) \gg e^{\omega_i(Y)}$, i.e. $\log \mu_i(g) \geq \omega_i(Y) - O(1)$. Comme $\|g\gamma^{-1}c^{-1}e_i\| \asymp e^{\omega_i(Y)}$, on a en fait $\mu_i(g) \asymp e^{\omega_i(Y)}$ et donc $\log \mu_i(g) = \omega_i(Y) + O(1)$. En d'autres termes,

$$d(c_0(g), Y) = O(1),$$

et cela montre ce qu'on veut, car par définition de $A_\tau = \exp \mathfrak{a}_\tau^-$, l'élément Y est à distance bornée de \mathfrak{a}^- . \square

Exercice 2. Vérifier que pour $G = \mathrm{GL}_d$, la proposition ci-dessus est exactement équivalente au second théorème de Minkowski, sans l'optimalité des constantes.

Comme il est plus commode de travailler avec des éléments qui sont vraiment dans \mathfrak{a}^- , plutôt que dans un petit voisinage, nous remplaçons la fonction c_0 sur G par une fonction c , qui lui est proche, mais à valeurs dans \mathfrak{a}^- . On munit \mathfrak{a} d'un produit scalaire invariant par l'action du groupe de Weyl. Comme \mathfrak{a}^- est une partie convexe de \mathfrak{a} on dispose d'une projection $p_{\mathfrak{a}^-} : \mathfrak{a} \rightarrow \mathfrak{a}^-$, qui à Y_0 associe l'unique élément Y tel que $d(Y_0, Y) = d(Y_0, \mathfrak{a}^-)$.

Définition 4.2.3. On définit la fonction $c : G \rightarrow \mathfrak{a}^-$ par la formule

$$c(g) = p_{\mathfrak{a}^-}(c_0(g)).$$

Remarque. D'après la proposition 4.2.2, on a $c(g) = c_0(g) + O(1)$. En effet, $c(g)$ est le point de \mathfrak{a}^- le plus proche de $c_0(g)$.

La fonction $c(g)$ sur G/Γ s'interprète naturellement à partir de la théorie de la réduction, c'est le contenu de la proposition suivante, qui apparaît implicitement dans la démonstration de la proposition 4.2.2.

Proposition 4.2.4 (Composante diagonale d'une décomposition de Siegel). *Si $g = kanc\gamma$ est une décomposition de Siegel de g , alors la composante a est bien déterminée à une constante multiplicative près. En fait,*

$$a = e^{c(g)+O(1)}.$$

Démonstration. Dans la représentation fondamentale V_i , les réseaux $V_i(\mathbb{Z})$ et $\sum_{c \in C} cV_i(\mathbb{Z})$ sont commensurables, donc leurs minima successifs sont comparables. L'écriture $g = kanc\gamma$ montre donc que le premier minimum $\lambda_1(gV_i(\mathbb{Z}))$ est comparable à $e^{\omega_i(Y)}$, où $a = e^Y$, $Y \in \mathfrak{a}_i^-$, et ce premier minimum est atteint sur un point de $V_i(\mathbb{Z}) \cap \tilde{X}_i$. Par conséquent, pour chaque i , $\omega_i(Y) = \log \lambda_1(gV_i(\mathbb{Z})) + O(1) = \log \mu_i(g) + O(1) = \omega_i(c(g)) + O(1)$, ce qu'il fallait démontrer. \square

4.3 Drapeau partiel associé à un réseau

Nous avons vu que dans une décomposition de Siegel $g = kanc\gamma$, l'élément a ne dépend pas du choix de la décomposition, à constante multiplicative près. Selon la position de a dans A_τ , la classe de l'élément $c\gamma$ modulo un certain sous-groupe parabolique P_g dépendant de g est aussi indépendante de la décomposition. Nous détaillons maintenant cette construction, dont les idées nous seront utiles plus tard.

Rappelons que $\Pi = \{\alpha_1, \dots, \alpha_r\}$ est une base du système de racines de G pour T , pour un ordre associé au parabolique minimal B . À chaque partie $\theta \subset \Pi$ on

associe un sous-groupe parabolique de la façon suivante : on définit un sous-tore de T par

$$S_\theta = \left(\bigcap_{\alpha \in \theta} \ker \alpha \right)^0$$

puis

$$P_\theta = Z(S_\theta)U,$$

où $Z(S_\theta)$ désigne le centralisateur de S_θ dans G , et U le radical unipotent de B . Les poids de T dans la représentation adjointe sur l'algèbre de Lie \mathfrak{p}_θ correspondent aux racines positives et aux racines négatives dont la décomposition en racines simples est faite d'éléments de θ .

Proposition 4.3.1 (Drapeau partiel associé à $g\Gamma$). *Soit \mathfrak{S} un ensemble de Siegel pour G et C une partie finie de $G(\mathbb{Q})$ telle que $G = \mathfrak{S}C\Gamma$. Il existe une constante $C_0 \geq 0$ telle que l'énoncé suivant soit vérifié. Pour $g \in G$, soit*

$$\theta_g = \{i \in [1, r] \mid \alpha_i(c(g)) \geq -C_0\}$$

et $Q_g = P_{\theta_g}$ le sous-groupe parabolique associé. Si Q est un sous-groupe parabolique contenant Q_g , alors dans une décomposition de Siegel

$$g = kanc\gamma, \quad \text{avec } kan \in \mathfrak{S}, c \in C, \text{ et } \gamma \in \Gamma,$$

la classe $D_g = Qc\gamma \in Q \backslash G$ est indépendante du choix de la décomposition de Siegel. De plus, l'application $h \mapsto D_h$ est localement constante.

Remarque. Si $c(g) = 0$, on a nécessairement $Q = G$, et la proposition ne donne aucune information supplémentaire sur $g\Gamma$.

Exemple. Dans le cas où $G = \mathrm{SL}_d$, l'espace Ω s'identifie à l'espace des réseaux unimodulaires de \mathbb{R}^d . Notons

$$\lambda_1(g) \leq \dots \leq \lambda_d(g)$$

les minima successifs de $g\mathbb{Z}^d$, et choisissons une famille linéairement indépendante v_1, \dots, v_d dans \mathbb{Z}^d telle que

$$\forall i \in [1, d], \quad \|gv_i\| = \lambda_i(g).$$

La condition $\alpha_i(c(g)) \geq -C_0$ se traduit en termes des minima successifs par l'inégalité

$$\lambda_{i+1}(g) \leq e^{C_0} \lambda_i(g).$$

Si $i \notin \theta_g$, on a donc $\lambda_{i+1}(g) > \lambda_i(g)$, et le sous-réseau $\Delta_i = \mathbb{Z}v_{i+1} \oplus \dots \oplus \mathbb{Z}v_i$ est uniquement défini. Le drapeau D_g s'identifie au drapeau partiel

$$\{0\} < \Delta_{i_1} < \dots < \Delta_{i_k} < \mathbb{Z}^d, \quad \{i_1, \dots, i_k\} = [1, r] \setminus \theta_g.$$

À cause du cas particulier donné en exemple ci-dessus, nous dirons que D_g est le *drapeau partiel* associé à l'élément $g \in \Omega$. La démonstration de la proposition 4.3.1 repose sur l'observation importante suivante.

Proposition 4.3.2 (Racine et covolume). *Soit G un \mathbb{Q} -groupe semi-simple et V_k la représentation fondamentale de G associée au poids ω_k . Soit g dans G et v_0 dans $V_k(\mathbb{Z}) \cap \tilde{X}_k$ tel que $\mu_k(g) = \|gv_0\|$. Pour tout vecteur $v \in V_k(\mathbb{Z})$ linéairement indépendant de v_0 .*

$$\|gv\| \gg e^{-\alpha_k(c(g))} \mu_k(g).$$

La constante implicite dans la notation de Vinogradov ne dépend pas de $g \in G$. En outre, il existe une constante $C_0 \geq 0$ telle que si $\alpha_k(c(g)) \leq -C_0$, et $g = \text{kanc}\gamma$ est une décomposition de Siegel de g , alors v_0 est colinéaire à $\gamma^{-1}c^{-1}e_k$.

Démonstration. Dans cette démonstration, on munit l'espace des racines d'un produit scalaire invariant par l'action du groupe de Weyl. Quitte à changer le réseau rationnel $V_k(\mathbb{Z})$, on peut supposer qu'on dispose d'une base (u_i) de $V_k(\mathbb{Z})$ constituée de vecteurs de poids. Le plus haut poids ω_k est associé au vecteur $e_k = u_1$, et tout autre poids de la représentation peut s'écrire

$$\omega = \omega_k - \sum_i n_i \alpha_i,$$

où les n_i sont des entiers naturels. De plus, comme ω_k est le plus haut poids de la représentation et $\langle \omega_k, \alpha_i \rangle = 0$ si $i \neq k$,

$$\|\omega_k\|^2 \geq \|\omega\|^2 = \|\omega_k\|^2 + \left\| \sum_i n_i \alpha_i \right\|^2 - 2n_k \langle \omega_k, \alpha_k \rangle,$$

et donc $n_k \geq 1$ si $\omega \neq \omega_k$.

Par abus de notation, on note encore ω_k le caractère de B associé au poids ω_k . Posons $\Phi : g \mapsto \|ge_k\|$. Bien sûr,

$$\forall b \in B, \quad \Phi(gb) = |\omega_k(b)| \cdot \Phi(g),$$

i.e. Φ est une fonction de type (B, ω_k) , au sens de Borel [8, §14.1]. En outre,

$$\forall \gamma \in \Gamma \cap B, \quad |\omega_k(\gamma)| = 1,$$

et donc Φ est invariante à droite par $\Gamma \cap B$. Soit enfin

$$\theta = \{i \mid \langle \alpha_i, \omega_k \rangle > 0\} = \{k\} \quad \text{et} \quad \theta' = [1, r] \setminus \{k\}.$$

Alors, $P_{\theta'} = \text{Stab } \mathbb{R}e_k$, donc, si $L_{\theta'}$ désigne un sous-groupe semi-simple (donc sans caractère) de $P_{\theta'}$, on doit avoir

$$\forall \ell \in L_{\theta'}, \quad \Phi(g\ell) = \|g\ell e_k\| = |\omega_k(\ell)| \cdot \|ge_k\| = \|ge_k\| = \Phi(g),$$

ce qui montre que Φ est invariante à droite par $L_{\theta'}$. D'après Borel [8, théorème 16.9], il existe une partie finie $C' \subset G(\mathbb{Q})$ et un ensemble de Siegel $\mathfrak{S} = KA_\tau\omega$ tels que pour tout $g \in G$, la fonction

$$\begin{aligned} \Phi_g : \Gamma C' &\rightarrow \mathbb{R}^+ \\ u &\mapsto \Phi(gu), \end{aligned}$$

atteint son minimum en un point de $\Gamma C' \cap g^{-1}\mathfrak{S}$. Remarquons qu'à une constante multiplicative près,

$$\mu_k(g) \asymp \min\{\Phi_g(u) ; u \in \Gamma C'\}.$$

Soit donc $u = \gamma'c' \in \Gamma C'$ tel que

$$\|g\gamma'c'e_k\| = \Phi_g(\gamma'c') = \min\{\|g\gamma'c'e_k\| ; c' \in C', \gamma' \in \Gamma\},$$

et, suivant l'ensemble de Siegel choisi ci-dessus,

$$g\gamma'c' = kan.$$

Comme les réseaux $gV_k(\mathbb{Z})$ et $g\gamma'c'V_k(\mathbb{Z})$ sont commensurables, leurs minima successifs sont comparables. Dans la base de $V_k(\mathbb{Z})$ constituée de vecteurs de poids, l'élément $a = e^{c(g)+O(1)}$ agit suivant la matrice $\text{diag}(e^{\omega(c(g))})$, où ω décrit les poids de la représentation V_k ; à une constante multiplicative près, cela donne tous les minima successifs de $gV_k(\mathbb{Z})$. La plus petite valeur propre de a est $\mu_k(g) \asymp e^{\omega_k(c(g))}$. Si $\omega = \omega_k - \sum_i n_i \alpha_i$ est un poids différent de ω_k , alors d'après le calcul ci-dessus, $n_k \geq 1$, et donc

$$e^{\omega(c(g))} \geq e^{\omega_k(c(g)) - \alpha_k(c(g))} = e^{-\alpha_k(c(g))} \mu_k(g).$$

Soit maintenant $v \in V_k(\mathbb{Z})$. Si $(e_\omega)_\omega$ désigne une base de $V_k(\mathbb{Z})$ constituée de vecteurs de poids, le réseau engendré par les vecteurs $\gamma'c'e_\omega$ est commensurable à $V_k(\mathbb{Z})$ à un facteur borné près. Pour un certain entier D indépendant de v , on peut donc écrire

$$Dgv = \sum_\omega n_\omega g\gamma'c'e_\omega = \sum_\omega n_\omega kane_\omega,$$

avec $n_\omega \in \mathbb{N}$, et les termes de cette somme sont essentiellement orthogonaux. Si v n'est pas colinéaire à v_0 , il existe $\omega \neq \omega_k$ tel que $|n_\omega| \geq 1$, et cela implique

$$\|gv\| \gg \frac{1}{D} \|kane_\omega\| \gg e^{\omega(c(g))} \geq e^{-\alpha_k(c(g))} \mu_k(g).$$

La dernière assertion découle de cette inégalité et de ce que si $g = kanc\gamma$ est une décomposition de Siegel de g , alors

$$\|g\gamma^{-1}c^{-1}e_k\| \asymp \|ae_k\| \asymp e^{\omega_k(c(g))} \asymp \mu_k(g).$$

□

Démonstration de la proposition 4.3.1. Pour $k \in [1, r]$, soit $P_k = P_{[1, r] \setminus \{k\}}$ le k -ième sous-groupe parabolique maximal. Comme

$$Q_g = P_{\theta_g} = \bigcap_{k \notin \theta_g} P_k,$$

il suffit de montrer que pour chaque $k \notin \theta_g$, l'élément $P_k c \gamma$ ne dépend pas du choix de la décomposition de Siegel.

Soit donc $k \notin \theta_g$ fixé, et V_k la représentation fondamentale associée. Si C_0 est choisi assez grand, l'inégalité $\alpha_k(c(g)) < -C_0$, avec la proposition 4.3.2, montre que si $g = kanc\gamma$ est une décomposition de Siegel et $u \in V_k(\mathbb{Z})$, l'égalité

$$\|gu\| = \mu_k(g),$$

ne peut être atteinte que si u est colinéaire à $\gamma^{-1}c^{-1}e_k$. Identifiant $P_k \backslash G$ à l'orbite de la droite $[e_k]$ de plus haut poids dans la représentation fondamentale V_k ,

grâce à l'application $g \mapsto [g^{-1}e_k]$, cela montre que $P_k c\gamma$ ne dépend pas du choix de la représentation de Siegel : c'est la direction qui réalise le premier minimum $\lambda_1(gV_k(\mathbb{Z}))$ du réseau $gV_k(\mathbb{Z})$.

Pour chaque $k \notin \theta_g$, la proposition 4.3.2 montre que $\lambda_1(gV_k(\mathbb{Z})) < \lambda_2(gV_k(\mathbb{Z}))$, donc le vecteur de $V_k(\mathbb{Z})$ qui réalise le premier minimum est localement constant au voisinage de g . Cela montre la dernière assertion de la proposition. \square

4.4 Une relation d'ordre sur \mathfrak{a}

Nous utiliserons la relation d'ordre partiel sur \mathfrak{a} donnée par

$$Y_1 \prec Y_2 \iff \forall i, \omega_i(Y_1) \leq \omega_i(Y_2).$$

En particulier, nous nous intéresserons à l'ensemble des minorants de $c_0(g)$ dans \mathfrak{a}^- . C'est un ensemble convexe, et la proposition suivante montre qu'il est stable par une opération de maximum.

Proposition 4.4.1. *Si $(Y_s)_{s \in S}$ est une famille d'éléments de \mathfrak{a}^- alors l'élément $Y \in \mathfrak{a}$ défini par*

$$\forall i, \omega_i(Y) = \sup_{s \in S} \omega_i(Y_s)$$

est dans \mathfrak{a}^- . En particulier, pour tout $Y_0 \in \mathfrak{a}$ l'ensemble

$$m_{Y_0} = \{Y \in \mathfrak{a}^- \mid Y \prec Y_0\}.$$

admet un unique plus grand élément.

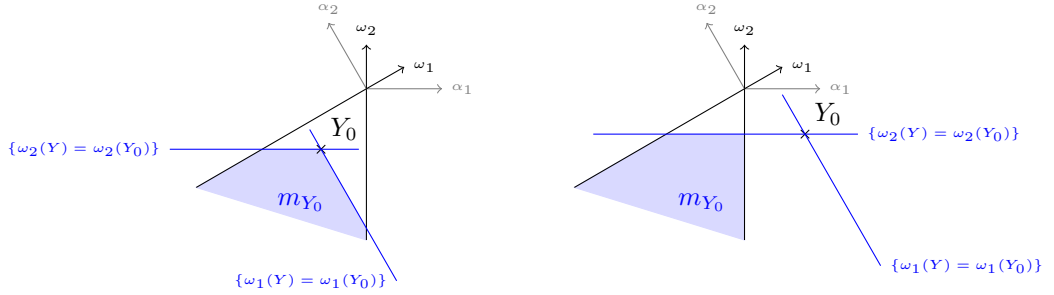


FIGURE 4.2 : L'ensemble m_{Y_0} pour SL_3

Démonstration. Dans cette démonstration on identifie \mathfrak{a} à \mathfrak{a}^* grâce au produit scalaire usuel. La famille des poids fondamentaux (ϖ_j) s'identifie alors à la base duale de la base (α_i) des racines simples :

$$\forall i, j, \quad \langle \alpha_i, \varpi_j \rangle = \delta_{ij}.$$

Rappelons que le plus haut poids ω_i est relié à ϖ_i par $\omega_i = b_i \varpi_i$, pour un certain $b_i \in \mathbb{N}^*$. Si l'on décompose

$$Y_s = \sum_i t_i^{(s)} \alpha_i, \quad \text{avec } t_i^{(s)} \in \mathbb{R},$$

alors $Y = \sum_i (\sup_s t_i^{(s)}) \alpha_i$ et

$$\langle \alpha_k, Y \rangle = \langle \alpha_k, \sum_i (\sup_s t_i^{(s)}) \alpha_i \rangle = \sum_i (\sup_s t_i^{(s)}) \langle \alpha_k, \alpha_i \rangle.$$

Il s'agit de voir que cette quantité est négative. Cela découle de ce que pour $i \neq k$, $\langle \alpha_k, \alpha_i \rangle \leq 0$, tandis que $\langle \alpha_k, \alpha_k \rangle \geq 0$. En effet, pour chaque s , l'inégalité $\langle \alpha_k, Y_s \rangle \leq 0$ donne

$$-\sum_{i \neq k} t_i^{(s)} \langle \alpha_k, \alpha_i \rangle \geq \langle \alpha_k, \alpha_k \rangle t_k^{(s)}$$

et comme pour tout $i \neq k$, $\langle \alpha_k, \alpha_i \rangle \leq 0$, cela implique

$$-\sum_{i \neq k} (\sup_u t_i^{(u)}) \langle \alpha_k, \alpha_i \rangle \geq \langle \alpha_k, \alpha_k \rangle t_k^{(s)}.$$

Comme ceci vaut pour tout s , on trouve bien

$$-\sum_{i \neq k} (\sup_u t_i^{(u)}) \langle \alpha_k, \alpha_i \rangle \geq \langle \alpha_k, \alpha_k \rangle \sup_s t_k^{(s)},$$

c'est-à-dire $\alpha_k(Y) \leq 0$. Soit maintenant $Y_0 \in \mathfrak{a}$ un élément quelconque. Comme m_{Y_0} est non vide, la propriété de stabilité que nous venons de démontrer permet de définir son plus grand élément Y par

$$\forall i, \omega_i(Y) = \sup_{Y' \in m_{Y_0}} \omega_i(Y').$$

□

Exercice 3. Soit $G = \mathrm{SL}_d$. On identifie \mathfrak{a} aux fonctions sur $\{0, \dots, d\}$ qui s'annulent en 0 et d par l'application $Y_0 \mapsto (\omega_i(Y_0))_{1 \leq i \leq d-1}$.

1. Montrer que \mathfrak{a}^- s'identifie à l'ensemble des fonctions convexes négatives.
2. Vérifier que la proposition ci-dessus traduit simplement le fait que la borne supérieure d'une famille de fonctions convexes négatives est encore une fonction convexe négative.

Le dessin ci-dessous donne un exemple pour SL_4 . On identifie \mathfrak{a} aux fonctions sur $\{0, \dots, 4\}$ qui s'annulent en 0 et 4, et \mathfrak{a}^- au sous-ensemble des fonctions convexes.

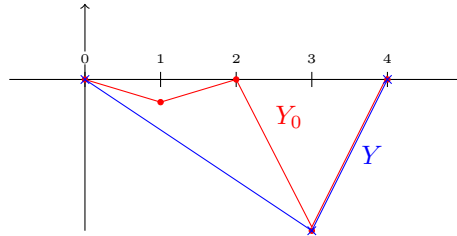


FIGURE 4.3 : Y est le plus grand minorant de Y_0 dans \mathfrak{a}^- .

En fait, le plus grand élément de m_{Y_0} s'interprète géométriquement comme une projection de Y_0 sur \mathfrak{a}^- . On munit \mathfrak{a} du produit scalaire usuel, invariant par l'action du groupe de Weyl. Comme \mathfrak{a}^- est une partie convexe de \mathfrak{a} on dispose d'une projection $p_{\mathfrak{a}^-} : \mathfrak{a} \rightarrow \mathfrak{a}^-$, qui à Y_0 associe l'unique élément Y tel que $d(Y_0, Y) = d(Y_0, \mathfrak{a}^-)$.

Proposition 4.4.2 (Plus grand minorant et projection orthogonale). *Pour tout Y_0 dans \mathfrak{a} , le point $p_{\mathfrak{a}^-}(Y_0)$ est le plus grand élément de m_{Y_0} .*

Démonstration. Ici encore, on identifie \mathfrak{a} à \mathfrak{a}^* à l'aide du produit scalaire usuel. Soit $Y_0 \in \mathfrak{a}$, et

$$I_0 = \{i \mid \langle \alpha_i, Y_0 \rangle \geq 0\}.$$

Soit Y_1 la projection orthogonale de Y_0 sur la face $\bigcap_{i \in I_0} \alpha_i^\perp$, donnée par

$$Y_1 = Y_0 - \sum_{i \in I_0} t_i^{(0)} \alpha_i,$$

où les $t_i^{(0)}$ sont choisis de sorte que pour tout $j \in I_0$, $\langle \alpha_j, Y_0 \rangle = \sum_{i \in I_0} t_i^{(0)} \langle \alpha_j, \alpha_i \rangle$. Si $A = (\langle \alpha_i, Y_0 \rangle)_{i \in I_0}$, ces équations s'écrivent matriciellement $A = G \cdot T^{(0)}$, où $G = (\langle \alpha_j, \alpha_i \rangle)_{i, j \in I_0}$. Comme G est une matrice de Gram telle que $\langle \alpha_j, \alpha_i \rangle \leq 0$ si $i \neq j$, c'est une matrice inversible, et G^{-1} est à coefficients positifs, d'après [11, Chapitre V, §3, n° 6, Lemme 6, page 79]. Or A est à coefficients positifs aussi, et donc le vecteur $T^{(0)} = G^{-1}A$ est à coefficients positifs. Cela revient à dire que pour tout i , $\omega_i(Y_1) \leq \omega_i(Y_0)$, i.e. $Y_1 \prec Y_0$.

De même, à partir de Y_1 , on définit $I_1 = \{i \mid \langle \alpha_i, Y_1 \rangle \geq 0\}$, et Y_2 la projection orthogonale de Y_1 sur $\bigcap_{i \in I_1} \alpha_i^\perp$, ...etc. On obtient ainsi une suite de points

$$Y_0 \succ Y_1 \succ Y_2 \succ \dots$$

Notons que pour tout n , $I_n \subset I_{n+1}$. En effet, si $\langle \alpha_i, Y_n \rangle \geq 0$, alors par définition, $\langle \alpha_i, Y_{n+1} \rangle = 0$. En particulier, la suite (I_n) est stationnaire, donc la suite (Y_n) aussi. Soit Y sa limite et $I = \{i \mid \langle \alpha_i, Y \rangle = 0\}$.

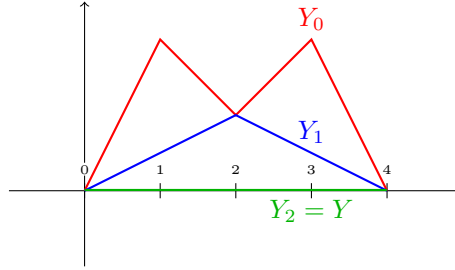


FIGURE 4.4 : Une suite $Y_0 \succ Y_1 \succ Y_2$ pour $G = \text{SL}_4$

Naturellement $Y \in \mathfrak{a}^-$, et par construction,

$$Y = Y_0 - \sum_{i \in I} t_i \alpha_i, \quad \forall i, t_i \geq 0.$$

Donc Y est la projection orthogonale de Y_0 sur $\bigcap_{i \in I} \alpha_i^\perp$.

Pour voir que Y est bien égal à la projection de Y_0 sur \mathfrak{a}^- , on vérifie que pour tout Y' dans \mathfrak{a}^- , $\langle Y' - Y, Y_0 - Y \rangle \leq 0$. Écrivons $Y' - Y = \sum_i s_i \varpi_i$. Pour $i \in I$, $\langle \alpha_i, Y \rangle = 0$ et $\langle \alpha_i, Y' \rangle \leq 0$, donc $s_i \leq 0$. Par conséquent,

$$\langle Y' - Y, Y_0 - Y \rangle = \sum_{i \in [1, r], j \in I} s_i t_j \langle \alpha_j, \varpi_i \rangle = \sum_{i \in [1, r], j \in I} s_i t_j \delta_{ij} = \sum_{i \in I} s_i t_i \leq 0.$$

Donc Y est la projection de Y_0 sur \mathfrak{a}^- . Reste à voir que c'est bien le plus grand minorant de Y_0 dans \mathfrak{a}^- .

Tout d'abord, par construction, Y est bien un minorant de Y_0 . Soit maintenant $Y' \in \mathfrak{a}^-$ un autre minorant de Y_0 . Pour tout $i \notin I$, $\omega_i(Y) = \omega_i(Y_0) \geq \omega_i(Y')$, et le lemme ci-dessous permet d'en conclure l'inégalité souhaitée : $Y' \prec Y$. \square

Nous concluons cette partie par le lemme technique utilisé dans la démonstration ci-dessus, et dont nous ferons encore usage au chapitre suivant.

Lemme 4.4.3. *Soit $Y \in \mathfrak{a}^-$, et $I = \{i \mid \alpha_i(Y) = 0\}$. Si $Y' \in \mathfrak{a}^-$ vérifie pour chaque $i \notin I$, $\omega_i(Y') \leq \omega_i(Y)$, alors $Y' \prec Y$.*

Démonstration. Écrivons

$$Y - Y' = \sum_i s_i \alpha_i, \quad \text{avec } s_i \in \mathbb{R}.$$

Par hypothèse $\omega_j(Y) \geq \omega_j(Y')$ si $j \notin I$, et donc

$$\forall j \notin I, \quad s_j \geq 0.$$

D'autre part, pour $i \in I$, $\alpha_i(Y - Y') = -\alpha_i(Y') \geq 0$, et donc

$$\forall i \in I, \quad \sum_j s_j \langle \alpha_i, \alpha_j \rangle \geq 0.$$

Par conséquent,

$$\forall i \in I, \quad \sum_{j \in I} s_j \langle \alpha_i, \alpha_j \rangle \geq - \sum_{j \notin I} s_j \langle \alpha_i, \alpha_j \rangle \geq 0.$$

Cette inégalité peut encore s'écrire $G \cdot S \geq 0$, où $G = (\langle \alpha_i, \alpha_j \rangle)_{i, j \in I}$ et $S = (s_j)_{j \in I}$. Comme G^{-1} est à coefficients positifs, cela implique $S \geq 0$. Ainsi, pour tout i , $s_i \geq 0$, i.e. $Y' \prec Y$. \square

Remarque. Dans le cas $G = \text{SL}_d$, le contenu de ce dernier lemme est assez clair. Si Y est une fonction convexe sur $[0, d]$ (segment d'entiers) avec $Y(0) = Y(d) = 0$, et si Y' est une autre fonction convexe sur $[0, d]$, inférieure à Y en tout point angulaire (i.e. extrémal du graphe), alors la fonction Y' est toujours inférieure à la fonction Y .

Chapitre 5

Approximation des points algébriques

Dans tout ce mémoire, contrairement à l'usage le plus répandu, on note $\overline{\mathbb{Q}}$ le sous-corps de \mathbb{R} constitué des nombres algébriques sur \mathbb{Q} .

Comme précédemment, $X = P \backslash G$ est une variété de drapeaux, munie de sa distance de Carnot-Carathéodory, et d'une hauteur H_χ induite par une représentation linéaire irréductible de G de plus haut poids χ . Rappelons que nous avons défini l'exposant diophantien d'un point x dans $X(\mathbb{R})$ par

$$\beta_\chi(x) = \inf\{\beta \in \mathbb{R} \mid \exists c > 0 : \forall v \in X(\overline{\mathbb{Q}}), d(x, v) \geq cH_\chi(v)^{-\beta}\},$$

et qu'il existe une constante $\beta_\chi(X)$ telle que pour presque tout x dans $X(\mathbb{R})$, $\beta_\chi(x) = \beta_\chi(X)$.

Dans ce chapitre, nous étudions l'exposant diophantien $\beta_\chi(x)$ d'un point $x \in X(\overline{\mathbb{Q}})$, où $\overline{\mathbb{Q}}$ désigne le sous-corps de \mathbb{R} constitué des éléments algébriques sur \mathbb{Q} . À l'aide des outils de la théorie de la réduction rappelés à la partie précédente, le théorème du sous-espace de Schmidt nous permettra de décrire le comportement asymptotique des orbites diagonales dans l'espace de réseaux $\Omega = G/\Gamma$. Ensuite, grâce à la correspondance développée au chapitre 2 nous pourrons traduire ces résultats en termes d'approximation diophantienne des points de X .

5.1 Orbites diagonales algébriques dans G/Γ

Dans ce paragraphe, G est un \mathbb{Q} -groupe semi-simple, $T \subset G$ un tore \mathbb{Q} -déployé maximal, $A = T^0(\mathbb{R})$ la composante neutre des points réels de T , et \mathfrak{a} son algèbre de Lie. Soit $(a_t)_{t>0}$ un sous-groupe à un paramètre de A . Écrivant $a_t = e^{tY}$ pour un certain $Y \in \mathfrak{a}$, on peut choisir un ordre sur \mathfrak{a} de sorte que Y appartienne à la chambre de Weyl négative \mathfrak{a}^- dans \mathfrak{a} :

$$\forall t \in \mathbb{R}, a_t = e^{tY}, \quad Y \in \mathfrak{a}^-.$$

Remarque. Dans ce paragraphe, l'élément Y est quelconque dans \mathfrak{a} , et nous n'étudions que l'espace de réseaux $\Omega = G/\Gamma$. Plus tard, nous choisirons l'élément Y

comme en (2.1), et la correspondance établie au chapitre 2 nous permettra d'obtenir les résultats l'approximation diophantienne que nous avons en vue.

Soit alors B le \mathbb{Q} -sous-groupe parabolique minimal correspondant à l'ensemble des racines positives pour l'ordre choisi sur \mathfrak{a} , et

$$P = \{g \in G \mid \lim_{t \rightarrow \infty} a_t g a_{-t} \text{ existe}\}$$

le sous-groupe parabolique associé à (a_t) . Soit W le groupe de Weyl associé à G et T , quotient du normalisateur de T par son centralisateur, et

$$W_P = (W \cap P) \backslash W.$$

La décomposition de Bruhat [10, Théorème 5.15] de G permet d'écrire

$$G = \bigsqcup_{w \in W_P} PwB.$$

On fixe aussi un sous-groupe compact maximal K dans $G(\mathbb{R})$. Enfin, étant donné un sous-groupe arithmétique Γ dans G , on fixe une partie finie $C \subset G(\mathbb{Q})$ et un ensemble de Siegel $\mathfrak{S} = KA_u\omega$ par rapport à K , B et T tel que

$$G = \mathfrak{S}CT.$$

Rappelons qu'une décomposition de Siegel d'un élément $g \in G$ est une écriture de g sous la forme $g = kan\gamma$, avec $k \in K$, $a \in A_u = \exp \mathfrak{a}_u^-$, $n \in \omega$ et $\gamma \in CT$. Ce paragraphe a pour but le théorème suivant.

Théorème 5.1.1 (Orbites diagonales des points algébriques dans Ω). *Soit $Y \in \mathfrak{a}^-$, et $(a_t) = (e^{tY})_{t>0}$ le sous-groupe à un paramètre associé. Soit $s \in G(\mathbb{Q})$. Pour tout $t > 0$, soit*

$$a_t s = k_t b_t n_t \gamma_t,$$

une décomposition de Siegel de $a_t s$.

1. Il existe un élément $c_\infty \in \mathfrak{a}^-$ tel que $\lim_{t \rightarrow \infty} \frac{1}{t} \log b_t = c_\infty$.
2. Si $\theta_\infty = \{\alpha \in \Pi \mid \alpha(c_\infty) = 0\}$ et $Q_\infty = P_{\theta_\infty}$ est le sous-groupe parabolique associé à θ_∞ , alors $Q_\infty \gamma_t = Q_\infty \gamma_\infty$ est indépendant de t au voisinage de l'infini.
3. Soit $w \in W_P$ tel que $s\gamma_\infty^{-1} \in PwB$. Alors $c_\infty = p_{\mathfrak{a}^-}(Y^w)$, où $Y^w = (\text{Ad } w)^{-1}Y$, et $p_{\mathfrak{a}^-} : \mathfrak{a} \rightarrow \mathfrak{a}^-$ désigne la projection sur le convexe \mathfrak{a}^- .

Remarque. Soit $c : G \rightarrow \mathfrak{a}^-$ la fonction définie au chapitre 4, telle que si $g = kan\gamma$ est une décomposition de Siegel, alors $a = e^{c(g)+O(1)}$. Le premier point du théorème se réécrit $\lim_{t \rightarrow \infty} \frac{1}{t} c(a_t s) = c_\infty$. Avec les notations de la proposition 4.3.1, cela implique en particulier que pour tout $t > 0$ assez grand, $Q_{a_t s} \subset Q_\infty$. Le second point énonce alors que le drapeau partiel $D_{a_t s} \in Q_\infty \backslash G$ associé à $a_t s$ est constant au voisinage de l'infini.

Remarque. Vu l'énoncé du théorème, la formule pour c_∞ ne doit pas dépendre du choix de γ_∞ . En d'autres termes c_∞ est déterminé par la variété $PwQ_\infty\gamma_\infty$ contenant s . C'est d'ailleurs ce que donne la démonstration du théorème.

La démonstration du théorème 5.1.1 repose sur le théorème suivant, dû à Schmidt [53, Theorem 3A].

Théorème 5.1.2 (Théorème du sous-espace fort). *Soit (a_t) un sous-groupe diagonal à un paramètre dans $\mathrm{GL}_d(\mathbb{R})$ et $L \in \mathrm{GL}_d(\overline{\mathbb{Q}})$. Notons $\lambda_1(t) \leq \dots \leq \lambda_d(t)$ les minima successifs du réseau $a_t LZ^d$, pour $t > 0$, et supposons qu'il existe $\delta > 0$, $i \in [1, d]$, et un ensemble non borné \mathfrak{N} tels que,*

$$\forall t \in \mathfrak{N}, \quad \lambda_i(t) \leq e^{-\delta t} \lambda_{i+1}(t).$$

Alors, il existe un sous-espace rationnel $T \leq \mathbb{Q}^d$ de dimension i et un sous-ensemble non borné $\mathfrak{N}' \subset \mathfrak{N}$ tels que pour tout $t \in \mathfrak{N}'$, les i premiers minima successifs de $a_t LZ^d$ sont réalisés en des vecteurs v_1, \dots, v_i de $a_t LT$.

Ce théorème implique d'ailleurs la proposition suivante, qui décrit de façon plus précise le comportement de l'orbite dans l'espace des réseaux.

Proposition 5.1.3. *Soit (a_t) un sous-groupe diagonal à un paramètre dans $\mathrm{GL}_d(\mathbb{R})$ et $L \in \mathrm{GL}_d(\overline{\mathbb{Q}})$. Pour $t > 0$, notons $\lambda_1(t) \leq \dots \leq \lambda_d(t)$ les minima successifs du réseau $a_t LZ^d$. Alors, pour chaque $i \in [1, d]$ la limite*

$$\Lambda_i = \lim_{t \rightarrow \infty} \frac{1}{t} \log \lambda_i(t)$$

existe. De plus, si $\Lambda_i < \Lambda_{i+1}$, alors il existe un unique sous-espace rationnel S_i de dimension i tel que pour tout $t > 0$ suffisamment grand, les i premiers minima successifs de $a_t LZ^d$ sont atteints dans S_i .

Remarque. Les sous-espaces S_i forment un drapeau partiel dans \mathbb{Q}^d .

Démonstration. Pour $i = 1, \dots, d$, posons

$$\Lambda_i = \liminf_{t \rightarrow \infty} \frac{1}{t} \log \lambda_i(t).$$

On définit les indices $i_0, i_1, \dots, i_s, i_{s+1}$ par $i_0 = 0$, $i_{s+1} = d$, et

$$\Lambda_1 = \dots = \Lambda_{i_1} < \Lambda_{i_1+1} = \dots = \Lambda_{i_2} < \dots < \Lambda_{i_s+1} = \dots = \Lambda_d.$$

Nous allons montrer par récurrence sur $k \in [0, s]$ la propriété suivante : Il existe un drapeau partiel $0 = S_0 < S_1 < \dots < S_k$ de sous-espaces rationnels tel que pour chaque $\ell \in [1, k]$,

- $\dim S_\ell = i_\ell$;
- $\forall t > 0$ assez grand, $a_t LS_\ell$ contient les i_ℓ premiers minima de $a_t LZ^d$;
- si $i_{\ell-1} < i \leq i_\ell$, alors $\lim_{t \rightarrow \infty} \frac{1}{t} \log \lambda_i(t) = \Lambda_{i_\ell} = \frac{\tau(S_\ell) - \tau(S_{\ell-1})}{i_\ell - i_{\ell-1}}$.

Dans la formule ci-dessus, $\tau(W)$ désigne le taux de dilatation du sous-espace W par le flot $(a_t L)$. Si \mathbf{w} représente W dans une puissance extérieure de \mathbb{R}^d , dans la décomposition de $L\mathbf{w}$ suivant les espaces propres de a_t , la plus grande valeur propre apparaissant est égale à $e^{t\tau(W)}$. De manière équivalente,

$$\tau(W) = \lim_{t \rightarrow \infty} \frac{1}{t} \log \|a_t L\mathbf{w}\|.$$

Pour $k = 0$, la propriété est triviale. Supposons donc la propriété vraie pour $k - 1$, avec $k \in [1, s + 1]$. Soit (t_n) une suite qui tend vers l'infini telle que $\Lambda_{i_k} = \lim \frac{1}{t_n} \log \lambda_{i_k}(t_n)$. Posant $\delta = \frac{1}{3}(\Lambda_{i_{k+1}} - \Lambda_{i_k})$, on a, pour n suffisamment grand,

$$\lambda_{i_k}(a_{t_n} \Delta) \leq e^{t_n(\Lambda_{i_k} + \delta)} \leq e^{t_n(\Lambda_{i_{k+1}} - 2\delta)} \leq e^{-t_n \delta} \lambda_{i_{k+1}}(a_{t_n} \Delta).$$

D'après le théorème 5.1.2 ci-dessus, il existe un sous-espace rationnel S_k de dimension i_k tel que le long d'une sous-suite de (t_n) , les i_k premiers minima de $a_{t_n} L \mathbb{Z}^d$ sont toujours atteints dans $a_{t_n} L S_k$.

Par hypothèse de récurrence, pour $\ell < k$, si $i_{\ell-1} < i \leq i_\ell$,

$$\lim \frac{1}{t_n} \log \lambda_i(t_n) = \Lambda_{i_\ell},$$

et par définition de (t_n) et des indices i_{k-1} et i_k ,

$$\lim \frac{1}{t_n} \log \lambda_{i_k}(t_n) = \Lambda_{i_k} = \dots = \Lambda_{i_{k-1}+1} = \lim \frac{1}{t_n} \log \lambda_{i_{k-1}+1}(t_n).$$

Comme $a_{t_n} L S_k$ contient les i_k premiers minima, cela implique

$$\text{covol}_{a_{t_n} L S_k}(a_{t_n} L(S_k \cap \mathbb{Z}^d)) \leq e^{t_n \sum_{\ell=1}^k (i_\ell - i_{\ell-1}) \Lambda_{i_\ell} + o(t_n)}$$

d'où l'on tire

$$\tau(S_k) \leq \sum_{\ell=1}^k (i_\ell - i_{\ell-1}) \Lambda_{i_\ell}.$$

Mais d'après l'hypothèse de récurrence, $\tau(S_{k-1}) = \sum_{\ell=1}^{k-1} (i_\ell - i_{\ell-1}) \Lambda_{i_\ell}$, et donc

$$\frac{\tau(S_k) - \tau(S_{k-1})}{i_k - i_{k-1}} \leq \Lambda_{i_k} = \dots = \Lambda_{i_{k-1}+1}. \quad (5.1)$$

Comme l'hypothèse de récurrence implique $S_{k-1} \leq S_k$, le second théorème de Minkowski appliqué dans $a_t L S_k$, donne, pour tout $t > 0$ assez grand,

$$\begin{aligned} \lambda_{i_{k-1}+1}(t) \dots \lambda_{i_k}(t) &\ll \left(\frac{\text{covol}(a_t(S_k \cap \mathbb{Z}^d))}{\text{covol}(a_t(S_{k-1} \cap \mathbb{Z}^d))} \right) \\ &\leq \exp [t(\tau(S_k) - \tau(S_{k-1})) + o(t)]. \end{aligned}$$

Avec (5.1), cela montre qu'on doit avoir, pour chaque $i \in [i_{k-1} + 1, i_k]$,

$$\Lambda_i = \lim \frac{1}{t} \log \lambda_i(t) = \frac{\tau(S_k) - \tau(S_{k-1})}{i_k - i_{k-1}}.$$

Pour $\varepsilon = \frac{1}{3}(\Lambda_{i_{k+1}} - \Lambda_{i_k})$, pour $t > 0$ assez grand, le sous-réseau $a_t L(S_k \cap \mathbb{Z}^d)$ contient i_k vecteurs linéairement indépendants de norme inférieure à $e^{t(\Lambda_{i_k} + \varepsilon)}$, et comme $\Lambda_{i_{k+1}} > \Lambda_{i_k} + 2\varepsilon$, tout vecteur de $a_t L \mathbb{Z}^d$ hors de $a_t L S_k$ est de norme supérieure à $e^{t(\Lambda_{i_k} + 2\varepsilon)}$. Cela montre que pour $t > 0$ assez grand, les i_k premiers minima de $a_t L \mathbb{Z}^d$ sont atteints dans $a_t L S_k$. \square

Nous pouvons enfin démontrer le théorème 5.1.1.

Démonstration du théorème 5.1.1. Soit $\rho : G \rightarrow \mathrm{SL}_d$ une représentation rationnelle fidèle de G . Pour $t > 0$, et $i \in [1, d]$, notons $\lambda_i(t) = \lambda_i(\rho(a_t s)\mathbb{Z}^d)$. D'après le corollaire 5.1.3, les limites

$$\Lambda_i = \lim_{t \rightarrow \infty} \frac{1}{t} \log \lambda_i(t)$$

sont bien définies. Si $a_t s = k_t b_t n_t \gamma_t$ est une décomposition de Siegel de $a_t s$, alors, à une constante multiplicative près, les minima successifs de $\rho(a_t s)\mathbb{Z}^d$ s'obtiennent en ordonnant les valeurs propres de la matrice diagonale $\rho(b_t)$. Cela montre que la limite $\lim_{t \rightarrow +\infty} \frac{1}{t} \log \rho(b_t)$ est bien définie, et comme $\rho : A \rightarrow (\mathbb{R}_+^*)^d$ est un morphisme de groupes injectif, il en découle que la limite

$$c_\infty = \lim_{t \rightarrow \infty} \frac{1}{t} \log b_t$$

existe. Comme $d(\log b_t, \mathfrak{a}^-) = O(1)$, on a bien sûr $c_\infty \in \mathfrak{a}^-$. Cela montre le premier point du théorème. Ensuite, la proposition 4.3.1 montre que pour tout $t > 0$ suffisamment grand, l'application $t \mapsto Q_\infty \gamma_t$ est localement constante. Par connexité, elle est donc constante au voisinage de l'infini.

Fixons maintenant $\gamma_\infty \in G(\mathbb{Q})$ tel que pour tout t suffisamment grand, $Q_\infty \gamma_t = Q_\infty \gamma_\infty$. D'après la proposition 4.3.2, pour chaque $k \notin \theta_\infty$, le plus petit vecteur de $a_t s V_k(\mathbb{Z})$ est atteint dans la direction $a_t s \gamma_\infty^{-1} e_k$, et

$$\mu_k(a_t s) = \min\{\|g\mathbf{v}\| ; \mathbf{v} \in V_k(\mathbb{Z}) \cap \tilde{X}_k\} \asymp \|a_t s \gamma_\infty^{-1} e_k\|.$$

Écrivons $s \gamma_\infty^{-1} = p w b$, avec $p \in P$, $w \in W_P$ et $b \in B$. Alors, pour $t > 0$ grand,

$$\|a_t s \gamma_\infty^{-1} e_k\| \asymp \|a_t w b e_k\| \asymp \|a_t w e_k\| \asymp e^{t \omega_k(Y^w)}.$$

Cela montre déjà que pour $k \notin \theta_\infty$,

$$\omega_k(c_\infty) = \omega_k(Y^w).$$

Le même calcul pour $k \in \theta_\infty$ montre au moins que $\omega_k(c_\infty) \leq \omega_k(Y^w)$, et donc $c_\infty \prec Y^w$ puis

$$c_\infty \prec p_{\mathfrak{a}^-}(Y^w).$$

Réciproquement, notons que pour $k \notin \theta_\infty$, $\omega_k(c_\infty) = \omega_k(Y^w) \geq \omega_k(p_{\mathfrak{a}^-}(Y^w))$, car $p_{\mathfrak{a}^-}(Y^w)$ minore Y^w . Donc le lemme 4.4.3, appliqué à $Y = c_\infty$ et $Y' = p_{\mathfrak{a}^-}(Y^w)$ implique que $c_\infty \succ p_{\mathfrak{a}^-}(Y^w)$. Cela montre bien l'égalité souhaitée :

$$c_\infty = p_{\mathfrak{a}^-}(Y^w).$$

□

5.2 Flots semi-stables et extrémalité

Nous nous intéressons ici à un cas particulier du théorème 5.1.1, pour lequel on a toujours $c_\infty = 0$. Commençons par rappeler une terminologie introduite par Pengyu Yang.

Définition 5.2.1 (Variété de Bruhat instable). La variété de Bruhat standard X_w est définie comme l'adhérence de Zariski d'une cellule de Bruhat :

$$X_w = \overline{PwB}, \quad w \in W_P.$$

Une *variété de Bruhat* est une variété de la forme $X_w g$, pour $g \in G$ et $w \in W_P$. Une variété de Bruhat est dite *rationnelle* si elle peut s'écrire $X_w \gamma$, avec $\gamma \in G(\mathbb{Q})$. La variété $X_w g$ est *instable* pour le flot $a_t = e^{tY}$ s'il existe un poids dominant ω tel que $\omega(Y^w) < 0$.

Rappelons que l'on note en exposant l'action adjointe à droite de W sur \mathfrak{a} : $Y^w = (\text{Ad } w)^{-1}Y$. La notion d'instabilité ne dépend pas du choix du représentant de $w \in W_P = (W \cap P) \backslash W$, car si $p \in W \cap P$, alors $Y^p = Y$.

Remarque. Si PwB est instable, alors il existe un poids fondamental ω_i , $i \in [1, r]$ tel que $\omega_i(Y^w) < 0$. En effet, tout poids dominant est combinaison linéaire à coefficients entiers positifs de poids fondamentaux.

Le théorème 5.1.1 admet le corollaire important suivant.

Corollaire 5.2.2 (Points semi-stables dans G/Γ). Avec les notations du théorème 5.1.1, si $s \in G(\mathbb{Q})$ n'est inclus dans aucune variété de Bruhat rationnelle instable, alors $c_\infty = 0$. Par conséquent, dans toute représentation rationnelle V de G ,

$$\lim_{t \rightarrow \infty} \frac{1}{t} \log \lambda_1(a_t s V(\mathbb{Z})) = 0.$$

Démonstration. D'après le troisième point du théorème 5.1.1, on peut écrire $c_\infty = p_{\mathfrak{a}^-}(Y^w)$, où w est tel que $s \in PwB\gamma$. On raisonne alors par contraposée. Si $c_\infty \neq 0$, il existe donc un poids fondamental ω_i tel que $\omega_i(Y^w) < 0$, et la cellule de Bruhat $X_w \gamma$ est instable. La seconde assertion du corollaire découle de la première, car dans la représentation irréductible rationnelle V de G proximale de plus haut poids χ ,

$$\lambda_1(a_t s V(\mathbb{Z})) \asymp \chi(b_t).$$

□

Remarque. En fait, $c_\infty = 0$ si et seulement si s n'est inclus dans aucune variété de Schubert rationnelle instable. Dans ce cas, le second point du théorème est trivial, car $Q_\infty = G$.

Le corollaire ci-dessus permet déjà de démontrer un analogue du célèbre théorème de Roth [48] pour une variété de drapeaux générale. Soit $X = P \backslash G$ une variété de drapeaux, obtenue comme quotient d'un \mathbb{Q} -groupe semi-simple G par un sous-groupe parabolique P . On munit X de la distance de Carnot-Carathéodory usuelle, et d'une hauteur H_χ induite par une représentation irréductible de G de poids dominant χ , et on considère l'exposant diophantien β_χ sur X , défini au chapitre 2.

Définition 5.2.3. Un point x dans $X(\mathbb{R})$ est dit *extrémal* si $\beta_\chi(x) = \beta_\chi(X)$.

Le théorème 2.4.5 nous assure que, pour la mesure de Lebesgue, presque tous les points de $X(\mathbb{R})$ sont extrémaux. Nous donnons maintenant un critère suffisant pour

qu'un point $x \in X(\overline{\mathbb{Q}})$ soit extrémal. Dorénavant, le sous-groupe à un paramètre (a_t) est celui construit au chapitre 2, donné par la formule

$$a_t = e^{tY} \quad \text{où } Y \in \mathfrak{a} \text{ est défini par } \alpha(Y) = \begin{cases} 0 & \text{si } \alpha \in \theta \\ -1 & \text{si } \alpha \notin \theta. \end{cases} \quad (5.2)$$

Vues comme des parties de la variété de drapeaux X , les variétés de Bruhat seront plutôt appelées *variétés de Schubert*. Une variété de Schubert sera dite instable si la variété de Bruhat correspondante l'est pour le sous-groupe (a_t) ci-dessus.

Théorème 5.2.4 (Critère d'extrémalité pour les points algébriques). *Soit X une variété de drapeaux rationnelle, munie de la distance de Carnot-Carathéodory usuelle, et d'une hauteur H_χ induite par une représentation irréductible de G . Si $x \in X(\overline{\mathbb{Q}})$ n'est inclus dans aucune variété de Schubert rationnelle instable, alors x est extrémal.*

Démonstration. Soit $s_x \in G$ tel que $x = Ps_x$. Comme x n'appartient à aucune variété de Schubert instable, s_x n'appartient à aucune variété de Bruhat stable. Le corollaire 5.2.2 ci-dessus montre donc que dans la représentation V_χ de poids dominant χ ,

$$\lim_{t \rightarrow \infty} \frac{1}{t} \log \lambda_1(a_t s_x V_\chi(\mathbb{Z})) = 0.$$

D'après le lemme 2.4.6, cela implique que $\beta_\chi(x) = \beta_\chi(X)$. \square

5.3 L'exposant diophantien d'un point algébrique

Comme ci-dessus, $X = P \backslash G$ est une variété de drapeaux, obtenue comme quotient d'un \mathbb{Q} -groupe semi-simple G par un sous-groupe parabolique P . On munit X de la distance de Carnot-Carathéodory usuelle, et d'une hauteur H_χ induite par une représentation irréductible de G de poids dominant χ , et on considère l'exposant diophantien β_χ sur X , défini au chapitre 2. Ayant fixé dans V_χ un réseau rationnel $V_\chi(\mathbb{Z})$, nous noterons $\Gamma = \text{Stab}_G V_\chi(\mathbb{Z})$ le sous-groupe arithmétique de G associé. Le sous-groupe à un paramètre (a_t) est celui défini par la formule (5.2).

En règle générale, pour un point $x \in X(\overline{\mathbb{Q}})$ non nécessairement extrémal, le théorème 5.1.1 donne une méthode pour le calcul de l'exposant diophantien $\beta_\chi(x)$. C'est le contenu du théorème ci-dessous. Rappelons que l'action adjointe à droite du groupe de Weyl est notée en exposant : $Y^w = (\text{Ad } w)^{-1}Y$. Et de même pour l'action co-adjointe : $\chi^w = \chi \circ \text{Ad } w$.

Théorème 5.3.1 (Exposant d'un point algébrique). *Soit $x \in X$, soit $s_x \in G$ tel que $x = Ps_x$, et soit (a_t) le sous-groupe diagonal défini en (5.2). Soit $c_\infty, Q_\infty, \gamma_\infty$ les éléments donnés par le théorème 5.1.1 pour décrire l'orbite $(a_t s_x \Gamma)$ dans G/Γ , et*

$$s_x \gamma_\infty^{-1} = pwb, \quad p \in P, \quad w \in W_P, \quad b \in B,$$

une décomposition de Bruhat de $s_x \gamma_\infty^{-1}$.

Alors

$$\gamma_\chi(x) = -\langle \chi^w, p_{\mathfrak{a}^-}(Y^w) \rangle,$$

et par conséquent,

$$\beta_\chi(x) = \frac{1}{-\langle \chi, Y \rangle + \langle \chi^w, p_{\mathfrak{a}^-}(Y^w) \rangle}.$$

En particulier, l'exposant $\beta_\chi(x)$ est entièrement déterminé par la variété de Schubert $PwB\gamma_\infty \ni x$.

Remarque. Si la variété de Bruhat rationnelle $PwB\gamma_\infty$ est semi-stable, alors pour tout $i \in [1, r]$, $\omega_i(Y^w) \geq 0$, et donc $p_{\mathfrak{a}^-}(Y^w) = 0$. On retrouve bien $\gamma_\chi(x) = 0$ et $\beta_\chi(x) = \beta_\chi(X)$.

Remarque. Si $w = I$, alors $Y^w = Y \in \mathfrak{a}^-$. Dans ce cas, $\gamma_\chi(x) = -\langle \chi, Y \rangle$ est maximal, et l'exposant diophantien $\beta_\chi(x)$ vaut $+\infty$. Cela n'est pas surprenant, car alors $x = P\gamma_\infty$ est un point de $X(\mathbb{Q})$.

Démonstration. Écrivons $s_x\gamma_\infty^{-1} = pwb$. Pour tout $p \in P$, le comportement asymptotique de $s_x\Gamma$ est équivalent à celui de $p^{-1}s_x\Gamma$, et nous pouvons donc supposer sans perte de généralité que l'élément s_x est de la forme

$$s_x = wb\gamma_\infty.$$

D'après le théorème 5.1.1, pour t suffisamment grand, dans la décomposition de Siegel

$$a_t s_x \gamma_\infty^{-1} = kan\gamma,$$

l'élément γ appartient à Q_∞ . Par conséquent, dans la décomposition de Siegel

$$a_t^w b = (w^{-1}k)an\gamma,$$

on a $\gamma \in Q_\infty$, $an \in B \subset Q_\infty$, et donc $w^{-1}k \in K \cap Q_\infty$.

Soit

$$Q_\infty = L_\infty R_\infty,$$

la décomposition de Levi standard de Q_∞ , où R_∞ désigne le radical unipotent de Q_∞ et L_∞ le \mathbb{Q} -sous-groupe réductif engendré par l'ensemble de racines θ_∞ associé à Q_∞ . Suivant cette décomposition, écrivons

$$b = \ell u, \quad n = n_L n_U \quad \text{et} \quad \gamma = \gamma_L \gamma_U.$$

Comme $\gamma_L^{-1} n_U \gamma_L \gamma_U \in R_\infty$ et

$$a_t^w \ell u = w^{-1} k a n_L \gamma_L \gamma_L^{-1} n_U \gamma_L \gamma_U,$$

on doit avoir

$$a_t^w \ell = (w^{-1}k) a n_L \gamma_L,$$

ce qui donne une décomposition de Siegel de $a_t^w \ell$. Cela montre que les minima successifs de $a_t s_x V_\chi(\mathbb{Z})$ sont essentiellement égaux à ceux de $a_t^w \ell V_\chi(\mathbb{Z})$. De plus, les drapeaux partiels de $V_\chi(\mathbb{Z})$ (à $e^{\varepsilon t}$ près) pour $a_t^w \ell$ et $a_t^w b$ sont égaux. En effet, le drapeau partiel de $V_\chi(\mathbb{Z})$ qui réalise les minima (à $e^{\varepsilon t}$ près) de $a_t s_x \gamma_\infty^{-1} = a_t w b$ est stable par Q_∞ . Ce drapeau se décrit de la façon suivante :

$$D_0 = \{V_1 < V_1 \oplus V_2 < \dots\}$$

où

$$V_1 = \text{Vect}\{e_\beta; \beta(c_\infty) = \beta_1 \text{ minimal}\},$$

$$V_2 = \text{Vect}\{e_\beta; \beta(c_\infty) = \beta_2 > \beta_1 \text{ minimal}\}$$

et ainsi de suite. Chacun de ces espaces est stable par L_∞ , qui est engendré par les racines $\alpha \in \theta_\infty$, pour lesquelles $\alpha(c_\infty) = 0$. Et chaque $V_1 \oplus \dots \oplus V_k$ est stable par $Q_\infty = L_\infty R_\infty$. Et comme $\gamma_L \in Q_\infty$ et $\gamma \in Q_\infty$, on trouve bien que les filtrations pour $a_t^w \ell$ et $a_t^w b$, données par $\gamma_L^{-1} D_0 = \gamma^{-1} D_0 = D_0$ sont égales.

Nous sommes donc ramenés à comprendre la géométrie du réseau $a_t^w \ell V_\chi(\mathbb{Z})$, et plus particulièrement la quantité $r_\chi(w a_t^w \ell)$.

Comme $a_t^w \ell$ est dans le \mathbb{Q} -groupe réductif L_∞ , les minima successifs de $a_t^w \ell V_\chi(\mathbb{Z})$ sont compatibles avec la décomposition de V_χ en sous- L_∞ -modules irréductibles. Chacun de ces sous-modules est semi-stable pour le flot $(a_t^w \ell)$, et il nous suffit de comprendre le module V'_χ engendré par $w^{-1} e_\chi$. Si l'on note

$$\tau(V'_\chi, a_t^w) = \log \det(a_t^w |_{V'_\chi})$$

son taux de dilatation par le flot (a_t^w) , on obtient donc

$$\gamma_\chi(x) = -\frac{\tau(V'_\chi, a_t^w)}{\dim V'_\chi}.$$

Le taux de dilatation est donné par la somme (chaque poids est compté autant de fois qu'il apparaît dans V'_χ)

$$\tau(V'_\chi, a_t^w) = \sum_{\omega \prec V'_\chi} \omega(Y^w).$$

Nous identifions maintenant \mathfrak{a} et \mathfrak{a}^* grâce au produit scalaire usuel. Alors, la somme $\sum_{\omega \prec V'_\chi} \omega$ est un élément de $\mathfrak{a}_\infty = \bigcap_{\alpha \in \theta_\infty} \alpha^\perp$, et chaque élément $\omega \prec V'_\chi$ a la même projection sur \mathfrak{a}_∞ , qui est donc égale à $p_\infty(\chi^w)$, où $p_\infty : \mathfrak{a} \rightarrow \mathfrak{a}_\infty$ est la projection orthogonale. Cela donne déjà une expression pour $\gamma_\chi(x)$:

$$\gamma_\chi(x) = -\langle p_\infty(\chi^w), Y^w \rangle = -\langle \chi^w, p_\infty(Y^w) \rangle.$$

Mais d'après le théorème 5.1.1, $p_\infty(Y^w) = c_\infty = p_{\mathfrak{a}^-}(Y^w)$, et donc

$$\gamma_\chi(x) = -\langle \chi^w, p_{\mathfrak{a}^-}(Y^w) \rangle.$$

La formule pour $\beta_\chi(x)$ est alors une conséquence de la proposition 2.4.4. \square

Dans certains cas, le théorème 5.3.1 permet de montrer que l'exposant d'un point algébrique quelconque de X est minoré par l'exposant générique. Les deux corollaires suivants sont ainsi des résultats analogues au théorème de Dirichlet [17], pour le moment valables uniquement pour les points algébriques, hélas.

Corollaire 5.3.2 (Variétés de drapeaux de rang 1). *Supposons que la variété de drapeaux X s'écrive $X = P \backslash G$ avec P un \mathbb{Q} -sous-groupe parabolique strict maximal de G . Alors, pour tout $x \in X(\mathbb{Q})$,*

$$\beta_\chi(x) \geq \beta_\chi(X).$$

De plus, l'égalité a lieu si et seulement si x n'appartient à aucune sous-variété de Schubert rationnelle instable.

Démonstration. Il existe $i \in [1, r]$ tel que l'ensemble de racines simples associé au parabolique maximal P soit

$$\theta = [1, r] \setminus \{i\}.$$

Soit V_χ une représentation irréductible de G engendrée par un vecteur de plus haut poids e_χ tel que $\text{Stab}_G[e_\chi] = P$. On doit avoir

$$\chi = n\varpi_i, \quad n \geq 1.$$

Dans la suite, nous identifions encore \mathfrak{a} à \mathfrak{a}^* grâce au produit scalaire usuel. Avec cette identification,

$$Y = -\varpi_i.$$

Par conséquent,

$$\gamma_\chi(x) = -\langle \chi^w, p_{\mathfrak{a}^-}(Y^w) \rangle = n\langle Y^w, p_{\mathfrak{a}^-}(Y^w) \rangle = n\|p_{\mathfrak{a}^-}(Y^w)\|^2 \geq 0,$$

et avec la proposition 2.4.4 et la définition de $\beta_\chi(X)$ donnée au théorème 2.4.5,

$$\beta_\chi(x) \geq \beta_\chi(X).$$

De plus, l'égalité a lieu si et seulement si $p_{\mathfrak{a}^-}(Y^w) = 0$, i.e. $c_\infty = 0$. Cela équivaut à ce que x n'appartienne à aucune sous-variété de Schubert rationnelle instable. \square

Le même argument donne un résultat analogue si X est la variété drapeau complète d'un \mathbb{Q} -groupe déployé, munie de la hauteur anti-canonique.

Corollaire 5.3.3 (Variétés de drapeaux déployée). *Soit $X = P \backslash G$, avec G un \mathbb{Q} -groupe semi-simple \mathbb{Q} -déployé et P un sous-groupe parabolique minimal de G . On munit X de la hauteur anti-canonique H_χ associée à $\chi = \sum_{\alpha \in \Sigma^+} \alpha$, somme des racines positives. Pour tout $x \in X(\overline{\mathbb{Q}})$,*

$$\beta_\chi(x) \geq \beta_\chi(X),$$

avec égalité si et seulement si x n'appartient à aucune sous-variété de Schubert instable.

Démonstration. D'après [37, Proposition 2.69], la somme des racines positives est égale à la double somme des poids fondamentaux

$$\chi = \sum_{\Sigma^+} \alpha = 2 \sum_i \varpi_i = -2Y.$$

On peut donc reprendre l'argument de la démonstration précédente :

$$\gamma_\chi(x) = 2\|p_{\mathfrak{a}^-}(Y^w)\|^2 \geq 0.$$

Cela implique $\beta_\chi(x) \geq \beta_\chi(X)$, avec égalité si et seulement si $c_\infty = p_{\mathfrak{a}^-}(Y^w) = 0$, i.e. x n'appartient à aucune sous-variété de Schubert rationnelle instable. \square

Remarque. L'inégalité

$$\inf_{x \in X(\overline{\mathbb{Q}})} \beta_\chi(x) \geq \beta_\chi(X),$$

n'est pas valable en général. Nous verrons au paragraphe 9.4 un exemple de variété de drapeaux X munie de la distance de Carnot-Carathéodory et d'une hauteur H_χ telle qu'il existe un point algébrique $x \in X(\overline{\mathbb{Q}})$ tel que $\beta_\chi(x) < \beta_\chi(X)$.

Concluons cette partie par une question qui nous semble digne d'intérêt, quoique nous ne puissions pas y apporter de réponse. Dans le cas où X est une variété grassmannienne, c'est une formulation un peu plus précise d'une question de Schmidt [51, §16].

Question : L'égalité suivante est-elle toujours valable :

$$\inf_{x \in X(\mathbb{Q})} \beta_\chi(x) = \inf_{x \in X(\mathbb{R})} \beta_\chi(x) ?$$

Chapitre 6

Non divergence quantitative

Dans toute ce chapitre, G est un \mathbb{Q} -groupe semi-simple de rang r , et Γ un sous-groupe arithmétique. On fixe un tore \mathbb{Q} -déploé maximal T dans G , et un \mathbb{Q} -sous-groupe parabolique minimal B contenant T . On note $\{\alpha_1, \dots, \alpha_r\}$ la base du système de racines de (G, T) pour l'ordre associé à B , et $\{\varpi_1, \dots, \varpi_r\}$ les poids fondamentaux correspondants. Pour $i = 1, \dots, r$ on note V_i une représentation irréductible de G engendrée par une unique droite de plus haut poids $\omega_i = b_i \varpi_i$, avec $b_i \in \mathbb{N}^$ minimal. L'algèbre de Lie réelle de T est notée \mathfrak{a} , et la chambre de Weyl négative associée à B est notée \mathfrak{a}^- .*

Le but de ce chapitre est de développer un analogue, pour un \mathbb{Q} -groupe semi-simple G arbitraire, des résultats obtenus petit à petit par Margulis, Dani et Kleinbock [44, 14, 31, 34] pour le groupe SL_d .

La version précise qui nous intéresse est celle de Kleinbock [34, Theorem 0.2]. Cela dit, même pour SL_d , les énoncés que nous démontrons généralisent strictement ceux qui étaient déjà connus, en ce que la forme des voisinages de la pointe que l'on cherche à éviter est plus flexible. Alors que ce travail était en cours de rédaction, Lindenstrauss, Margulis, Mohammadi et Shah [42] ont aussi amélioré la non divergence pour SL_d , et leurs observations permettent de retrouver une partie des résultats exposés ici, notamment le théorème 6.2.1, dans ce cas particulier. Cela dit, notre approche est différente, et a le mérite de s'appliquer sans distinction à tout \mathbb{Q} -groupe semi-simple.

Les résultats de la théorie de la réduction pour les groupes arithmétiques, rappelés au chapitre 4, nous ont permis d'associer à chaque point x dans $\Omega = G/\Gamma$ un vecteur $c(x)$ dans \mathfrak{a}^- qui décrit la position de x dans Ω . Nous considérons maintenant une mesure de probabilité μ sur G satisfaisant certaines propriétés de régularité, et nous expliquerons comment contrôler les valeurs de $c(g)$, lorsque g est choisi aléatoirement suivant μ .

Ce contrôle de la fonction c hors d'un ensemble de petite mesure est ce qu'on appelle la non divergence quantitative.

6.1 Sous-ensembles de G/Γ

Pour énoncer la non divergence quantitative, nous devons en premier lieu généraliser la définition de la fonction $c : G \rightarrow \mathfrak{a}^-$. Rappelons que dans la représentation fondamentale V_i , on note $V_i(\mathbb{Z})$ un réseau rationnel stable par Γ , et

$$\tilde{X}_i = G \cdot e_i$$

l'orbite du vecteur de plus haut poids sous l'action de G . Étant donnée une partie compacte $S \subset G$ nous lui associons un élément $c(S) \in \mathfrak{a}^-$, de manière analogue à ce qui a été fait en 4.2. Pour chaque i , on pose

$$\mu_i(S) = \min_{v \in V_i(\mathbb{Z}) \cap \tilde{X}_i} \max_{g \in S} \|gv\|.$$

Puis on considère l'élément $c_0(S)$ de \mathfrak{a} défini par

$$\forall i \in [1, r], \quad \omega_i(c_0(S)) = \log \mu_i(S),$$

et enfin on pose

$$c(S) = p_{\mathfrak{a}^-}(c_0(S)).$$

Remarque. Si $S = \{g\}$ est réduit à un singleton, on retrouve la définition précédente : $c(S) = c(g)$.

Exercice 4. Soit $G = \mathrm{SL}_3$. Pour $\varepsilon > 0$, on considère

$$S_\varepsilon = \left\{ \begin{pmatrix} t & 1 & 0 \\ t^2 - \varepsilon & t & 0 \\ 0 & 0 & \varepsilon^{-1} \end{pmatrix} ; t \in [0, 1] \right\}.$$

Montrer que lorsque $\varepsilon > 0$ tend vers zéro, la distance de $c_0(S_\varepsilon)$ à \mathfrak{a}^- tend vers l'infini.

Nous utiliserons aussi la relation d'ordre sur \mathfrak{a} définie au paragraphe 4.4 par

$$Y_1 \prec Y_2 \iff \forall i, \omega_i(Y_1) \leq \omega_i(Y_2).$$

Proposition 6.1.1. *Soit $S \subset G$ une partie compacte.*

$$\forall g \in S, \quad c(g) \prec c(S).$$

Démonstration. Soit $g \in S$ quelconque. Naturellement, pour chaque i , $\mu_i(g) \leq \mu_i(S)$. Par conséquent, $c_0(g) \prec c_0(S)$. Comme $c(g)$ et $c(S)$ sont les plus grands minorants respectifs dans \mathfrak{a}^- de $c_0(g)$ et $c_0(S)$, la proposition est claire. \square

Remarque. On pourrait vouloir aussi définir un drapeau partiel associé à S . Cependant, un tel drapeau (s'il existe?) n'est pas uniquement défini. Par exemple, pour $G = \mathrm{SL}_4$, si $S = \{g_1, g_2\}$, avec $g_1 = \mathrm{diag}(\varepsilon^3, \varepsilon^{-1}, \varepsilon^{-1}, \varepsilon^{-1})$ et $g_2 = \mathrm{diag}(\varepsilon, \varepsilon, \varepsilon, \varepsilon^{-3})$, on trouve $c(S) = (\log \varepsilon, 2 \log \varepsilon, \log \varepsilon)$. Le point $i = 2$ est anguleux, au sens où $\alpha_2(c(S)) < 0$; et il existe pourtant deux 2-plans distincts, à savoir $v_1 = e_1 \wedge e_2$ et $v_2 = e_1 \wedge e_3$ pour lesquels $\log \sup_{g \in S} \|gv_i\| = \omega_2(c(S))$. Toutefois, si S est le support d'une mesure régulière, le théorème de non divergence nous permettra de définir un drapeau partiel associé à S .

Nous voulons maintenant montrer que si $S = \mathrm{Supp} \mu$ est le support d'une mesure suffisamment régulière sur G , alors l'ensemble des points g dans S tels que $c(g)$ est distant de $c(S)$ est de petite mesure. Mais pour cela, nous devons d'abord expliquer quelles conditions de régularité nous allons imposer sur μ .

6.2 Fonctions régulières et non divergence

Dans cette partie, μ désigne une mesure de Radon sur G , et $S = \text{Supp } \mu$. Soit U un ouvert de G . Une fonction $f : U \rightarrow \mathbb{R}$ borélienne est dite (C, α) -régulière pour μ si elle vérifie, pour toute boule $B = B(x, r) \cap U$ dans U et tout $\varepsilon > 0$,

$$\mu(\{g \in B \mid |f(g)| \leq \varepsilon \|f\|_{B, \mu}\}) \leq C\varepsilon^\alpha \mu(B),$$

où $\|f\|_{B, \mu} = \sup_{g \in B \cap \text{Supp } \mu} |f(g)|$. Ci-dessous, et dans toute la suite, lorsque $B = B(x, r)$ est une boule dans un espace métrique, et $\lambda \in \mathbb{R}_+^*$, on note $\lambda B = B(x, \lambda r)$. Par exemple, $5B = B(x, 5r)$. La mesure μ sera dite C -doublante si pour toute boule $B(x, r)$ dans G ,

$$\mu(2B) \leq C\mu(B).$$

Nous pouvons maintenant donner une version de la non divergence quantitative dans G/Γ .

Théorème 6.2.1 (Non divergence quantitative). *Soient G un \mathbb{Q} -groupe semi-simple, Γ un sous-groupe arithmétique, et $C_0, C_1, \alpha_0 > 0$. Il existe deux constantes positives $C, \alpha > 0$ telles qu'on ait la propriété suivante.*

Soit μ une mesure borélienne finie C_1 -doublante sur G et $B \subset G$ une boule satisfaisant :

$$\forall i \in [1, r], \forall v \in \tilde{X}_i \cap V_i(\mathbb{Z}), \quad g \mapsto \|gv\| \text{ est } (C_0, \alpha_0)\text{-régulière sur } 5B \text{ pour } \mu.$$

Alors, pour tout $\varepsilon > 0$,

$$\mu(\{g \in B \mid \|c(g) - c(S)\| \geq -\log \varepsilon\}) \leq C\varepsilon^\alpha \mu(B).$$

Remarque. Écrivons $g = k_g a_g n_g \gamma_g$, suivant une décomposition de Siegel, de sorte que $a_g = e^{c(g) + O(1)}$. Le théorème nous assure que pour un ensemble de grande mesure, l'élément a_g est déterminé par S , à une constante multiplicative près. Si $\theta_S = \{\alpha \in \Pi \mid \alpha(c(S)) < \log \varepsilon\}$, on peut ajouter que l'élément $P_{\theta_S} \gamma_g$ est constant sur un ensemble de mesure relative au moins $1 - C\varepsilon^\alpha$. Nous expliquerons cela ci-dessous, au paragraphe 6.5.

Le restant de cette partie est consacré à la démonstration de ce théorème. On pourrait peut-être donner une démonstration directe, dans l'esprit de celle de Margulis et ses co-auteurs pour SL_d , mais ce n'est pas tout à fait évident, car il faut comprendre les relations entre les petits vecteurs de $g\Gamma$ dans les différentes représentations fondamentales V_i . Nous proposons une autre approche, qui consiste à étudier d'abord séparément chaque condition de la forme $\mu_k(g) \leq \varepsilon \mu_k(S)$, pour k fixé, puis à réunir toutes ces conditions pour obtenir l'énoncé global donné ci-dessus. Ces deux étapes correspondent aux deux paragraphes suivants.

6.3 Non divergence pour une racine fixée

Ayant fixé k , nous voulons comprendre l'ensemble des points $g \in S$ qui satisfont $\mu_k(g) \leq \varepsilon \mu_k(S)$. Cet ensemble peut être de grande mesure et c'est ce qui fait que dans l'énoncé 6.2.1, on doit considérer simultanément toutes les représentations fondamentales, via la fonction c .

Exercice 5. Si $h : X \rightarrow G$ est une fonction, on note $c(h) = c(\{h(x); x \in X\})$. Soit $\varepsilon > 0$. Vérifier qu'avec l'application $h : [0, 1] \rightarrow \mathrm{SL}_3(\mathbb{R})$ définie par

$$h(x) = \begin{pmatrix} x & 1 & 0 \\ x^2 - \varepsilon^2 & x & 0 \\ 0 & 0 & \varepsilon^{-2} \end{pmatrix}$$

on a pour tout x , $\mu_1(x) \leq \varepsilon \mu_1(h)$.

L'observation cruciale, exprimée dans le théorème 6.3.1 ci-dessous, est en quelque sorte que si un point g satisfait $\mu_k(g) \leq \varepsilon \mu_k(S)$, i.e.

$$\omega_k(c(g)) \leq \omega_k(c(S)) + \log \varepsilon,$$

alors la probabilité d'avoir

$$\alpha_k(c(g)) \leq \log \varepsilon.$$

est très petite. Pour la démonstration, il nous est nécessaire de contrôler tous les $\mu_i(g)$ à une petite constante multiplicative $\varepsilon^{1/3}$ près, mais cela doit plutôt être vu comme un détail technique.

Théorème 6.3.1 (Non divergence dans une représentation fondamentale). *Soient C_0, C_1, α_0 des paramètres strictement positifs, et $k \in [1, r]$ fixé.*

Soit μ une mesure de Radon C_1 -doublante sur G , et B une boule dans G . On suppose que pour tout $v \in V_k(\mathbb{Z}) \cap \tilde{X}_k$,

$$g \mapsto \|gv\| \text{ est } (C_0, \alpha_0) \text{ - régulière sur } 5B \text{ pour } \mu.$$

Soient $\rho \in]0, 1[$ et $\varepsilon \in]0, 1[$. On note $S = B \cap \mathrm{Supp} \mu$ et on suppose que $\rho \leq \varepsilon \mu_k(S)$. Alors l'ensemble

$$\mathcal{A}_\varepsilon^{(k)}(\rho) = \left\{ x \in B \mid \begin{array}{l} \varepsilon^{\frac{1}{3}} \rho \leq \mu_k(x) \leq \rho, \\ \alpha_k(c(x)) \leq \log \varepsilon \end{array} \right\}$$

vérifie

$$\nu(\mathcal{A}_\varepsilon^{(k)}(\rho)) \leq C_2 \varepsilon^{\alpha_2} \nu(B),$$

où $\alpha_2 = \frac{\alpha_0}{2}$ et $C_2 = K_0 C_1^3 C_0$, avec K_0 une constante de Besicovitch pour $G \cap 5B$.

Remarque. Étant donné $M \geq 0$ l'ensemble

$$\mathcal{A}_{M,\varepsilon}^{(k)}(\rho) = \left\{ x \in B \mid \begin{array}{l} \varepsilon^M \rho \leq \mu_k(x) \leq \rho \\ \alpha_k(c(x)) \leq \log \varepsilon \end{array} \right\}$$

peut être recouvert par $3M$ ensembles du type $\mathcal{A}_\varepsilon^{(k)}(\rho')$, avec $\rho' \in [\varepsilon^M \rho, \rho]$, dont le théorème ci-dessus permet de majorer la mesure. On a donc aussi une borne

$$\mu(\mathcal{A}_{M,\varepsilon}^{(k)}(\rho)) \leq CM \varepsilon^\alpha \mu(B).$$

Démonstration du théorème 6.3.1. Soit $x \in \mathcal{A}_\varepsilon^{(k)}(\rho)$. Par définition, il existe un vecteur primitif $v_x \in \tilde{X}_k \cap V_k(\mathbb{Z})$ tel que

$$\|xv_x\| \leq \rho.$$

Soit B_x la boule de rayon maximal telle que

$$\forall y \in B_x \cap S, \quad \|yv_x\| \leq \varepsilon^{-1/2}\rho.$$

Notons que $B_x \subset 3B$, $2B_x \subset 5B$ et

$$\sup_{y \in 2B_x \cap S} \|yv_x\| \geq \varepsilon^{-1/2}\rho.$$

Soit $y \in B_x \cap S \cap \mathcal{A}_\varepsilon^{(k)}(\rho)$, et $v \in V_k(\mathbb{Z})$. Si v est linéairement indépendant de v_x , alors, d'après la proposition 4.3.2,

$$\|yv\| \gg e^{-\alpha_k(c(y))} \mu_k(y) \geq \varepsilon^{-1} \varepsilon^{1/3} \rho = \varepsilon^{-2/3} \rho > \|yv_x\|.$$

Par conséquent, v_x est l'unique vecteur de $V_k(\mathbb{Z})$ tel que $\mu_k(y) = \|yv_x\|$. Comme $y \in \mathcal{A}_\varepsilon^{(k)}(\rho)$, cela implique en particulier

$$\|yv_x\| \leq \rho.$$

Or, la fonction $f : y \mapsto \|yv_x\|$ est (C_0, α_0) -régulière sur $2B_x$ et vérifie $\|f\|_{2B_x, \mu} \geq \varepsilon^{-1/2}\rho$, on trouve donc

$$\mu(B_x \cap \mathcal{A}_\varepsilon^{(k)}(\rho)) = \mu(B_x \cap S \cap \mathcal{A}_\varepsilon^{(k)}(\rho)) \leq C_0 \varepsilon^{\alpha_0/2} \mu(2B_x) \leq C_0 C_1 \varepsilon^{\alpha_0/2} \mu(B_x).$$

Par la propriété de Besicovitch dans l'espace métrique $G \cap 5B$, il existe une sous-famille dénombrable $(B_{x_i})_{i \in \mathbb{N}}$ de multiplicité au plus K_0 telle que $\mathcal{A}_\varepsilon^{(k)}(\rho) \subset \bigcup_{i \in \mathbb{N}} B_{x_i} \subset 3B$, ce qui permet d'écrire

$$\mu(\mathcal{A}_\varepsilon^{(k)}(\rho)) \leq \sum_{i \in \mathbb{N}} \mu(B_{x_i} \cap \mathcal{A}_\varepsilon^{(k)}(\rho)) \leq C_0 C_1 \varepsilon^{\frac{\alpha_0}{2}} \sum_{i \in \mathbb{N}} \mu(B_{x_i}) \leq C_0 C_1^3 K_0 \varepsilon^{\frac{\alpha_0}{2}} \mu(B).$$

□

6.4 Non divergence globale

La fin de la démonstration du théorème 6.2.1 consiste à mettre ensemble les bornes obtenues pour chaque racine α_k , $k = 1, \dots, r$, après avoir observé que si $\|c(x) - c(S)\| \geq -\log \varepsilon$, alors il doit exister k tel que $\mu_k(x) < \varepsilon^\tau \mu_k(S)$ et $\alpha_k(c(x)) < \tau \log \varepsilon$. Nous mettons cette observation sous la forme d'un lemme élémentaire sur les systèmes de racines.

Lemme 6.4.1. *Soit Σ un système de racines dans un espace euclidien \mathfrak{a} de dimension r . Il existe $\tau > 0$ tel que la propriété suivante soit satisfaite.*

Pour $\varepsilon \in (0, 1)$ et $Y_1, Y_2 \in \mathfrak{a}^-$, si $Y_1 \prec Y_2$ et $\|Y_2 - Y_1\| \geq -\log \varepsilon$, alors il existe $k \in [1, r]$ tel que

1. $\omega_k(Y_1) \leq \omega_k(Y_2) + \tau \log \varepsilon$;
2. $\alpha_k(Y_1) \leq \tau \log \varepsilon$.

Démonstration. Posons

$$Y = Y_2 - Y_1 = \sum_i t_i \alpha_i.$$

Comme $Y_1 \prec Y_2$, on doit avoir $\forall i, t_i \geq 0$. Comme

$$\sum t_i \|\alpha_i\| \geq \|Y_2 - Y_1\| \geq -\log \varepsilon$$

il doit exister j tel que $t_j = \varpi_j(Y) \geq \frac{-\log \varepsilon}{C_1}$, où $C_1 = \sum_i \|\alpha_i\|$. Or, écrivant

$$Y = \sum_k \alpha_k(Y) \varpi_k,$$

on observe que

$$\varpi_j(Y) = \sum_k \langle \varpi_k, \varpi_j \rangle \alpha_k(Y) \leq \max_k \alpha_k(Y) \sum_k \langle \varpi_k, \varpi_j \rangle,$$

car pour tous j, k , $\langle \varpi_k, \varpi_j \rangle \geq 0$ et $\max_k \alpha_k(Y) \geq 0$. Avec $C_2 = \sum_k \langle \varpi_k, \varpi_j \rangle$, cela montre qu'il existe k tel que $\alpha_k(Y) \geq \frac{-\log \varepsilon}{C_1 C_2}$. Posant $c = (C_1 C_2)^{-1}$, on trouve

$$\alpha_k(Y_1) = \alpha_k(Y_2) - \alpha_k(Y) \leq \alpha_k(Y_2) + c \log \varepsilon \leq c \log \varepsilon.$$

De plus, comme $Y = \sum_i t_i \alpha_i$, cela implique

$$\sum_i t_i \langle \alpha_k, \alpha_i \rangle \geq -c \log \varepsilon$$

et comme $\langle \alpha_k, \alpha_i \rangle \leq 0$ pour $i \neq k$,

$$\|\alpha_k\|^2 \varpi_k(Y) = \|\alpha_k\|^2 t_k \geq -c \log \varepsilon.$$

Comme $\omega_k = b_k \varpi_k$ pour un certain $b_k \in \mathbb{N}^*$, cela montre ce qu'on voulait, avec $\tau = \frac{c}{\max_k \|\alpha_k\|^2}$:

$$\omega_k(Y_1) \leq \omega_k(Y_2) + \tau \log \varepsilon.$$

□

Avec ce lemme, nous pouvons maintenant déduire le théorème 6.2.1 du théorème 6.3.1.

Démonstration du théorème 6.2.1. Il suffit de montrer que sous les hypothèses du théorème,

$$\mu(\{x \in B \mid -2 \log \varepsilon \geq \|c(x) - c(S)\| \geq -\log \varepsilon\}) \leq C \varepsilon^\alpha \mu(B). \quad (6.1)$$

En effet, on aura alors, quitte à supposer $\varepsilon < \frac{1}{2}$,

$$\begin{aligned} \mu(\{x \in B \mid \|c(x) - c(S)\| \geq -\log \varepsilon\}) &\leq \sum_{m \geq 0} \mu(\{x \in B \mid -2 \log \varepsilon^{2^m} \geq \|c(x) - c(S)\| \geq -\log \varepsilon^{2^m}\}) \\ &\leq C \sum_{m \geq 0} \varepsilon^{2^m \alpha} \mu(B) \\ &\leq \frac{C}{1 - 2^{-\alpha}} \varepsilon^\alpha \mu(B). \end{aligned}$$

Pour voir (6.1), notons $\mathcal{A} = \{x \in B \mid -2 \log \varepsilon \geq \|c(x) - c(S)\| \geq -\log \varepsilon\}$. D'après le lemme 6.4.1, il existe $\tau > 0$ tel que \mathcal{A} est recouvert par les ensembles

$$\mathcal{A}^{(k)} = \left\{ x \in B \mid \begin{array}{l} -2 \log \varepsilon \geq \|c(x) - c(S)\| \geq -\log \varepsilon \\ \omega_k(c(x)) \leq \omega_k(c(S)) + \tau \log \varepsilon \\ \alpha_k(c(x)) \leq \tau \log \varepsilon \end{array} \right\}$$

Enfin, grâce au contrôle $-2 \log \varepsilon \geq \|c(x) - c(S)\|$ sur la norme de $c(x) - c(S)$, chaque $\mathcal{A}^{(k)}$ peut être recouvert par $M \asymp (\frac{6}{\tau})^r$ ensembles de la forme

$$\mathcal{A}_\varepsilon^{(k)}(\rho_1, \dots, \rho_r) = \left\{ x \in B \mid \begin{array}{l} \varepsilon^{\frac{\tau}{3}} \rho_i \leq \mu_i(x) \leq \rho_i, \quad \forall i \in [1, r] \\ \alpha_k(c(x)) \leq \tau \log \varepsilon \end{array} \right\}$$

Pour chacun de ces ensembles, le théorème 6.3.1 donne

$$\mu(\mathcal{A}_\varepsilon^{(k)}(\rho_1, \dots, \rho_r)) \leq C_2 \varepsilon^{\alpha_2 \frac{\tau}{3}} \mu(B),$$

et par suite,

$$\mu(\mathcal{A}) \leq \sum_k \sum_{\rho_1, \dots, \rho_r} \mu(\mathcal{A}_\varepsilon^{(k)}(\rho_1, \dots, \rho_r)) \leq C \varepsilon^\alpha \mu(B),$$

avec $\alpha = \frac{\tau \alpha_2}{3}$ et $C = r M C_2 \asymp r (\frac{6}{\tau})^r C_2$. \square

6.5 Drapeau partiel pour une mesure régulière

Comme conséquence du théorème 6.2.1 de non divergence, nous montrons maintenant que si S est le support d'une mesure régulière sur G , on peut définir un drapeau partiel associé à S .

Proposition 6.5.1. *Soient G un \mathbb{Q} -groupe semi-simple, Γ un sous-groupe arithmétique, et $C_0, \alpha_0 > 0$. Il existe deux constantes $C', \alpha' > 0$ telles qu'on ait la propriété suivante.*

Soit μ une mesure borélienne finie sur G et $B \subset G$ une boule satisfaisant :

$$\forall i \in [1, r], \forall v \in \tilde{X}_i \cap V_i(\mathbb{Z}), \quad g \mapsto \|gv\| \text{ est } (C_0, \alpha_0)\text{-régulière sur } 5B \text{ pour } \mu.$$

Soit $S = B \cap \text{Supp } \mu$, et

$$I_S(\varepsilon) = \{i \in [1, r] \mid \alpha_i(c(S)) \geq \log \varepsilon\}.$$

Pour $\varepsilon > 0$ suffisamment petit, pour chaque $i \notin I_S(\varepsilon)$, il existe une unique direction dans V_i contenant un vecteur $v_i \in V_i(\mathbb{Z}) \cap \tilde{X}_i$ tel que

$$\sup_{g \in S} \|gv_i\| = \min_{v \in V_i(\mathbb{Z}) \cap \tilde{X}_i} \sup_{g \in S} \|gv\|.$$

De plus, il existe un élément $\gamma_S \in G(\mathbb{Q})$ tel que

$$\forall i \notin I_S(\varepsilon), \quad v_i = \gamma_S e_i,$$

et si on note $g = k_g a_g n_g \gamma_g$ une décomposition de Siegel de $g \in S$,

$$\mu(\{g \in B \mid P_{I_S(\varepsilon)} \gamma_g = P_{I_S(\varepsilon)} \gamma_S\}) \geq 1 - C' \varepsilon^{\alpha'} \mu(B).$$

Remarque. L'élément $P_{I_S(\varepsilon)}\gamma_S \in P_{I_S(\varepsilon)}\backslash G$ est le drapeau partiel associé à l'ensemble S , pour le paramètre ε .

Démonstration. D'après le théorème 6.2.1,

$$\mu(\{g \in B \mid \|c(g) - c(S)\| \geq -\log \varepsilon\}) \leq C\varepsilon^\alpha \mu(B).$$

Soit $C_1 > 0$ une constante dépendant de G , et dont nous choisirons la valeur ci-dessous. Pour $\varepsilon > 0$ suffisamment petit, l'inégalité ci-dessus montre en particulier qu'il existe $g_1 \in S$ tel que

$$\|c(g_1) - c(S)\| \leq -\frac{\log \varepsilon}{C_1}.$$

Cela implique en particulier que pour toute racine simple α ,

$$|\alpha(c(g_1)) - \alpha(c(S))| \leq -\frac{\log \varepsilon}{2}.$$

Par conséquent, si $i \notin I_S(\varepsilon)$,

$$\alpha_i(c(g_1)) < \frac{\log \varepsilon}{2},$$

et avec la proposition 4.3.2, si $v \in V_i(\mathbb{Z})$ n'est pas colinéaire à la direction v_i qui réalise le premier minimum de $g_1 V_i(\mathbb{Z})$, on doit avoir

$$\|g_1 v\| \gg e^{-\alpha_i(c(g_1))} \mu_i(g_1) \geq \varepsilon^{-\frac{1}{2}} \mu_i(g_1) \geq \varepsilon^{-\frac{1}{2} + \frac{1}{C_1}} \mu_i(S).$$

Cela implique que pour chaque $i \notin I_S(\varepsilon)$, le vecteur $v_i \in V_i(\mathbb{Z}) \cap \tilde{X}_i$ engendre l'unique direction telle que

$$\sup_{g \in S} \|gv_i\| = \mu_i(S).$$

Comme cette direction est aussi uniquement déterminée par l'égalité $\|g_1 v_i\| = \mu_i(g_1)$ et qu'on a $\alpha_i(c(g_1)) < \frac{\log \varepsilon}{2}$, une décomposition de Siegel $g_1 = kan\gamma$ permet d'écrire, pour chaque $i \notin I_S(\varepsilon)$, avec $\gamma_S = \gamma$,

$$v_i = \gamma_S^{-1} e_i.$$

Enfin, si $g \in S$ vérifie $\|c(g) - c(S)\| \leq -\frac{\log \varepsilon}{C_1}$ le raisonnement fait ci-dessus pour g_1 s'applique aussi à g , et montre que si $i \notin I_S(\varepsilon)$, alors v_i est aussi l'unique vecteur de $V_i(\mathbb{Z})$ tel que $\|gv_i\| = \mu_i(g)$. En d'autres termes, pour chaque $i \notin I_S(\varepsilon)$, $\gamma_g^{-1} e_i = \gamma_S^{-1} e_i$, i.e.

$$P_{I_S(\varepsilon)}\gamma_g = P_{I_S(\varepsilon)}\gamma_S.$$

Cela démontre le dernier point de la proposition, car

$$\mu(\{g \in S \mid \|c(g) - c(S)\| \geq -\frac{\log \varepsilon}{C_1}\}) \leq C'\varepsilon^{\alpha'} \mu(S).$$

□

Chapitre 7

Flots diagonaux dans G/Γ

Dans ce chapitre, G est un \mathbb{Q} -groupe semi-simple de \mathbb{Q} -rang r , et Γ un sous-groupe arithmétique. On fixe un tore \mathbb{Q} -déployé maximal T dans G , et un \mathbb{Q} -sous-groupe parabolique minimal B contenant T . On note $\{\alpha_1, \dots, \alpha_r\}$ la base du système de racines de (G, T) pour l'ordre associé à B , et $\{\varpi_1, \dots, \varpi_r\}$ les poids fondamentaux correspondants. Pour $i = 1, \dots, r$, on note V_i la représentation irréductible de G engendrée par une unique droite rationnelle de plus haut poids $\omega_i = b_i \varpi_i$, avec $b_i \in \mathbb{N}^*$ minimal. On note $A = T^0(\mathbb{R})$ la composante neutre des points réels de T . L'algèbre de Lie de A est notée \mathfrak{a} , et la chambre de Weyl négative associée à B est notée \mathfrak{a}^- . On considère un sous-groupe à un paramètre (a_t) dans A , donné par $a_t = e^{tY}$, avec $Y \in \mathfrak{a}^-$.

Ce chapitre a pour but de décrire le comportement asymptotique d'une orbite diagonale dans l'espace de réseaux $\Omega = G/\Gamma$, lorsque le point de départ est choisi aléatoirement, suivant une mesure suffisamment régulière. On observe que ces résultats sont très similaires à ceux obtenus au chapitre 5 lorsque le point de départ était un réseau algébrique. On donne d'ailleurs une généralisation du théorème 5.1.1, pour une orbite partant d'un point choisi aléatoirement sur une variété algébrique définie sur $\overline{\mathbb{Q}}$.

Ces résultats généraux sur l'espace de réseaux Ω serviront de base à notre étude de l'approximation diophantienne dans $X = P \backslash G$, détaillée au chapitre suivant.

7.1 Mesures régulières

Commençons par une définition qui résume les propriétés de régularité que doit satisfaire une mesure pour que s'applique le théorème de non divergence.

Définition 7.1.1. Nous dirons qu'une mesure borélienne sur G est *localement régulière* en un point s_0 dans G s'il existe une boule ouverte $B = B(s_0, r)$ et des constantes $C, \alpha > 0$ telles que

$$\forall i \in [1, r], \forall v \in \tilde{X}_i \cap V_i(\mathbb{Z}), \forall g \in G, \quad s \mapsto \|gsv\| \text{ est } (C, \alpha)\text{-régulière sur } B \text{ pour } \mu.$$

Cette définition est stable par translation par un élément de G : si μ est localement régulière en s_0 , alors $g_*\mu$ est localement régulière en gs_0 . Grâce au théorème 6.2.1 de non divergence quantitative, nous allons voir que si (a_t) est un flot

diagonal fixé dans G , et μ une mesure localement régulière en s_0 , alors il existe une boule ouverte $B = B(s_0, r)$ telle que pour $s \in B$, les orbites $(a_t s \Gamma)_{t>0}$ ont presque toutes le même comportement asymptotique. Rappelons que pour une partie compacte $S \subset G$, on définit $c_0(S)$ par

$$\forall i \in [1, r], \quad \omega_i(c_0(S)) = \log \mu_i(S)$$

où $\mu_i(S) = \min_{v \in \tilde{X}_i \cap V_i(\mathbb{Z})} \max_{s \in S} \|sv\|$, et

$$c(S) = p_{a^-}(c_0(S)).$$

Avec le théorème 6.2.1 de non divergence, ce vecteur permet de contrôler la position dans Ω de $s\Gamma$, lorsque s est choisi aléatoirement dans S .

Théorème 7.1.2 (Orbites diagonales partant d'une mesure régulière). *Soit $(a_t)_{t>0}$ un sous-groupe à un paramètre dans A , et μ une mesure sur G localement régulière en un point $s_0 \in G$. Il existe une boule ouverte B centrée en s_0 telle que pour μ -presque tout $s \in B$, notant $S = B \cap \text{Supp } \mu$,*

$$\lim_{t \rightarrow \infty} \frac{1}{t} (c(a_t s) - c(a_t S)) = 0.$$

Démonstration. Soient $\delta > 0$ et $t > 0$. D'après le théorème 6.2.1 appliqué à la mesure $(a_t)_* \mu$, avec $\varepsilon = e^{-\delta t}$.

$$\mu(\{s \in B \mid \|c(a_t s) - c(a_t S)\| \geq \delta t\}) \leq C e^{-\alpha \delta t} \mu(B),$$

qui est le terme général d'une série convergente. Le lemme de Borel-Cantelli montre donc que pour tout $\delta > 0$, pour presque tout s dans B , pour tout $t \in \mathbb{N}$ suffisamment grand,

$$\|c(a_t s) - c(a_t S)\| < \delta t.$$

Or il existe une constante C telle que pour tous $t, t' \in \mathbb{R}$, $\|c(a_t s) - c(a_{t'} s)\| + \|c(a_t S) - c(a_{t'} S)\| \leq C|t - t'|$, et donc, pour tout $t > 0$ suffisamment grand,

$$\|c(a_t s) - c(a_t S)\| < \delta t + C.$$

Comme $\delta > 0$ est arbitrairement proche de 0, cela montre bien la limite souhaitée. \square

Remarque. On peut en outre contrôler le drapeau partiel associé à $a_t s$. Pour tout $\delta > 0$, soit

$$I_{a_t S}(e^{-\delta t}) = \{i \in [1, r] \mid \alpha(c(a_t S)) \geq -\delta t\}.$$

Suivant la proposition 6.5.1 on définit le drapeau partiel $P_{I_{a_t S}(e^{-\delta t})} \gamma_{a_t S}$ associé à $a_t S$. Notons aussi $a_t s = k_{t,s} a_{t,s} n_{t,s} \gamma_{t,s}$ une décomposition de Siegel de $a_t s$. Alors, pour presque tout $s \in S$, pour tout $t > 0$ suffisamment grand,

$$P_{I_{a_t S}(e^{-\delta t})} \gamma_{t,s} = P_{I_{a_t S}(e^{-\delta t})} \gamma_{a_t S}.$$

7.2 Adhérence de Zariski et hérédité

Soit S une partie de G . Dans chaque représentation fondamentale $\rho_i : G \rightarrow \mathrm{GL}(V_i)$ on considère dans $\mathrm{End} V_i$ le sous-espace vectoriel

$$\mathcal{H}_i(S) = \mathrm{Vect}\{\rho_i(s); s \in S\}$$

et on définit

$$\mathcal{H}(S) = \{g \in G \mid \forall i \in [1, r], \rho_i(g) \in \mathcal{H}_i(S)\}.$$

Proposition 7.2.1. *Il existe une boule B_0 dans G telle que pour toute partie compacte $S \subset G$, il existe une constante C telle que pour tout élément $a \in G$,*

$$\|c(aS) - c(a\mathcal{H}(S) \cap B_0)\| \leq C.$$

Démonstration. Pour $i \in [1, r]$, considérons la partie $\rho_i(S)$ dans l'espace vectoriel $\mathrm{End} V_i$. À une constante multiplicative près ne dépendant que de S , si $\varphi : \mathrm{End} V_i \rightarrow V_i$ est une application linéaire, alors

$$\sup_{u \in \rho_i(S)} \|\varphi(u)\| \asymp \sup_{u \in \mathcal{H}_i(S) \cap B(0,1)} \|\varphi(u)\|.$$

Cela s'applique en particulier aux applications de la forme $u \mapsto auv$, pour $a \in G$ et $v \in V_i$, et l'on obtient ainsi, pour une boule $B_0 \subset G$,

$$\sup_{g \in S} \|agv\| \asymp \sup_{g \in \mathcal{H}(S) \cap B_0} \|agv\|.$$

□

Étant donnée une mesure μ localement régulière en s_0 , on pose

$$\mathcal{H}_\mu(s_0) = \bigcap_{\varepsilon > 0} \mathcal{H}(B(s_0, \varepsilon) \cap \mathrm{Supp} \mu)$$

et

$$\mathcal{H}'_\mu(s_0) = B_0 \cap \bigcap_{\varepsilon > 0} \mathcal{H}(B(s_0, \varepsilon) \cap \mathrm{Supp} \mu),$$

où B_0 est la boule dans G donnée par la proposition ci-dessus. L'ensemble $\mathcal{H}_\mu(s_0)$ est un *ensemble algébrique* dans G : il s'obtient comme l'ensemble des zéros d'une famille de polynômes. En outre, lorsque le point s est choisi aléatoirement suivant μ au voisinage de s_0 , le comportement asymptotique de l'orbite $(a_t s \Gamma)$ est déterminé presque sûrement par $\mathcal{H}_\mu(s_0)$.

Corollaire 7.2.2. *Soit μ une mesure sur G localement régulière en s_0 . Pour μ -presque tout s au voisinage de s_0 ,*

$$\lim_{t \rightarrow \infty} \frac{1}{t} [c(a_t s) - c(a_t \mathcal{H}'_\mu(s_0))] = 0.$$

Démonstration. Cela découle immédiatement du théorème 7.1.2, et de la proposition 7.2.1. □

7.3 Encadrement du taux de fuite

Dans la suite, nous considérons un sous-groupe à un paramètre (a_t) dans A , donné par

$$a_t = e^{tY}, \quad \text{avec } Y \in \mathfrak{a}^-,$$

et nous notons P le sous-groupe parabolique associé à (a_t) :

$$P = \{g \in G \mid \lim_{t \rightarrow \infty} a_t g a_{-t} \text{ existe}\}.$$

Nous voulons étudier le comportement asymptotique de la fonction c le long des orbites de (a_t) dans Ω . Notre premier résultat concerne un point choisi aléatoirement suivant une mesure localement régulière μ qui satisfait une condition géométrique naturelle. Rappelons qu'une sous-variété de Bruhat dans G est une sous-variété de la forme

$$X_w g = \overline{PwB}g, \quad \text{avec } w \in W_P \text{ et } g \in G.$$

Étant donnée une famille $(A_i)_{i \in I}$ d'éléments de \mathfrak{a} , son plus grand minorant $A = \inf_{i \in I} A_i$ pour la relation d'ordre \prec est défini par

$$\forall k \in [1, r], \quad \omega_k(A) = \inf_{i \in I} \omega_k(A_i).$$

Pour le sous-groupe diagonal $(a_t) = (e^{tY})$, avec $Y \in \mathfrak{a}$, on définit aussi le taux de contraction $\tau_{\mathbb{R}}(M, a_t) \in \mathfrak{a}^-$ de M par (a_t) par la formule

$$\tau_{\mathbb{R}}(M, a_t) = \inf\{p_{\mathfrak{a}^-}(Y^w) ; w \in W_P \text{ tel que } \exists g \in G : M \subset X_w g\}.$$

Nous aurons aussi besoin de la quantité analogue

$$\tau_{\mathbb{Q}}(M, a_t) = \inf\{p_{\mathfrak{a}^-}(Y^w) ; w \in W_P \text{ tel que } \exists g \in G(\mathbb{Q}) : M \subset X_w g\}.$$

Remarquons que les ensembles ci-dessus ne sont jamais vides, car on a toujours $M \subset X_{w_0} g = G$ si w_0 est l'élément de longueur maximale dans le groupe de Weyl.

Exemple. Suivant Pengyu Yang, nous dirons qu'une variété de Bruhat $X_w g$ est *instable* pour le flot $a_t = e^{tY}$ s'il existe un poids fondamental ω tel que $\omega(Y^w) < 0$. Cela revient à dire que $\tau_{\mathbb{R}}(X_w, a_t) \neq 0$. En effet, s'il existe i tel que $\omega_i(Y^w) < 0$, alors $\omega_i(p_{\mathfrak{a}^-}(Y^w)) \leq \omega_i(Y^w) < 0$, donc $p_{\mathfrak{a}^-}(Y^w) \neq 0$; et réciproquement, si $\tau_{\mathbb{R}}(X_w, a_t) \neq 0$, alors il existe i tel que $\omega_i(Y^w) < 0$.

Rappelons qu'un ensemble algébrique dans G est dit *irréductible* s'il ne peut pas s'écrire comme réunion non triviale de deux sous-ensembles algébriques.

Théorème 7.3.1 (Encadrement du taux de fuite). *Soit μ une probabilité sur G régulière en s_0 , telle que $\mathcal{H}_{\mu}(s_0)$ est irréductible. Alors, pour presque tout s au voisinage de s_0 ,*

$$\tau_{\mathbb{R}}(\mathcal{H}'_{\mu}(s_0), a_t) \prec \liminf_{t \rightarrow \infty} \frac{1}{t} c(a_t s) \prec \limsup_{t \rightarrow \infty} \frac{1}{t} c(a_t s) \prec \tau_{\mathbb{Q}}(\mathcal{H}_{\mu}(s_0), a_t).$$

Remarque. En général, si $\mathcal{H}_{\mu}(s_0)$ n'est pas irréductible, on peut l'écrire comme une réunion finie de composantes irréductibles : $\mathcal{H}_{\mu}(s_0) = \cup_i F_i$. On a alors $\mu = \sum_i \mu_i$, où $\mu_i = \mu|_{F_i}$. Chacune des mesures μ_i est localement régulière en s_0 , et $\mathcal{H}_{\mu_i}(s_0) = F_i$ est irréductible. On peut donc se ramener facilement au cadre du théorème.

Nous verrons au chapitre suivant que la mesure de Lebesgue sur une sous-variété analytique est localement régulière. Admettant ce point pour l'instant, on retrouve comme cas particulier du théorème ci-dessus le résultat suivant, essentiellement dû à Pengyu Yang [61].

Corollaire 7.3.2 (Variétés analytiques stables). *Soit M une sous-variété analytique connexe de G qui n'est incluse dans aucune sous-variété de Bruhat instable pour (a_t) . Alors, pour presque tout $s \in M$, pour toute représentation rationnelle V ,*

$$\lim_{t \rightarrow \infty} \frac{1}{t} \log \lambda_1(a_t s V(\mathbb{Z})) = 0.$$

Démonstration. Si M n'est incluse dans aucune sous-variété de Bruhat instable pour (a_t) , alors $\tau_{\mathbb{R}}(M, a_t) = 0$. Le théorème 7.3.1 montre donc que presque sûrement $\lim_{t \rightarrow \infty} \frac{1}{t} c(a_t s) = 0$. Ensuite, si V est une représentation rationnelle, et χ le plus haut poids apparaissant dans V , le premier minimum de $a_t s V(\mathbb{Z})$ est donné par

$$\lambda_1(a_t s V(\mathbb{Z})) \asymp e^{\chi(c(a_t s))} = e^{o(t)}.$$

□

Pour la démonstration du théorème 7.3.1, nous aurons besoin de la proposition suivante, très voisine d'un résultat plus général de Pengyu Yang [61, Theorem 1.2]. Toutefois, la démonstration dans notre cas particulier est sensiblement plus simple, car on ne s'intéresse qu'aux vecteurs dans l'orbite d'un vecteur de plus haut poids; en particulier nous n'aurons pas besoin des résultats de théorie géométrique des invariants dus à Mumford [47] ou Kempf [27].

Proposition 7.3.3 (Stabilité linéaire). *Soit S un ensemble algébrique irréductible dans G , et $\tau = \tau_{\mathbb{R}}(S, a_t)$. Il existe $c > 0$ tel que pour tout $i \in [1, r]$ et tout vecteur $v \in \tilde{X}_i$,*

$$\forall t > 0, \quad \sup_{s \in S} \|a_t s v\| \geq c e^{t \omega_i(\tau)} \|v\|.$$

La démonstration de cette proposition est basée sur l'observation suivante.

Lemme 7.3.4. *Soit V une représentation de G engendrée par une unique droite rationnelle $\mathbb{Q}e_{\chi}$ de plus haut poids χ . Pour $\lambda \in \mathbb{R}$, notons*

$$G(e_{\chi}, V^{\lambda}(a_t)) = \{g \in G \mid \lim_{t \rightarrow \infty} \frac{1}{t} \log \|a_t g e_{\chi}\| \leq \lambda\}.$$

On peut écrire

$$G(e_{\chi}, V^{\lambda}(a_t)) = \bigsqcup_{w \in W^{\lambda}(\chi, a_t)} PwB$$

comme une réunion de cellules de Bruhat de G , où

$$W^{\lambda}(\chi, a_t) = \{w \in W_P \mid \langle \chi, Y^w \rangle \leq \lambda\}.$$

Démonstration. Soit g un élément quelconque de G , et $g = pwb$ sa décomposition de Bruhat, avec $p \in P$, $b \in B$ et $w \in W_P$. Le sous-groupe parabolique minimal B préserve la direction e_{χ} , et lorsque t tend vers l'infini, l'élément $a_t p a_t^{-1}$ converge dans G . Donc $a_t g e_{\chi}$ et $a_t w e_{\chi}$ ont le même comportement asymptotique. Comme

$$a_t w e_{\chi} = w w^{-1} a_t w e_{\chi} = w e^{t Y^w} e_{\chi} = e^{t \langle \chi, Y^w \rangle} w e_{\chi},$$

on trouve bien que $g = pwb$ est dans $G(e_{\chi}, V^{\lambda}(a_t))$ si et seulement si $w \in W^{\lambda}(\chi, a_t)$. □

La proposition 7.3.3 découle du lemme ci-dessus, par un argument élémentaire de compacité.

Démonstration de la proposition 7.3.3. Soit $i \in [1, r]$. Notons $\pi^+ : V_i \rightarrow V_i$ la projection sur la somme des espaces propres de a_t associés à des valeurs propres supérieures ou égales à $\omega_i(\tau)$. On a l'équivalence

$$\pi^+(sv) = 0 \quad \Leftrightarrow \quad \lim_{t \rightarrow \infty} \frac{1}{t} \log \|a_t sv\| < \omega_i(\tau).$$

Soit $v = g^{-1}e_i \in \tilde{X}_i$. Avec l'équivalence ci-dessus, le lemme 7.3.4 montre que si $\pi^+(sv) = 0$, alors s appartient à une cellule de Bruhat $PwBg$ avec $w \in W^\lambda(\omega_i, a_t)$, avec $\lambda < \omega_i(\tau)$, i.e. $\omega_i(Y^w) \leq \lambda < \omega_i(\tau)$. Mais par définition de $\tau = \tau_{\mathbb{R}}(S, a)$,

$$\omega_i(\tau) \leq \inf_{PwBg \supset S} \omega_i(Y^w),$$

donc S n'est inclus dans aucune cellule de Bruhat $PwBg$, avec $g \in G$ et $w \in W^\lambda(\omega_i, a_t)$. Par irréductibilité, S n'est pas inclus dans la réunion (finie) de ces cellules, et il existe donc $s \in S$ tel que $\pi^+(sv) \neq 0$. Comme $v \mapsto \sup_{s \in S} \|\pi^+(sv)\|$ est semi-continue inférieurement sur le compact $\tilde{X}'_i = \{v \in \tilde{X}_i \mid \|v\| = 1\}$, il existe $c > 0$ tel que

$$\forall v \in \tilde{X}_i, \quad \sup_{s \in S} \|\pi^+(sv)\| \geq c\|v\|.$$

Cela implique, pour tout $v \in \tilde{X}_i$,

$$\sup_{s \in S} \|a_t sv\| \geq \sup_{s \in S} e^{t\omega_i(\tau)} \|\pi^+(sv)\| \geq ce^{t\omega_i(\tau)} \|v\|.$$

□

Nous pouvons enfin démontrer le théorème 7.3.1.

Démonstration du théorème 7.3.1. Notons

$$\tau = \tau_{\mathbb{R}}(\mathcal{H}_\mu(s_0), a_t).$$

La proposition 7.3.3 montre que pour chaque $i \in [1, r]$, il existe $c > 0$ tel que

$$\forall t > 0, \forall v \in V_i(\mathbb{Z}) \cap \tilde{X}_i, \quad \sup_{s \in \mathcal{H}_\mu(s_0)} \|a_t sv\| \geq ce^{t\omega_i(\tau)} \|v\| \geq ce^{t\omega_i(\tau)}.$$

Cela implique naturellement les inégalités

$$\liminf_{t \rightarrow \infty} \frac{1}{t} \log \left(\min_{v \in V_i(\mathbb{Z}) \cap \tilde{X}_i} \sup_{s \in \mathcal{H}_\mu(s_0)} \|a_t sv\| \right) \geq \omega_i(\tau), \quad i = 1, \dots, r$$

ce qui se réécrit

$$\liminf_{t \rightarrow \infty} \frac{1}{t} c(a_t \mathcal{H}_\mu(s_0)) \succ \tau_{\mathbb{R}}(\mathcal{H}_\mu(s_0), a_t).$$

Soit B la boule centrée en s_0 donnée par le théorème 7.1.2, et $S = B \cap \text{Supp } \mu$. D'après la proposition 7.2.1, $c(a_t S) - c(a_t \mathcal{H}_\mu(s_0)) = O(1)$, et donc

$$\liminf_{t \rightarrow \infty} \frac{1}{t} c(a_t S) \succ \tau_{\mathbb{R}}(\mathcal{H}_\mu(s_0), a_t).$$

Le théorème 7.1.2 permet d'en déduire que pour presque tout s au voisinage de s_0 ,

$$\liminf_{t \rightarrow \infty} \frac{1}{t} c(a_t s) \succ \tau_{\mathbb{R}}(\mathcal{H}_{\mu}(s_0), a_t).$$

Montrons maintenant l'inégalité concernant la limite supérieure. Supposons $\mathcal{H}_{\mu}(s_0) \subset PwB\gamma$, avec $\gamma \in G(\mathbb{Q})$. Alors, pour tout $i \in [1, r]$ et tout $t > 0$,

$$\sup_{s \in S} \|a_t s \gamma^{-1} e_i\| \ll e^{t\omega_i(Y^w)}$$

et par conséquent

$$\limsup_{t \rightarrow \infty} \frac{1}{t} c(a_t s) \prec p_{\mathfrak{a}^-}(Y^w).$$

Comme ceci vaut pour tout w tel qu'il existe $\gamma \in G(\mathbb{Q})$ vérifiant $PwB\gamma \supset S$, on trouve bien

$$\limsup_{t \rightarrow \infty} \frac{1}{t} c(a_t s) \prec \tau_{\mathbb{Q}}(S, a).$$

□

7.4 Variétés algébriques définies sur $\overline{\mathbb{Q}}$

Dans le cas où l'ensemble algébrique $\mathcal{H}_{\mu}(s_0)$ est défini sur $\overline{\mathbb{Q}}$, on peut améliorer le théorème 7.3.1 et déterminer la limite $\lim_{t \rightarrow \infty} \frac{1}{t} c(a_t s)$, pour μ -presque tout s au voisinage de s_0 . C'est ce que décrit le théorème ci-dessous.

Théorème 7.4.1 (Orbites diagonales et sous-variétés algébriques). *Soit μ une mesure localement régulière en $s_0 \in G$ telle que $M = \mathcal{H}_{\mu}(s_0)$ soit irréductible et définie sur $\overline{\mathbb{Q}}$. Soit $(a_t)_{t>0}$ un sous-groupe diagonal à un paramètre dans G et $c_M = \tau_{\mathbb{Q}}(M, a)$. Pour $s \in M$ et $t > 0$, on note*

$$a_t s = k_{t,s} b_{t,s} n_{t,s} \gamma_{t,s},$$

une décomposition de Siegel de $a_t s$.

1. Pour presque tout s au voisinage de s_0 , $\lim_{t \rightarrow \infty} \frac{1}{t} \log b_{t,s} = c_M$.
2. Il existe $\gamma_M \in \Gamma$ tel que pour $\theta_M = \{i \in [1, r] \mid \alpha_i(c_M) = 0\}$ et $Q_M = P_{\theta_M}$ le sous-groupe parabolique associé à θ_M , alors pour presque tout s au voisinage de s_0 , pour tout $t > 0$ suffisamment grand, $Q_M \gamma_{t,s} = Q_M \gamma_M$.
3. Si $X_w \supset M \gamma_M^{-1}$ est la plus petite variété de Bruhat standard contenant $M \gamma_M^{-1}$, alors $c_M = p_{\mathfrak{a}^-}(Y^w)$.

Pour la démonstration, nous appliquerons le théorème 5.1.1 à un point $s_1 \in M \cap G(\overline{\mathbb{Q}})$ bien choisi, dont l'existence sera assurée par le lemme suivant. Nous dirons que des ensembles algébriques F_i , $i \in I$ sont de degré borné s'il existe une constante $D \geq 0$ telle pour pour chaque i , F_i est l'ensemble des zéros d'une famille de polynômes de degré au plus D .

Lemme 7.4.2. *Soit k un corps de nombres, et V une variété algébrique affine irréductible définie sur k . On suppose que $(F_i)_{i \in I}$ est une famille de sous-ensembles algébriques stricts définis sur k et de degré borné. Alors, il existe un point $s_1 \in V(\overline{\mathbb{Q}}) \setminus \bigcup_{i \in I} F_i$.*

Démonstration. Si $V = \mathbb{A}^d$ est l'espace affine tout entier, le résultat est clair : si le point $s_1 = (x_1, \dots, x_d)$ à coordonnées dans \mathbb{Q} est choisi de sorte que pour chaque i , $[k(x_1, \dots, x_{i+1}) : k(x_1, \dots, x_i)] > D$ alors s_1 ne satisfait aucune relation de degré au plus D à coefficients dans k .

D'après le lemme de normalisation de Noether [55, Theorem 10, page 66], il existe toujours un morphisme fini de variétés algébriques $V \rightarrow \mathbb{A}^{\dim V}$ défini sur k , et le cas général découle donc du cas particulier ci-dessus. \square

Démonstration du théorème 7.4.1. D'après le théorème 7.3.1, on sait déjà que pour presque tout $s \in M$,

$$\limsup_{t \rightarrow \infty} \frac{1}{t} \log b_{t,s} \prec c_M.$$

Comme les sous-variétés de Bruhat rationnelles sont définies sur \mathbb{Q} et de degré borné, le lemme ci-dessus montre qu'il existe un point $s_1 \in M \cap G(\overline{\mathbb{Q}})$ qui n'est inclus dans aucune sous-variété de Bruhat rationnelle qui ne contient pas M . D'après le théorème 5.1.1,

$$\lim_{t \rightarrow \infty} \frac{1}{t} \log b_{t,s_1} = c_M.$$

Cela implique nécessairement

$$\frac{1}{t} c(a_t M) \succ \frac{1}{t} c(a_t s_1) = c_M + o(1),$$

et avec le théorème 7.1.2, pour presque tout s au voisinage de s_0 ,

$$\liminf_{t \rightarrow \infty} \frac{1}{t} c(a_t s) = \liminf_{t \rightarrow \infty} \frac{1}{t} c(a_t M) \succ c_M.$$

Cela montre le premier point du théorème.

Ensuite, on applique la proposition 6.5.1 pour $t > 0$, avec $\varepsilon = e^{-\delta t}$, où $\delta > 0$ est choisi tel que

$$\forall i \notin \theta_M, \quad \delta < \alpha_i(c_M).$$

Cela montre qu'il existe un élément $\gamma_t \in G(\mathbb{Q})$ tel que dans une petite boule B centrée en s_0 ,

$$\mu(\{s \in B \mid Q_M \gamma_{s,t} \neq Q_M \gamma_t\}) \leq C' e^{-\delta \alpha' t} \mu(B).$$

Par le lemme de Borel-Cantelli, il s'ensuit que pour presque tout s au voisinage de s_0 , pour tout $t > 0$ suffisamment grand,

$$Q_M \gamma_{s,t} = Q_M \gamma_t.$$

Mais d'après la proposition 4.3.1, à s fixé, l'application $t \mapsto Q_M \gamma_{s,t}$ est localement constante, et donc constante au voisinage de l'infini. Ainsi, il existe un élément $\gamma_M \in G(\mathbb{Q})$ tel que pour tout $t > 0$ suffisamment grand,

$$Q_M \gamma_{s,t} = Q_M \gamma_M.$$

Enfin, si $s_1 \in G(\overline{\mathbb{Q}})$ est le point déjà utilisé ci-dessus et $X_w \supset M \gamma_M^{-1}$, alors $s_1 \in PwB$, et d'après le théorème 5.1.1,

$$c_M = \lim_{t \rightarrow \infty} \frac{1}{t} c(a_t s_1) = p_{\alpha^-}(Y^w).$$

\square

Corollaire 7.4.3 (Mesures algébriques semi-stables). *Soit μ une mesure localement régulière en $s_0 \in G$ telle que $M = \mathcal{H}_\mu(s_0)$ soit irréductible et définie sur $\overline{\mathbb{Q}}$. Si M n'est incluse dans aucune sous-variété de Bruhat rationnelle instable, alors pour toute représentation rationnelle V , pour presque tout s au voisinage de s_0 ,*

$$\lim_{t \rightarrow \infty} \frac{1}{t} \log \lambda_1(a_t s V(\mathbb{Z})) = 0.$$

Démonstration. Avec les notations du théorème 7.4.1, soit

$$X_w \supset M\gamma_M^{-1}$$

la plus petite sous-variété de Bruhat standard contenant $M\gamma_M^{-1}$. Comme M n'est incluse dans aucune sous-variété de Bruhat instable, on doit avoir, pour chaque $i \in [1, r]$, $\omega_i(Y^w) \geq 0$. Par suite, $p_{\mathfrak{a}^-}(Y^w) = 0$, et pour presque tout s au voisinage de s_0 ,

$$\lim_{t \rightarrow \infty} \frac{1}{t} \log c(a_t s) = 0.$$

Cela montre ce qu'on veut, car la décomposition de Siegel de $a_t s$ montre que dans une représentation rationnelle V de plus haut poids χ ,

$$\lambda_1(a_t s V(\mathbb{Z})) \asymp e^{t\chi(c(a_t s))} = e^{o(t)}.$$

□

Chapitre 8

Approximation dans les sous-variétés

Dans ce chapitre, nous nous donnons une sous-variété analytique M dans la variété de drapeaux X , et étudions les propriétés diophantiennes d'un point x choisi aléatoirement sur M . Plus précisément, nous cherchons d'abord à déterminer sous quelles conditions la conclusion du théorème 2.4.5 reste valable, et montrons un critère analogue à celui du théorème 5.2.4 obtenu pour les points algébriques. Ensuite, nous étudierons le cas où la variété M est algébrique et définie sur $\overline{\mathbb{Q}}$, où nous pouvons donner une formule pour l'exposant presque sûr d'un point choisi aléatoirement dans M .

Dans toute la suite, $X = P \backslash G$ désigne une variété de drapeaux obtenue comme quotient d'un \mathbb{Q} -groupe semi-simple G par un sous-groupe parabolique P défini sur \mathbb{Q} . On munit X de la métrique de Carnot-Carathéodory introduite au paragraphe 2.2, et d'une hauteur H_χ provenant d'une représentation irréductible de G engendrée par une unique droite de plus haut poids χ . Enfin, on suppose que G est de rang rationnel r , et on note V_i , $i = 1, \dots, r$ ses représentations fondamentales.

8.1 Variétés analytiques réelles

Si M est une sous-variété analytique de $\mathrm{SL}_d(\mathbb{R})$ de dimension m , on note λ_M la mesure de Lebesgue sur M , i.e. la mesure de Hausdorff de dimension m restreinte à M . Comme nous nous intéresserons seulement à des événements de mesure pleine ou nulle, seule la classe de λ_M aura une importance pour nous, et l'on aurait aussi bien pu définir λ_M localement comme l'image de la mesure de Lebesgue sur $\mathbb{R}^{\dim M}$ par un paramétrage analytique local de M .

La mesure λ_M est localement régulière. C'est ce résultat important, dû à Kleinbock et Margulis [31], qui fait l'intérêt principal du théorème 7.1.2. Nous rappelons donc ici les grandes lignes de sa démonstration. L'argument est basé sur la proposition suivante [33, Proposition 2.1].

Proposition 8.1.1. *Soit U un ouvert connexe de \mathbb{R}^n , et \mathcal{F} un sous-espace de dimension finie de fonctions analytiques sur U à valeurs réelles. Pour tout x dans*

U , il existe des constantes $C, \alpha > 0$ et un voisinage $W \ni x$ tels que toute fonction $f \in \mathcal{F}$ soit (C, α) -régulière.

Démonstration. Nous admettons cette proposition pour l'instant, en attendant d'inclure la démonstration donnée par Kleinbock et Margulis [31, Proposition 3.4]. \square

Corollaire 8.1.2. *Soit M une sous-variété analytique de X , λ_M une mesure de Lebesgue sur M , $x_0 \in M$ et $s : X \rightarrow G$ une section analytique locale au voisinage de x_0 . Il existe des constantes $C, \alpha > 0$ et une boule ouverte $B = B(x_0, r)$ telles que pour tout $g \in G$, pour tout $i \in [1, r]$ et tout $v \in V_i$, l'application*

$$x \mapsto \|gs(x)v\|$$

est (C, α) -régulière sur B pour la mesure λ_M .

Démonstration. Soit U un ouvert de \mathbb{R}^m et $\varphi : U \rightarrow M$ un paramétrage local de M au voisinage de x_0 tel que $\lambda_M = \varphi_*\lambda$ soit l'image par φ de la mesure de Lebesgue λ sur U . Supposons en outre que $\varphi(0) = x_0$. Soit \mathcal{F}_0 l'espace vectoriel engendré par les applications coefficients :

$$\mathcal{F}_0 = \text{Vect}\{u \mapsto \langle v, s(\varphi(u))w \rangle; v, w \in V_i, i \in [1, r]\},$$

et

$$\mathcal{F} = \text{Vect}\{f_1 f_2; f_1, f_2 \in \mathcal{F}_0\}.$$

Ces espaces de fonctions analytiques sur U sont de dimension finie, donc d'après la proposition 8.1.1, il existe un voisinage W de 0 dans \mathbb{R}^m et $C, \alpha > 0$ tels que toute fonction $f \in \mathcal{F}$ soit (C, α) -régulière sur W pour la mesure de Lebesgue. Les applications de la forme $u \mapsto \|gs(\varphi(u))v\|^2$ sont des éléments de \mathcal{F} , donc satisfont l'égalité souhaitée. \square

Une première application de ces propriétés de régularité des variétés analytiques et des résultats du chapitre précédent est que l'exposant diophantien est constant presque sûrement sur une sous-variété analytique.

Théorème 8.1.3 (Exposant diophantien d'une sous-variété analytique). *Soit M une sous-variété analytique connexe de X . Il existe une constante $\beta_\chi(M)$ telle que pour presque tout $x \in M$, $\beta_\chi(x) = \beta_\chi(M)$.*

Démonstration. Soit x_0 un point de M . Pour $x \in M$ et $t > 0$, notons

$$c_t^x = (\log \mu_1(a_t s_x^{-1} V_\chi(\mathbb{Z})), \dots, \log \mu_{\dim V_\chi}(a_t s_x^{-1} V_\chi(\mathbb{Z})))$$

la suite des logarithmes des covolumes successifs du réseau $a_t s_x^{-1} V_\chi(\mathbb{Z})$. Notons aussi \mathcal{C} l'ensemble des fonctions convexes sur le segment d'entiers $[0, \dim V_\chi]$ telles que $f(0) = f(\dim V_\chi) = 0$. Le théorème 6.2.1 appliqué dans le groupe $\text{GL}(V_\chi)$ dans un voisinage adéquat U de x_0 – dont l'existence est assurée par le corollaire 8.1.2 – montre qu'il existe une application

$$\begin{aligned} \mathbb{R}^+ &\rightarrow \mathcal{C} \\ t &\mapsto c_t^M \end{aligned}$$

telle que pour tout $\varepsilon > 0$ et tout $t \in \mathbb{R}^+$,

$$\lambda_M(\{x \in U \mid \|c_t^x - c_t^M\| \geq t\varepsilon\}) \leq e^{-t\alpha\varepsilon} \lambda_M(U).$$

En outre, d'après la remarque qui suit le théorème 6.2.1, si

$$I_t^M(\varepsilon) = \{i_1(M, \varepsilon, t), \dots, i_k(M, \varepsilon, t)\} \subset [1, \dim V_\chi]$$

désigne l'ensemble des points où la dérivée de $i \mapsto c_t^M(i)$ fait un saut de taille supérieure à $t\varepsilon$, il existe un drapeau partiel

$$\{0\} < V_{t,\varepsilon}^{i_1} < \dots < V_{t,\varepsilon}^{i_k} < V_\chi(\mathbb{Z})$$

tel qu'avec probabilité supérieure à $1 - Ce^{-t\alpha\varepsilon}$, pour chaque $\ell = 1, \dots, k$, les i_ℓ premiers minima successifs de $a_t s_x^{-1} V_\chi(\mathbb{Z})$ sont atteints dans $V_{t,\varepsilon}^{i_\ell}$.

Notons E_χ la somme des espaces de poids de a_t différents de e_χ . Pour chaque $i \in I_t^M(\varepsilon)$, il existe $f_i = f_i(t, \varepsilon) \geq 0$ tel que

$$\lambda_M(\{x \in U \mid e^{-t(f_i+\varepsilon)} \leq d(a_t s_x^{-1} V_{t,\varepsilon}^i, E_\chi) \leq e^{-t(f_i-\varepsilon)}\}) \geq (1 - Ce^{\alpha\varepsilon t}) \lambda_M(U).$$

En effet, si \mathbf{v} est un représentant de $V_{t,\varepsilon}^i$ dans $\wedge^i V_\chi$ et $(\mathbf{u}_j)_{j \in J}$ une base orthonormée de $\wedge^{i-1} E_\chi$, la distance $d(a_t s_x^{-1} V_{t,\varepsilon}^i, E_\chi)$ est comparable au maximum $\max_{j \in J} \frac{\|\mathbf{u}_j \wedge a_t s_x^{-1} \mathbf{v}\|}{\|a_t s_x^{-1} \mathbf{v}\|}$. Or, par régularité des fonctions $x \mapsto \|\mathbf{u}_j \wedge a_t s_x^{-1} \mathbf{v}\|$ et $x \mapsto \|a_t s_x^{-1} \mathbf{v}\|$, avec probabilité $1 - e^{\alpha\varepsilon t}$,

$$\|\mathbf{u}_j \wedge a_t s_x^{-1} \mathbf{v}\| \geq e^{-\varepsilon t} \sup_{y \in U} \|\mathbf{u}_j \wedge a_t s_y^{-1} \mathbf{v}\|$$

et

$$\|a_t s_x^{-1} \mathbf{v}\| \geq e^{-\varepsilon t} \sup_{y \in U} \|a_t s_y^{-1} \mathbf{v}\|.$$

Par conséquent, si f_i est choisi tel que $e^{-f_i t} = \max_j \frac{\sup_{y \in U} \|\mathbf{u}_j \wedge a_t s_y^{-1} \mathbf{v}\|}{\sup_{y \in U} \|a_t s_y^{-1} \mathbf{v}\|}$, on a, avec probabilité supérieure à $1 - Ce^{\alpha\varepsilon t}$,

$$d(a_t s_x^{-1} V_{t,\varepsilon}^i, E_\chi) \leq \max_j \frac{\sup_{y \in U} \|\mathbf{u}_j \wedge a_t s_y^{-1} \mathbf{v}\|}{\|a_t s_x^{-1} \mathbf{v}\|} \leq e^{-t(f_i-\varepsilon)}$$

et

$$d(a_t s_x^{-1} V_{t,\varepsilon}^i, E_\chi) \geq \max_j \frac{\|\mathbf{u}_j \wedge a_t s_x^{-1} \mathbf{v}\|}{\sup_y \|a_t s_y^{-1} \mathbf{v}\|} \geq e^{-t(f_i+\varepsilon)}.$$

Avec le lemme de Borel-Cantelli, ces inégalités montrent que pour presque tout x au voisinage de x_0 , pour tout $t > 0$ suffisamment grand,

$$\begin{cases} \|c_t^x - c_t^M\| \leq t\varepsilon \\ \forall \ell = 1, \dots, k, \quad c_t^x(i_\ell) = \log \|a_t s_x^{-1} V_{t,\varepsilon}^{i_\ell}\| \\ d(a_t s_x^{-1} V_{t,\varepsilon}^{i_\ell}, E_\chi) \in [e^{-t(f_i+\varepsilon)}, e^{-t(f_i-\varepsilon)}] \end{cases}$$

Notons que $f_{i_1} \geq f_{i_2} \geq \dots \geq f_{i_k}$. Soit $j_{t,\varepsilon} \in I_t^M(\varepsilon)$ le plus petit indice tel que $f_{j_{t,\varepsilon}} \leq 2\varepsilon$. Montrons que pour presque tout x au voisinage de x_0 ,

$$\gamma_\chi(x) = \limsup_{t \rightarrow \infty} \frac{-1}{t} (c_t^M(j_{t,\varepsilon}) - c_t^M(j_{t,\varepsilon} - 1)) + O(\varepsilon).$$

Tout d'abord, l'inégalité $f_{j_{t,\varepsilon}} \leq 2\varepsilon$ implique $d(a_t s_x^{-1} V_{t,\varepsilon}^{j_{t,\varepsilon}}, E_X) \geq e^{-3t\varepsilon}$, et comme $a_t s_x^{-1} V_{t,\varepsilon}^{j_{t,\varepsilon}}(\mathbb{Z})$ admet une bonne¹ base constituée de vecteurs de norme au plus $e^{c_t^M(j_{t,\varepsilon}) - c_t^M(j_{t,\varepsilon}-1) + tO(\varepsilon)}$, il existe un tel vecteur $v \in a_t s_x^{-1} V_{t,\varepsilon}^{j_{t,\varepsilon}}(\mathbb{Z})$ tel que $\|\pi^+(v)\| \geq e^{-tO(\varepsilon)}\|v\|$. Cela implique

$$r_X(a_t(1-O(\varepsilon))s_x^{-1}V_X(\mathbb{Z})) \leq e^{c_t^M(j_{t,\varepsilon}) - c_t^M(j_{t,\varepsilon}-1) + O(\varepsilon)t},$$

puis

$$\gamma_X(x) \geq \limsup_{t \rightarrow \infty} \frac{-1}{t} (c_t^M(j_{t,\varepsilon}) - c_t^M(j_{t,\varepsilon} - 1)) - O(\varepsilon).$$

Réciproquement, soit $V_{t,\varepsilon}^{j'_{t,\varepsilon}}$ le sous-espace qui précède $V_{t,\varepsilon}^{j_{t,\varepsilon}}$ dans le drapeau $V_{t,\varepsilon}^{i_1} < \dots < V_{t,\varepsilon}^{i_k}$. Comme pour presque tout x , pour tout t assez grand

$$d(a_t s_x^{-1} V_{t,\varepsilon}^{j'_{t,\varepsilon}}, E_X) \leq e^{-(f_{j-1} - \varepsilon)t} \leq e^{-\varepsilon t}$$

aucun vecteur $v \in a_t s_x^{-1} V_{t,\varepsilon}^{j'_{t,\varepsilon}}$ ne saurait satisfaire $\|\pi^+(v)\| \geq \frac{\|v\|}{2}$. Or tout vecteur $v \in a_t s_x^{-1} V_X(\mathbb{Z})$ hors de $a_t s_x^{-1} V_{t,\varepsilon}^{j'_{t,\varepsilon}}$ vérifie

$$\|v\| \gg e^{c_t^M(j'_{t,\varepsilon}+1) - c_t^M(j'_{t,\varepsilon})} \geq e^{c_t^M(j_{t,\varepsilon}) - c_t^M(j_{t,\varepsilon}-1) + (j_{t,\varepsilon} - j'_{t,\varepsilon})t\varepsilon},$$

où la deuxième inégalité provient de ce que les sauts de la dérivée de $i \mapsto c_t^M(i)$ sont majorés par $t\varepsilon$ sur tout l'intervalle $]j'_{t,\varepsilon}, j_{t,\varepsilon}[$. Par suite

$$r_X(a_t s_x^{-1} V_X(\mathbb{Z})) \geq e^{c_t^M(j_{t,\varepsilon}) - c_t^M(j_{t,\varepsilon}-1) + tO(\varepsilon)}$$

puis

$$\gamma_X(x) \leq \limsup_{t \rightarrow \infty} \frac{-1}{t} (c_t^M(j_{t,\varepsilon}) - c_t^M(j_{t,\varepsilon} - 1)) + O(\varepsilon).$$

Ainsi, il existe un voisinage U de x_0 tel que pour tout $\varepsilon > 0$, il existe γ_ε tel que pour presque tout x dans U , $\gamma_X(x) \in [\gamma_\varepsilon - \varepsilon, \gamma_\varepsilon + \varepsilon]$. En faisant tendre ε vers 0, cela montre que $\gamma_X(x)$ est constant presque partout au voisinage de tout point $x_0 \in M$, et comme M est connexe, $\gamma_X(x)$ est constant presque sûrement sur M . Avec la proposition 2.4.4, on en déduit que $\beta_X(x)$ est constant presque sûrement sur M . \square

8.2 Un critère d'extrémalité

La distance de Carnot-Carathéodory et la hauteur sur X nous ont permis de définir au paragraphe 2.4 l'exposant diophantien $\beta_X(x)$ d'un point $x \in X(\mathbb{R})$. Nous avons vu en outre qu'il existe une constante $\beta_X(X)$ telle que pour presque tout $x \in X(\mathbb{R})$, $\beta_X(x) = \beta_X(X)$. Pour suivre la terminologie existant dans le cadre de l'espace projectif, nous posons la définition suivante.

Définition 8.2.1. Une mesure borélienne μ sur X est dite *extrémale* si pour presque tout x dans X , $\beta_X(x) = \beta_X(X)$. Dans le cas où μ est une mesure de Lebesgue sur une sous-variété analytique M , nous dirons aussi que M est extrémale.

¹Comme cette base réalise les minima, elle est presque orthogonale.

Nous voulons énoncer une condition suffisante pour qu'une sous-variété analytique $M \subset X$ soit extrémale. Pour cela, rappelons que si $\theta \subset \Pi$ est l'ensemble de racines simples associé sous-groupe parabolique P , on définit alors un sous-groupe à un paramètre dans G en posant

$$a_t = e^{tY} \quad \text{où } Y \in \mathfrak{a} \text{ est défini par } \alpha(Y) = \begin{cases} 0 & \text{si } \alpha \in \theta \\ -1 & \text{si } \alpha \notin \theta. \end{cases} \quad (8.1)$$

Rappelons qu'une sous-variété de Schubert dans X est une sous-variété de la forme

$$X_w g = \overline{PwB}g, \quad \text{avec } w \in W_P \text{ et } g \in G,$$

et qu'une variété de Schubert $X_w g$ est dite instable pour le flot $a_t = e^{tY}$ s'il existe un poids dominant ω tel que $\omega(Y^w) < 0$. Les résultats de la partie précédente permettent de montrer le théorème suivant.

Théorème 8.2.2 (Critère d'extrémalité pour les variétés analytiques). *Soit M une sous-variété analytique connexe de X . Si M n'est incluse dans aucune sous-variété de Schubert instable, alors M est extrémale.*

Démonstration. Soit $x_0 \in M$ et $s : X \rightarrow G$ une section analytique locale au voisinage de x_0 . Notons λ_M la mesure de Lebesgue sur M et $\mu = s_* \lambda_M$ la mesure image de λ_M par la section s . D'après le corollaire 8.1.2, la mesure μ est localement régulière au voisinage de $s_0 = s(x_0)$. Comme M n'est incluse dans aucune sous-variété de Schubert instable, la variété $\mathcal{H}_\mu(s_0)$ n'est incluse dans aucune sous-variété de Bruhat instable. Le corollaire 7.3.2 s'applique donc : pour λ_M -presque tout x au voisinage de x_0 ,

$$\lim_{t \rightarrow \infty} \frac{1}{t} \lambda_1(a_t s(x) V_X(\mathbb{Z})) = 0.$$

Le lemme 2.4.6 permet d'en conclure que $\beta_\chi(x) = \beta_\chi(X)$. Comme cela vaut pour λ_M -presque tout x au voisinage d'un point $x_0 \in M$ arbitraire, la variété M est extrémale. \square

Remarque. Une sous-variété $M \subset P \backslash G$ est dite *dégénérée* si M est contenue dans une variété de Schubert stricte. Naturellement, toute sous-variété incluse dans une variété de Schubert instable est dégénérée. Le théorème ci-dessus implique donc que toute sous-variété analytique $M \subset X$ non dégénérée est extrémale. Cependant, il peut exister des sous-variétés dégénérées extrémales ; nous en verrons quelques exemples au chapitre 9.

Avec une condition supplémentaire sur les coefficients qui définissent la sous-variété analytique M , on peut même améliorer ce critère.

Théorème 8.2.3 (Critère d'extrémalité pour les variétés algébriques). *Soit M une sous-variété analytique connexe de X dont l'adhérence de Zariski est définie sur $\overline{\mathbb{Q}}$. Si M n'est incluse dans aucune sous-variété de Schubert rationnelle instable, alors M est extrémale.*

Démonstration. La démonstration est identique à celle du théorème 8.2.2, en appliquant le corollaire 7.4.3 au lieu du corollaire 7.3.2. \square

Remarque. Ce critère n'est pas toujours optimal. Pour certains choix de X , il existe des sous-variétés M de dimension strictement positive telles que pour presque tout x dans M , $\beta_\chi(x) = \beta_\chi(X)$. Nous verrons toutefois plus loin quelques exemples où le critère est optimal : si M est incluse dans une sous-variété de Schubert rationnelle instable, alors M n'est pas extrémale. C'est le cas par exemple lorsque $X = \mathbb{P}^n$ est un espace projectif, ou lorsque $X = \text{Grass}(\ell, d)$ est une variété grassmannienne.

Plus généralement, lorsque l'adhérence de Zariski de M est définie sur $\overline{\mathbb{Q}}$, on peut donner une formule pour l'exposant diophantien presque sûr d'un point de M . C'est ce que nous détaillons au paragraphe suivant.

8.3 Sous-variétés algébriques définies sur $\overline{\mathbb{Q}}$

Ce paragraphe a pour but le théorème suivant, analogue du théorème 5.3.1, qui permet de calculer l'exposant diophantien $\beta_\chi(x)$ pour un point x arbitraire dans $X(\overline{\mathbb{Q}})$. Dans toute la suite, le groupe à un paramètre (a_t) est celui défini ci-dessus en (8.1).

Théorème 8.3.1 (Exposant diophantien d'une variété définie sur $\overline{\mathbb{Q}}$). *Soit M une sous-variété analytique connexe de X dont l'adhérence de Zariski est définie sur $\overline{\mathbb{Q}}$. Pour chaque $x \in X$, on note $s_x \in G$ un élément tel que $x = Ps_x$. Soit c_M, Q_M, γ_M les éléments donnés par le théorème 7.4.1 pour décrire l'orbite $(a_t s_x \Gamma)$ dans Ω lorsque x est choisi aléatoirement sur M , et*

$$X_w \supset M\gamma_M^{-1}, \quad w \in W_P,$$

la plus petite variété de Schubert standard contenant $M\gamma_M^{-1}$.

Alors pour presque tout $x \in M$,

$$\gamma_\chi(x) = -\langle \chi^w, p_{\mathfrak{a}^-}(Y^w) \rangle,$$

et par conséquent,

$$\beta_\chi(x) = \frac{1}{-\langle \chi, Y \rangle + \langle \chi^w, p_{\mathfrak{a}^-}(Y^w) \rangle}.$$

Démonstration. La démonstration est presque identique à celle du théorème 5.3.1, avec les changements qui s'imposent : il faut appliquer le théorème 7.4.1 au lieu du théorème 5.1.1, et remplacer les éléments $c_\infty, \gamma_\infty, P_\infty$ par $c_M, \gamma_M, P_M, \dots$ etc. Les détails sont laissés au lecteur. \square

Nous concluons ce chapitre en résumant quelques propriétés importantes de l'exposant diophantien d'un point x choisi aléatoirement sur une variété algébrique définie sur $\overline{\mathbb{Q}}$.

Corollaire 8.3.2. *Soit X une variété de drapeaux, munie de la distance de Carnot-Carathéodory usuelle et d'une hauteur H_χ associée au poids dominant χ . Soit $M \subset X$ une sous-variété analytique connexe dont l'adhérence de Zariski est définie sur $\overline{\mathbb{Q}}$.*

1. *L'exposant $\beta_\chi(M)$ est déterminé par l'intersection des sous-variétés de Schubert rationnelles contenant M . Et même, il existe une sous-variété de Schubert $X_w \gamma \supset M$ avec $\gamma \in G(\overline{\mathbb{Q}})$ telle que $\beta_\chi(M) = \beta_\chi(X_w \gamma)$.*

2. Pour tout $x \in M \cap X(\overline{\mathbb{Q}})$ hors de toute sous-variété de Schubert rationnelle $X'_w \gamma' \not\supset M$, $\beta_\chi(x) = \beta_\chi(M)$.

Chapitre 9

Quelques exemples

Pour illustrer les théorèmes généraux démontrés dans ce mémoire, nous en décrivons maintenant quelques cas particuliers. C'est souvent après l'étude approfondie de ces exemples importants qu'ont pu être démontrés les résultats plus abstraits sur les variétés de drapeaux générales.

9.1 Espace projectif

L'espace projectif \mathbb{P}^{d-1} constitue le cadre de l'approximation diophantienne classique. Dans ce cadre, tous les résultats présentés dans ce mémoire étaient déjà connus. Nous les rappelons toutefois brièvement, puisque notre objectif était justement de comprendre ces théorèmes de façon plus générale, à partir des groupes arithmétiques.

Si $x, y \in \mathbb{P}^{d-1}$ sont engendrés respectivement par les vecteurs $u, v \in \mathbb{R}^d$ leur distance est donnée par la formule

$$d(x, y) = \frac{\|u \wedge v\|}{\|u\|\|v\|}.$$

La hauteur sur $\mathbb{P}^{d-1}(\mathbb{Q})$ est la hauteur usuelle : si $v \in \mathbb{P}^{d-1}(\mathbb{Q})$ s'écrit en coordonnées homogènes $v = [v_1 : \dots : v_d]$, où les v_i sont des entiers premiers entre eux dans leur ensemble, alors

$$H(v) = \max_{1 \leq i \leq d} |v_i|.$$

Nous commençons par le célèbre théorème de Dirichlet [17], bien que ce résultat ne semble pas se généraliser aisément dans une variété drapeau arbitraire.

Théorème 9.1.1 (Théorème de Dirichlet). *Pour tout $x \in \mathbb{P}^{d-1}(\mathbb{R})$,*

$$\beta(x) \geq 1 + \frac{1}{d-1}.$$

Une simple application du lemme de Borel-Cantelli permet de montrer que presque tout x dans $\mathbb{P}^{d-1}(\mathbb{R})$ vérifie l'égalité $\beta(x) = 1 + \frac{1}{d-1}$. Le théorème de

Khintchine [29] donne un critère simple sur une fonction $\psi : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ décroissante pour que l'inégalité

$$d(x, v) \leq H(v)^{-1 - \frac{1}{d-1}} \psi(H(v)) \quad (9.1)$$

ait une infinité de solutions lorsque x est choisi suivant la mesure de Lebesgue sur \mathbb{P}^{d-1} .

Théorème 9.1.2 (Théorème de Khintchine). *Soit $\psi : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ une fonction décroissante.*

- Si $\int_1^\infty \psi(u)^{d-1} \frac{du}{u} < +\infty$, alors pour presque tout $x \in \mathbb{P}^{d-1}(\mathbb{R})$, l'inégalité (9.1) admet un nombre fini de solutions $v \in \mathbb{P}^{d-1}(\mathbb{Q})$.
- Si $\int_1^\infty \psi(u)^{d-1} \frac{du}{u} = +\infty$, alors pour presque tout $x \in \mathbb{P}^{d-1}(\mathbb{R})$, l'inégalité (9.1) admet une infinité de solutions $v \in \mathbb{P}^{d-1}(\mathbb{Q})$.

L'exposant diophantien d'un point $x \in \mathbb{P}^{d-1}(\overline{\mathbb{Q}})$ a été calculé par Schmidt [52] grâce à son théorème du sous-espace, qui généralise les résultats de Thue [60], Siegel [57] et Roth [48] pour $\mathbb{P}^1(\overline{\mathbb{Q}})$.

Théorème 9.1.3 (Théorème de Thue-Siegel-Roth-Schmidt). *Si $x \in \mathbb{P}^{d-1}(\overline{\mathbb{Q}})$, alors $\beta(x) = 1 + \frac{1}{d_x}$, où d_x est la dimension du plus petit sous-espace projectif rationnel contenant x .*

Le problème de l'approximation diophantienne sur les sous-variétés a été posé en premier par Mahler [43] pour la courbe $[1 : x : x^2 : \dots : x^{d-1}]$ dans \mathbb{P}^{d-1} . Ayant résolu le problème de Mahler, Sprindzuk a conjecturé dans [59] le résultat suivant, démontré finalement par Kleinbock et Margulis [31] en 1998. Rappelons qu'une sous-variété $M \subset \mathbb{P}^{d-1}(\mathbb{R})$ est dite non dégénérée si elle n'est incluse dans aucun sous-espace projectif strict.

Théorème 9.1.4 (Théorème de Kleinbock-Margulis). *Toute sous-variété analytique connexe non dégénérée dans $\mathbb{P}^{d-1}(\mathbb{R})$ est extrémale.*

Dans un travail en commun avec Emmanuel Breuillard [12], nous avons observé que les méthodes utilisées pour démontrer ces deux derniers théorèmes permettent de donner une formule pour l'exposant d'un point pris aléatoirement sur une sous-variété algébrique définie sur $\overline{\mathbb{Q}}$.

Théorème 9.1.5 (Exposant d'une sous-variété définie sur $\overline{\mathbb{Q}}$). *Soit $M \subset \mathbb{P}^{d-1}(\mathbb{R})$ une sous-variété analytique connexe. On suppose que le plus petit sous-espace projectif réel contenant M est défini sur $\overline{\mathbb{Q}}$. Alors, pour presque tout $x \in M$, $\beta(x) = 1 + \frac{1}{d_M}$, où d_M est la dimension du plus petit sous-espace projectif rationnel contenant M . En particulier, si M est non dégénérée, alors M est extrémale.*

Remarque. Dans l'espace projectif, les sous-variétés de Schubert ne sont autres que les sous-espaces projectifs. Toute sous-variété de Schubert stricte est instable pour le flot (a_t) , et par conséquent, si une sous-variété M n'est incluse dans aucune sous-variété de Schubert instable, elle est non dégénérée.

9.2 Quadriques

À notre connaissance, ce sont Kleinbock et Merrill [36] qui ont obtenu les premiers résultats remarquables pour l'approximation diophantienne intrinsèque sur les quadriques, en démontrant pour une sphère de dimension arbitraire les analogues des théorèmes de Dirichlet et de Khintchine. Dans un article avec Fishman et Simmons [20], ils ont ensuite généralisé leurs résultats à une quadrique arbitraire. Pour une introduction élémentaire à ces problèmes, on renvoie à l'article [35].

Dans ce cadre X désigne une quadrique projective non singulière, i.e. l'ensemble des droites isotropes pour une forme quadratique rationnelle Q non dégénérée sur \mathbb{R}^d . La distance et la hauteur sur X sont obtenues par restriction de la distance et de la hauteur usuelles sur \mathbb{P}^{d-1} . On suppose en outre que X contient un point rationnel ; par projection stéréographique, cela implique en fait que $X(\mathbb{Q})$ est dense dans $X(\mathbb{R})$.

Théorème 9.2.1 (Fishman-Kleinbock-Merrill-Simmons). *Soit X une quadrique rationnelle projective non singulière contenant un point rationnel. Pour presque tout $x \in X(\mathbb{R})$, $\beta(x) = 1$.*

Soit $X_0 \subset \mathbb{P}^3$ la quadrique définie par l'équation $x_1x_2 - x_3x_4$. La généralisation du théorème de Khintchine aux quadriques nécessite de distinguer deux cas, suivant que la quadrique X est rationnellement isomorphe à X_0 , ou non.

Théorème 9.2.2 (Fishman-Kleinbock-Merrill-Simmons). *Soit X une quadrique rationnelle projective non singulière de dimension n contenant un point rationnel, et $\psi : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ une fonction décroissante. Pour $x \in X(\mathbb{R})$ on considère l'inégalité*

$$d(x, v) \leq H(v)^{-1} \psi(H(v)). \quad (9.2)$$

Si X n'est pas rationnellement isomorphe à X_0 , alors :

- *si $\int_1^\infty \psi(u)^n \frac{du}{u} = +\infty$, l'inégalité (9.2) admet une infinité de solutions $v \in X(\mathbb{Q})$ pour presque tout $x \in X(\mathbb{R})$;*
- *si $\int_1^\infty \psi(u)^n \frac{du}{u} < +\infty$, l'inégalité (9.2) n'a qu'un nombre fini de solutions $v \in X(\mathbb{Q})$ pour presque tout $x \in X(\mathbb{R})$.*

Si X est rationnellement isomorphe à X_0 , alors :

- *si $\int_1^\infty \psi(u)^n (\log \log u) \frac{du}{u} = +\infty$, l'inégalité (9.2) admet une infinité de solutions $v \in X(\mathbb{Q})$ pour presque tout $x \in X(\mathbb{R})$;*
- *si $\int_1^\infty \psi(u)^n (\log \log u) \frac{du}{u} < +\infty$, l'inégalité (9.2) n'a qu'un nombre fini de solutions $v \in X(\mathbb{Q})$ pour presque tout $x \in X(\mathbb{R})$.*

Remarque. Écrivons $X = P \backslash G$, où $G = \mathrm{SO}_Q$ est le groupe orthogonal associé à la forme quadratique Q , et P le sous-groupe parabolique stabilisateur d'une droite rationnelle isotrope dans la représentation standard. Si $X \not\sim X_0$, le groupe G est \mathbb{Q} -simple et le sous-groupe parabolique P est maximal : $\mathrm{rang}_{\mathbb{Q}} P = \mathrm{rang}_{\mathbb{Q}} G - 1$. En revanche, si $X \sim X_0$, on a un isomorphisme $G \simeq \mathrm{SO}(2, 2) \simeq \mathrm{SO}(2, 1) \times \mathrm{SO}(2, 1)$, et $\mathrm{rang}_{\mathbb{Q}} P = \mathrm{rang}_{\mathbb{Q}} G - 2$. Avec les résultats généraux du chapitre 3, et en particulier les lemmes 3.1.2 et 3.1.3, cette différence explique la distinction de cas dans le théorème ci-dessus.

Dans un article récent [16], nous avons poursuivi les travaux de Fishman, Kleinbock, Merrill et Simmons en étudiant l'approximation diophantienne des points algébriques et des quantités dépendantes sur les quadriques. Cela nous a permis en particulier d'établir le résultat suivant.

Théorème 9.2.3 (Exposant diophantien d'une sous-variété algébrique). *Soit X une quadrique rationnelle projective non singulière contenant un point rationnel, et M une sous-variété analytique de X . On suppose que le plus petit sous-espace totalement isotrope réel contenant M est défini sur $\overline{\mathbb{Q}}$. Alors, pour presque tout $x \in M$,*

$$\beta(x) = 1 + \frac{1}{d_M},$$

où d_M est la dimension du plus petit sous-espace totalement isotrope rationnel contenant M . (S'il n'existe pas de tel sous-espace, on pose $d_M = +\infty$.)

Remarque. Le théorème ci-dessus s'applique en particulier dans les deux cas suivants :

- si $M = \{x\}$ est réduite à un seul point $x \in X(\overline{\mathbb{Q}})$, on obtient un analogue du résultat de Thue-Siegel-Roth-Schmidt pour la quadrique X ;
- si M est *non dégénérée*, i.e. n'est incluse dans aucun sous-espace totalement isotrope, alors $d_M = +\infty$ et M est extrémale.

Remarque. Dans une quadrique X , les sous-variétés de Schubert sont les sous-espaces totalement isotropes, toute sous-variété de Schubert stricte est instable. Comme dans le cas de l'espace projectif, une sous-variété n'est incluse dans aucune sous-variété de Schubert instable si et seulement si elle est non dégénérée.

9.3 Grassmannienne

Dans l'article [51] écrit en 1967, Schmidt a proposé d'utiliser le plongement de Plücker pour définir la hauteur d'un sous-espace rationnel, et étudier l'approximation d'un sous-espace réel x par des sous-espaces rationnels v de diverses dimensions. Cela s'inscrit bien dans le cadre de ce mémoire : si $G = \mathrm{SL}_d$ et P le sous-groupe parabolique stabilisateur du sous-espace $\mathrm{Vect}\{e_1, \dots, e_\ell\}$ dans la représentation standard, on obtient la grassmannienne des ℓ -plans dans un espace de dimension d comme quotient

$$X = \mathrm{Grass}(\ell, d) \simeq P \backslash G.$$

La hauteur utilisée par Schmidt est alors celle associée à la représentation fondamentale $\wedge^\ell \mathbb{R}^d$, la distance est la distance riemannienne usuelle. Cela permet de définir l'exposant diophantien d'un point $x \in \mathrm{Grass}(\ell, d)$. Avec ces définitions, Schmidt obtient une minoration optimale de l'exposant diophantien d'un point choisi aléatoirement sur la grassmannienne : pour presque tout $x \in \mathrm{Grass}(\ell, d)$, $\beta(x) \geq \frac{1}{\ell} + \frac{1}{d-\ell}$. Le théorème 2.4.5 permet de préciser ce résultat en une égalité presque sûre.

Théorème 9.3.1. *Pour presque tout $x \in \mathrm{Grass}(\ell, d)$, $\beta(x) = \frac{1}{\ell} + \frac{1}{d-\ell}$.*

Pour une variété grassmannienne, le théorème 3.2.1, analogue du théorème de Khintchine, s'écrit plus simplement comme suit.

Théorème 9.3.2. *Soit $X = \text{Grass}(\ell, d)$ la variété grassmannienne des sous-espaces de dimension ℓ dans un espace de dimension d . Étant donnée une fonction décroissante $\psi : \mathbb{R}^+ \rightarrow \mathbb{R}^+$ on considère l'inégalité*

$$d(x, v) \leq H(v)^{-\frac{1}{\ell} - \frac{1}{d-\ell}} \psi(H(v)). \tag{9.3}$$

- Si $\int_1^\infty \psi(u)^{\ell(d-\ell)} \frac{du}{u} = +\infty$, alors (9.3) admet une infinité de solutions $v \in X(\mathbb{Q})$ pour presque tout $x \in X(\mathbb{R})$.
- Si $\int_1^\infty \psi(u)^{\ell(d-\ell)} \frac{du}{u} < +\infty$, alors (9.3) n'admet qu'un nombre fini de solutions $v \in X(\mathbb{Q})$ pour presque tout $x \in X(\mathbb{R})$.

Remarque. On remarque que l'exposant $\ell(d - \ell)$ qui apparaît dans la condition d'intégrabilité sur ψ est égal à la dimension de X . Pour calculer cet exposant, on peut utiliser le lemme 3.1.2. La somme des racines apparaissant dans le radical unipotent de P est

$$\begin{aligned} \rho_\ell &= \sum_{\substack{1 \leq i \leq \ell \\ \ell < j \leq d}} \varepsilon_i - \varepsilon_j \\ &= (d - \ell)(\varepsilon_1 + \dots + \varepsilon_\ell) - \ell(\varepsilon_{\ell+1} + \dots + \varepsilon_d) \\ &= d(\varepsilon_1 + \dots + \varepsilon_\ell) = d\omega_\ell. \end{aligned}$$

L'exposant recherché est donc

$$\frac{a_X}{\beta_X} = \frac{d}{\frac{1}{\ell} + \frac{1}{d-\ell}} = \ell(d - \ell).$$

Toute sous-variété de Schubert X_{wg} dans $X = \text{Grass}(\ell, d)$ est de la forme

$$X_{wg} = \{x \in X \mid \forall i = 1, \dots, d - 1, \dim x \cap V_i \geq m_i\},$$

où $\{0\} = V_0 < V_1 < \dots < V_d = \mathbb{R}^d$ est un drapeau total de \mathbb{R}^d et $m_1 \leq \dots \leq m_d$ une suite d'entiers naturels. On peut montrer que toute sous-variété de Schubert distincte de $X = \text{Grass}(\ell, d)$ est incluse dans un pinceau

$$P_{W,r} = \{x \in X \mid \dim W \cap x \geq r\} \quad \text{avec } r > d - \ell - \dim W,$$

et qu'une sous-variété de Schubert est instable si et seulement si elle est incluse dans un pinceau $P_{W,r}$ contraignant, i.e. satisfaisant

$$\frac{r}{\dim W} > \frac{\ell}{d}.$$

Les théorèmes généraux de ce mémoire impliquent donc les résultats suivants.

Théorème 9.3.3 (Critère d'extrémalité dans la grassmannienne). *Soit M une sous-variété analytique de $\text{Grass}(\ell, d)$. Si M n'est incluse dans aucun pinceau contraignant, alors M est extrémale.*

À toute partie $M \subset X$, on associe un drapeau rationnel partiel $\{0\} = V_{d_0} < V_{d_1} < \dots < V_{d_{r-1}} < V_{d_r} = \mathbb{Q}^d$ avec pour chaque k , $\dim V_{d_k} = d_k$. Pour cela, on définit V_{d_1} comme l'unique sous-espace rationnel de dimension maximale qui maximise la quantité $\min_{x \in M} \frac{\dim x \cap V}{\dim V}$, parmi tous les sous-espaces vectoriels $V \leq \mathbb{Q}^d$; ensuite V_{d_2} est l'unique sous-espace rationnel contenant V_{d_1} , de dimension maximale, et qui maximise $\min_{x \in M} \frac{\dim x \cap V - \dim x \cap V_{d_1}}{\dim V - d_1}$, ...etc.

Théorème 9.3.4 (Exposant d'une sous-variété algébrique). *Soit M une sous-variété analytique connexe de $\text{Grass}(\ell, d)$ dont l'adhérence de Zariski est définie sur \mathbb{Q} , et $V_0 < V_{d_1} < \dots < V_{d_r}$, le drapeau partiel associé à M . Pour $k = 1, \dots, r$, on note*

$$i_k = \min_{x \in M} \dim x \cap V_{d_k} \quad \text{et} \quad c_k = -\frac{i_k}{\ell} + \frac{d_k - i_k}{d - \ell}.$$

Pour presque tout x dans M ,

$$\beta(x) = \left(\frac{1}{\ell} + \frac{1}{d - \ell} \right) \frac{1}{1 - \gamma_M},$$

où

$$\gamma_M = \sum_{k=1}^r \frac{i_k - i_{k-1}}{d_k - d_{k-1}} \left(\frac{i_k - i_{k-1}}{\ell} - \frac{d_k - d_{k-1} - i_k + i_{k-1}}{d - \ell} \right) = \frac{\ell(d - \ell)}{d} \sum_{k=1}^r \frac{(c_k - c_{k-1})^2}{d_k - d_{k-1}}.$$

En particulier, M est extrémale si, et seulement si, M n'est incluse dans aucun pinceau rationnel contraignant.

Démonstration. Nous donnerons une démonstration directe dans [15]. Ici nous remarquons seulement que ce théorème est un cas particulier du théorème 8.3.1; il suffit de voir que le drapeau partiel $\{0\} < V_{d_1} < \dots < V_{d_r}$ s'identifie à la variété de Schubert $X_w \gamma_M$ contenant M , et de faire le calcul explicite de la quantité $\langle \chi^w, p_{a^-}(Y^w) \rangle$. Les détails sont laissés au lecteur. Pour vérifier l'égalité entre les deux formules pour γ_M , il suffit d'observer que

$$i_k = \frac{\ell}{d} d_k - \frac{\ell(d - \ell)}{d} c_k,$$

et donc

$$\frac{i_k - i_{k-1}}{d_k - d_{k-1}} \left(\frac{i_k - i_{k-1}}{\ell} - \frac{d_k - d_{k-1} - i_k + i_{k-1}}{d - \ell} \right) = -\frac{\ell}{d} \left(1 - \frac{c_k - c_{k-1}}{d_k - d_{k-1}} (d - \ell) \right) (c_k - c_{k-1}).$$

L'égalité souhaitée s'en déduit en sommant sur k , et en observant que $0 = c_r = \sum_{k=1}^r c_k - c_{k-1}$.

Si M n'est incluse dans aucun pinceau rationnel contraignant, alors le drapeau associé est le drapeau trivial $\{0\} = V_0 < V_d = \mathbb{Q}^d$, donc $\gamma_M = 0$ et $\beta(x) = \frac{1}{\ell} + \frac{1}{d - \ell}$ pour presque tout x dans M . Réciproquement, s'il existe un pinceau rationnel contraignant contenant M , alors le drapeau associé à M est non trivial, et la formule ci-dessus montre donc que $\gamma_M > 0$. Cela implique que M n'est pas extrémale. \square

Dans son article [51], après avoir obtenu plusieurs encadrements pour l'exposant diophantien d'un élément $x \in \text{Grass}(\ell, d)$, Schmidt pose notamment le problème suivant : déterminer la valeur minimale de $\beta(x)$ lorsque x varie dans $X(\mathbb{R})$. Il est possible que cette valeur soit égale à $\frac{1}{\ell} + \frac{1}{d - \ell}$, valeur presque sûre de $\beta(x)$ lorsque x est choisi aléatoirement dans X . Nous n'avons pas de preuve de cela pour l'instant. Cependant, le théorème ci-dessus permet déjà de minorer convenablement l'exposant de tout point de $X(\mathbb{Q})$. En fait, dans l'écriture $X = P \backslash G$, le sous-groupe parabolique est maximal, et le corollaire ci-dessous est donc un cas particulier du corollaire 5.3.2.

Corollaire 9.3.5. *Soit $X = \text{Grass}(\ell, d)$. Pour tout $x \in X(\overline{\mathbb{Q}})$, $\beta(x) \geq \frac{1}{\ell} + \frac{1}{d - \ell}$, avec égalité si et seulement si x n'est inclus dans aucun pinceau rationnel contraignant.*

Exemple. Soit $X = \text{Grass}(2, d)$ la variété des 2-plans dans \mathbb{R}^d . Dans ce cas,

$$a_t = e^{tY}, \quad \text{avec} \quad Y = \frac{1}{\frac{1}{2} + \frac{1}{d-2}} \text{diag}\left(-\frac{1}{2}, -\frac{1}{2}, \frac{1}{d-2}, \dots, \frac{1}{d-2}\right).$$

On considère la sous-variété

$$M = \{x \in X \mid \dim x \cap V_1 \geq 1\}, \quad \text{où } V_1 = \text{Vect}(e_1, \dots, e_k).$$

Si $k < \frac{d}{2}$, M est un pinceau contraignant. Pour presque tout x dans M ,

$$\begin{aligned} c_\infty &= \lim_{t \rightarrow \infty} \frac{1}{t} c(a_t s_x) \\ &= \text{diag}\left(-\frac{1}{k} \frac{d-2k}{2(d-2)}, \dots, -\frac{1}{k} \frac{d-2k}{2(d-2)}, \frac{1}{d-k} \frac{d-2k}{2(d-2)}, \dots, \frac{1}{d-k} \frac{d-2k}{2(d-2)}\right). \end{aligned}$$

En fait, si w est une matrice de permutation telle que $w^{-1}\{1, 2\} = \{k, d\}$ (cela détermine un élément de W_P), alors

$$M = PwB.$$

On vérifie sans peine que $c_\infty = p_{\mathfrak{a}^-}(Y^w)$. D'ailleurs, $\theta_\infty = [1, d-1] \setminus \{k\}$ et si $\pi_\infty : \mathfrak{a} \rightarrow \mathfrak{a}$ est la projection sur $\bigcap_{i \in \theta_\infty} \alpha_i^\perp$ (l'espace des fonctions dont le seul point angulaire est en k), alors $c_\infty = p_{\mathfrak{a}^-}(Y^w) = \pi_\infty(Y^w)$.

La hauteur associée au plongement de Plücker correspond au plus haut poids $\chi = \varepsilon_1 + \varepsilon_2$, et $\chi^w = \varepsilon_{w^{-1}(1)} + \varepsilon_{w^{-1}(2)} = \varepsilon_k + \varepsilon_d$. Par conséquent, pour presque tout $x \in M$,

$$\gamma_\chi(x) = \langle \chi^w, \pi_\infty(Y^w) \rangle = -\frac{1}{k} \frac{d-2k}{2(d-2)} + \frac{1}{d-k} \frac{d-2k}{2(d-2)} = -\frac{(d-2k)^2}{2(d-2)k(d-k)},$$

et

$$\beta(x) = \left(\frac{1}{2} + \frac{1}{d-2}\right) \frac{1}{1 - \gamma_\chi(x)}.$$

Dans cet exemple, le sous-groupe Q_M est égal au stabilisateur de V_1 dans la représentation standard. Si $V_2 = \text{Vect}(e_{k+1}, \dots, e_d)$, on peut identifier le facteur de Levi de Q_M à $L_M = \text{GL}(V_1) \times \text{GL}(V_2)$. La représentation V_χ se décompose en irréductibles pour L_M de la façon suivante :

$$V_\chi = \wedge^2 V_1 \oplus V_1 \otimes V_2 \oplus \wedge^2 V_2.$$

La représentation irréductible contenant $we_\chi = e_k \wedge e_d$ est $V_1 \otimes V_2$. Grâce à la base $(e_i \wedge e_j)_{1 \leq i \leq k; k+1 \leq j \leq d}$, on calcule facilement le taux de contraction de $V_1 \wedge V_2$ par $a_t^w = e^{tY^w}$:

$$\frac{2}{d-2}(k-1)(d-k-1) + \left(\frac{1}{d-2} - \frac{1}{2}\right)(k-1) + \left(-\frac{1}{2} + \frac{1}{d-2}\right)(d-k-1) - 1 = -\frac{(d-2k)^2}{2(d-2)}$$

Comme $\dim V_1 \otimes V_2 = k(d-k)$, on trouve bien la même valeur que ci-dessus pour $\gamma_\chi(x)$.

9.4 Variété des drapeaux dans \mathbb{R}^d

Drapeaux dans \mathbb{R}^3 .

Ici $G = \mathrm{SL}_3$ et P est le sous-groupe parabolique minimal constitué des matrices triangulaires supérieures. La variété quotient $X = P \backslash G$ s'identifie à l'ensemble des drapeaux dans \mathbb{R}^3 :

$$X = \{x = (x_1, x_2) ; x_1 \in \mathrm{Grass}(1, 3), x_2 \in \mathrm{Grass}(2, 3), x_1 \leq x_2\}.$$

Cette fois, la distance de Carnot-Carathéodory sur X n'est pas riemannienne. Géométriquement, pour se déplacer en partant d'un drapeau $x = (x_1, x_2)$, on s'autorise à déplacer infinitésimalement x_1 dans x_2 , et x_2 contenant x_1 ; cela définit un champ de plans sur X , et les seuls chemins autorisés sont ceux qui sont tangents à ce champ de plans.

Le flot diagonal est donné par l'élément $Y = \mathrm{diag}(1, 0, -1)$. Les éléments I , $(1, 2)$ et $(2, 3)$ du groupe de Weyl S_3 donnent les variétés de Schubert instables. Dire qu'une M est incluse dans une cellule instable revient donc à dire que tous les éléments de M ont la même droite, ou le même plan.

Les autres sous-variétés de Schubert sont stables. Par exemple, la variété $M = \{(x_1, x_2) \mid x_2 \ni e_1\}$ est extrémale quel que soit le choix de hauteur sur $X(\mathbb{Q})$.

D'après le corollaire 5.3.3, si X est munie de la hauteur anti-canonique, alors

$$\forall x \in X(\overline{\mathbb{Q}}), \quad \beta_\chi(x) \geq \beta_\chi(X),$$

avec égalité si et seulement si x n'est inclus dans aucune sous-variété de Schubert rationnelle instable. En fait, pour la variété X des drapeaux dans \mathbb{R}^3 , ce résultat est encore valable quelle que soit la hauteur H_χ sur X .

Drapeaux dans \mathbb{R}^4 .

Cette fois, $G = \mathrm{SL}_4$ et $P = B$ est le sous-groupe parabolique minimal constitué des matrices triangulaires supérieures. La variété quotient $X = P \backslash G$ s'identifie à l'ensemble des drapeaux dans \mathbb{R}^4 :

$$X = \{x = (x_1, x_2, x_3) ; x_1 < x_2 < x_3, x_i \in \mathrm{Grass}(i, 4), i = 1, 2, 3\}.$$

C'est une variété de dimension 6, et la distance de Carnot-Carathéodory sur X est déterminée par un champ de 3-plans : au voisinage de (x_1, x_2, x_3) , on s'autorise à déplacer infinitésimalement x_1 dans x_2 , x_2 contenant x_1 et à l'intérieur de x_3 , et x_3 contenant x_2 .

Le flot diagonal (a_t) est donné par l'élément

$$Y = \frac{1}{2} \mathrm{diag}(-3, -1, 1, 3).$$

En écrivant la liste des Y^w , pour $w \in S_4$ on vérifie que

1. Si $w^{-1}(4) = 4$, tous les éléments de $M = BwB$ ont le même hyperplan, et M est instable.
2. Si $w^{-1}(4) = 3$, il existe un plan p tel que pour tout (x_1, x_2, x_3) dans $M = BwB$, $p \subset x_3$. La variété M est instable sauf si $w^{-1} : (1, 2, 3, 4) \mapsto (4, 2, 1, 3)$.

3. Si $w^{-1}(4) = 2$, il existe une droite d tel que pour tout (x_1, x_2, x_3) dans $M = BwB$, $d \subset x_3$. La variété M est instable sauf si $w^{-1} : (1, 2, 3, 4) \mapsto (4, 3, 1, 2)$ (aucune autre contrainte) ou $w^{-1} : (1, 2, 3, 4) \mapsto (3, 4, 1, 2)$ (on impose en outre qu'il existe un hyperplan h tel que pour tout x dans M , $x_1 \subset h$.)
4. Si $w^{-1}(4) = 1$, il n'y a pas de contrainte sur x_3 , et $M = BwB$ n'est pas instable, sauf pour $w^{-1} : (1, 2, 3, 4) \mapsto (2, 3, 4, 1)$ et $w^{-1} : (1, 2, 3, 4) \mapsto (3, 2, 4, 1)$.

Le corollaire 5.3.3 montre que si X est munie de la hauteur anti-canonique, alors tout point $x \in X(\overline{\mathbb{Q}})$ vérifie $\beta_\chi(x) \geq \beta_\chi(X)$. Cela cependant n'est pas vrai en général, comme le montre l'exemple suivant.

Exemple (Des points très mal approchables). Pour certains choix de hauteur sur la variété X des drapeaux dans \mathbb{R}^4 , il peut exister un point algébrique moins bien approchable qu'un point générique. On choisit un point x tel que $\langle e_1, e_2, e_4 \rangle$ soit stable par $a_t x$, et générique pour le reste. En d'autres termes, pour un élément p algébrique générique de $P(\overline{\mathbb{Q}})$,

$$x = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \cdot p = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ 0 & 0 & * & 0 \\ * & * & * & * \end{pmatrix}$$

Le sous-espace $\langle e_1, e_2, e_4 \rangle$ est semi-stable, contracté globalement par $e^{-\frac{t}{2}}$, donc les trois premiers minima successifs de $a_t x \mathbb{Z}^4$ sont atteints dans $\langle e_1, e_2, e_4 \rangle$, de longueur approximativement $e^{-\frac{t}{6}}$. Le dernier minimum est donc de longueur $e^{\frac{t}{2}}$. On choisit alors le poids χ induit par la représentation de plus haut poids $(k+2)\varepsilon_1 + (k+1)\varepsilon_2 + k\varepsilon_3$, avec k suffisamment grand. Cela correspond au diagramme de Young de longueurs $(k+2, k+1, k)$, ou en termes de poids fondamentaux : $\omega_1 + \omega_2 + k\omega_3$. Le vecteur e_χ est donné par le tableau rempli avec des 1 sur la première ligne, des 2 sur la deuxième, et des 3 sur la troisième.

Les premiers minima successifs de $a_t x V(\mathbb{Z})$ sont atteints avec des tableaux contenant seulement $(1, 2, 4)$; il valent à peu près $e^{-\frac{(3k+3)t}{6}}$. Ensuite viennent ceux qui contiennent une occurrence de 3, puis deux occurrences de 3, ...etc. Mais pour avoir une projection positive sur e_χ , il faut au moins k occurrences de 3, et alors la norme du vecteur est minorée par $e^{k\frac{t}{2} - (2k+3)\frac{t}{6}} = e^{(k-3)\frac{t}{6}}$. Dès que $k > 3$, on voit que $r_\chi(a_t x)$ tend vers l'infini à vitesse exponentielle, ce qui montre que $\gamma_\chi(x) < 0$, et donc $\beta_\chi(x) < \beta_\chi(X)$.

Remarque. On peut même donner un exemple pour la variété X des drapeaux dans \mathbb{R}^3 , si l'on autorise une quasi-distance différente de la distance de Carnot-Carothédory. À une petite perturbation près de a_t et χ , pour que P soit bien le sous-groupe de Borel, l'exemple est le suivant : $a_t = \text{diag}(e^{-2t}, e^t, e^t)$, et x est tel que $\langle e_1, e_3 \rangle$ est stable par $a_t x$. Les deux premiers minima successifs de $a_t x \mathbb{Z}^3$ sont atteints dans $\langle e_1, e_3 \rangle$, et de longueur $e^{-\frac{t}{2}}$; le troisième est de longueur e^t .

On choisit le poids χ donné par $\varepsilon_1 + \varepsilon_2$, ce qui correspond à la représentation $\wedge^2 \mathbb{R}^3$. On a alors $e_\chi = e_1 \wedge e_2$. Le premier minimum de $a_t x \wedge^2 \mathbb{Z}^3$ est de longueur e^{-t} mais sa projection sur e_χ est nulle. Les deux suivants sont de longueur $e^{\frac{t}{2}}$, et cela montre bien que $r_\chi(a_t x)$ tend vers l'infini à vitesse exponentielle.

Chapitre 10

Conclusion

Nous concluons ce mémoire par quelques problèmes ouverts qui nous semblent mériter d'être mentionnés.

Valeur minimale de l'exposant. Soit $X = P \backslash G$ une variété de drapeaux munie de la distance de Carnot-Carathéodory usuelle et de la hauteur induite par un poids dominant χ .

- Si χ est choisi de sorte que X est munie de la hauteur anti-canonique, a-t-on, pour tout $x \in X(\mathbb{Q})$, $\beta(x) \geq \beta(X)$? D'après le théorème 5.3.1, cela reviendrait à dire que dans ce cas, on a toujours $\langle \chi^w, p_{\mathfrak{a}}(Y^w) \rangle \leq 0$, quel que soit $w \in W_P$. Nous avons vu aux corollaires 5.3.2 et 5.3.3 que cette inégalité est valable lorsque X est de rang 1 ou lorsque G est déployé et P minimal.
- Déterminer $\inf_{x \in X(\mathbb{R})} \beta_{\chi}(x)$. Y a-t-il une égalité

$$\inf_{x \in X(\mathbb{R})} \beta_{\chi}(x) = \inf_{x \in X(\mathbb{Q})} \beta_{\chi}(x)?$$

Par exemple, pour la grassmannienne $X = \text{Grass}(\ell, d)$, a-t-on, pour tout x , $\beta(x) \geq \frac{1}{\ell} + \frac{1}{d-\ell}$?

Métrie riemannienne. Soit X une variété de drapeaux rationnelle. Lorsque X est munie d'une distance riemannienne, peut-on montrer des résultats analogues à ceux établis dans ce mémoire pour la métrie de Carnot-Carathéodory?

Autres variétés algébriques. Soit X une variété algébrique irréductible X définie sur \mathbb{Q} , munie d'une distance et d'une hauteur, ce qui permet de définir l'exposant diophantien $\beta(x)$ d'un point x dans $X(\mathbb{R})$. L'exposant diophantien est-il constant presque sûrement sur $X(\mathbb{R})$? Peut-on calculer sa valeur? Plus généralement, en dehors des variétés de drapeaux, pour quelles variétés algébriques peut-on obtenir une théorie de l'approximation diophantienne intrinsèque satisfaisante?

Bibliographie

- [1] Menny AKA, Emmanuel BREUILLARD, Lior ROSENZWEIG et Nicolas DE SAXCÉ. Diophantine properties of nilpotent Lie groups. *Compos. Math.*, 151(6) :1157-1188, 2015.
- [2] Menny AKA, Emmanuel BREUILLARD, Lior ROSENZWEIG et Nicolas de SAXCÉ. Diophantine approximation on matrices and Lie groups. *Geom. Funct. Anal.*, 28(1) :1-57, 2018.
- [3] Anne-Marie AUBERT et Roger HOWE. Géométrie des cônes aigus et application à la projection euclidienne sur la chambre de Weyl positive. *J. Algebra*, 149(2) :472-493, 1992.
- [4] A. BAKER. Linear forms in the logarithms of algebraic numbers. *Mathematika*, 13 :204-216, 1966.
- [5] V. BERESNEVICH et L. YANG. Khintchine's theorem and diophantine approximation on manifolds. *preprint arXiv :2105.13872*.
- [6] Victor BERESNEVICH. Rational points near manifolds and metric Diophantine approximation. *Ann. Math. (2)*, 175(1) :187-235, 2012.
- [7] Victor BERESNEVICH et Sanju VELANI. A mass transference principle and the Duffin-Schaeffer conjecture for Hausdorff measures. *Ann. Math. (2)*, 164(3) :971-992, 2006.
- [8] Armand BOREL. *Introduction aux groupes arithmétiques*. Publications de l'Institut de Mathématique de l'Université de Strasbourg, XV. Actualités Scientifiques et Industrielles, No. 1341. Hermann, Paris, 1969, page 125.
- [9] Armand BOREL et HARISH-CHANDRA. Arithmetic subgroups of algebraic groups. *Ann. Math. (2)*, 75 :485-535, 1962.
- [10] Armand BOREL et Jacques TITS. Groupes réductifs. *Inst. Hautes Études Sci. Publ. Math.*, (27) :55-150, 1965.
- [11] N. BOURBAKI. *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV : Groupes de Coxeter et systèmes de Tits. Chapitre V : Groupes engendrés par des réflexions. Chapitre VI : systèmes de racines*. Actualités Scientifiques et Industrielles, No. 1337. Hermann, Paris, 1968, 288 pp. (loose errata).
- [12] E. BREUILLARD et N. de SAXCÉ. A subspace theorem for manifolds. *preprint arXiv :2101.04055v2*.
- [13] S. G. DANI. Divergent trajectories of flows on homogeneous spaces and diophantine approximation. *J. Reine Angew. Math.*, 359 :55-89, 1985.

- [14] S. G. DANI. On orbits of unipotent flows on homogeneous spaces. II. *Ergodic Theory Dynam. Systems*, 6(2) :167-182, 1986.
- [15] N. de SAXCÉ. Approximation diophantienne dans la grassmannienne. *en préparation*.
- [16] N. de SAXCÉ. Approximation diophantienne sur les quadriques. *manuscrit disponible à l'adresse <https://www.math.univ-paris13.fr/~desaxce/>*.
- [17] DIRICHLET. Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen. *S. B. Preuss. Akad. Wiss.* :93-95, 1842.
- [18] M. EINSIEDLER, G. MARGULIS, A. MOHAMMADI et A. VENKATESH. Effective equidistribution and property (τ) . *J. Am. Math. Soc.*, 33(1) :223-289, 2020.
- [19] Lior FISHMAN, Dmitry KLEINBOCK, Keith MERRILL et David SIMMONS. Intrinsic Diophantine approximation on manifolds : general theory. *Trans. Am. Math. Soc.*, 370(1) :577-599, 2018.
- [20] FISHMAN, KLEINBOCK, MERRILL et SIMMONS. Intrinsic diophantine approximation on quadric hypersurfaces. *preprint arXiv :1405.7650v5*, 2014.
- [21] Jens FRANKE, Yuri I. MANIN et Yuri TSCHINKEL. Rational points of bounded height on Fano varieties. *Invent. Math.*, 95(2) :421-435, 1989.
- [22] Anish GHOSH, Alexander GORODNIK et Amos NEVO. Best possible rates of distribution of dense lattice orbits in homogeneous spaces. *J. Reine Angew. Math.*, 745 :155-188, 2018.
- [23] Anish GHOSH, Alexander GORODNIK et Amos NEVO. Diophantine approximation and automorphic spectrum. *Int. Math. Res. Not.*, 2013(21) :5002-5058, 2013.
- [24] Anish GHOSH, Alexander GORODNIK et Amos NEVO. Metric Diophantine approximation on homogeneous varieties. *Compos. Math.*, 150(8) :1435-1456, 2014.
- [25] Mikhael GROMOV. Carnot-Carathéodory spaces seen from within. In *Sub-Riemannian geometry*. Tome 144, Progr. Math. Pages 79-323. Birkhäuser, Basel, 1996.
- [26] David A. jun. VOGAN. *Representations of real reductive Lie groups*, tome 15. Birkhäuser/Springer, Basel, 1981.
- [27] George R. KEMPF. Instability in invariant theory. *Ann. Math. (2)*, 108 :299-316, 1978.
- [28] A. KHINTCHINE. Einige Sätze über Kettenbrüche, mit Anwendungen auf die Theorie der Diophantischen Approximationen. *Math. Ann.*, 92 :115-125, 1924.
- [29] A. KHINTCHINE. Zur metrischen Theorie der diophantischen Approximationen. *Mathematische Zeitschrift*, 24 :706-714, 1, 1926.
- [30] D. Y. KLEINBOCK et G. A. MARGULIS. Erratum to : logarithm laws for flows on homogeneous spaces. *Invent. Math.*, 211(2) :855-862, 2018.
- [31] D. Y. KLEINBOCK et G. A. MARGULIS. Flows on homogeneous spaces and diophantine approximation on manifolds. *Ann. of Math. (2)*, 148(1) :339-360, 1998.

- [32] D. Y. KLEINBOCK et G. A. MARGULIS. Logarithm laws for flows on homogeneous spaces. *Invent. Math.*, 138(3) :451-494, 1999.
- [33] Dmitry KLEINBOCK. An ‘almost all versus no’ dichotomy in homogeneous dynamics and diophantine approximation. *Geom. Dedicata*, 149 :205-218, 2010.
- [34] Dmitry KLEINBOCK. An extension of quantitative nondivergence and applications to diophantine exponents. *Trans. Amer. Math. Soc.*, 360(12) :6497-6523, 2008.
- [35] Dmitry KLEINBOCK et Nicolas de SAXCÉ. Rational approximation on quadrics : a simplex lemma and its consequences. *Enseign. Math. (2)*, 64(3-4) :459-476, 2018.
- [36] Dmitry KLEINBOCK et Keith MERRILL. Rational approximation on spheres. *Isr. J. Math.*, 209 :293-322, 2015.
- [37] Anthony W. KNAPP. *Lie groups beyond an introduction. 2nd ed.* Tome 140. Boston, MA : Birkhäuser, 2nd ed. Édition, 2002, pages xviii + 812.
- [38] Bertram KOSTANT. On convexity, the Weyl group and the Iwasawa decomposition. *Ann. Sci. Éc. Norm. Supér. (4)*, 6 :413-455, 1973.
- [39] Serge LANG. Report on Diophantine approximations. *Bull. Soc. Math. Fr.*, 93 :177-192, 1965.
- [40] R. P. LANGLANDS. On the classification of irreducible representations of real algebraic groups. In *Harmonic analysis of tempered distributions on semi-simple Lie groups of real rank one*, pages 101-170. 1989.
- [41] E. LE DONNE. *Lecture notes on sub-Riemannian geometry*. http://enrico.ledonne.googlepages.com/LeDonne_subRiemannian.pdf.
- [42] E. LINDENSTRAUSS, G. MARGULIS, A. MOHAMMADI et N. SHAH. Quantitative behavior of unipotent flows and an effective avoidance principle. *preprint arXiv :1904.00290v1*, 2019.
- [43] Kurt MAHLER. Über das Mass der Menge aller s -Zahlen. *Math. Ann.*, 106 :131-139, 1932.
- [44] G. A. MARGULIS. The action of unipotent groups in a lattice space. *Mat. Sb. (N.S.)*, 86(128) :552-556, 1971.
- [45] H. MINKOWSKI. *Geometrie der Zahlen*. In 2 Lieferungen. Lfg. 1. Leipzig : B. G. Teubner. 240 S. 8°. (1896). 1896.
- [46] Amir MOHAMMADI et Alireza Salehi GOLSEFIDY. Translate of horospheres and counting problems. *Am. J. Math.*, 136(5) :1301-1346, 2014.
- [47] D. MUMFORD. *Geometric invariant theory*. Tome 34. Springer-Verlag, Berlin, 1965.
- [48] Klaus F. ROTH. Rational approximations to algebraic numbers. *Proc. Int. Congr. Math.* 1958, 203-210 (1960). 1960.
- [49] Stephen Hoel SCHANUEL. Heights in number fields. *Bull. Soc. Math. Fr.*, 107 :433-449, 1979.
- [50] W. M. SCHMIDT. On badly approximable numbers and certain games. *Trans. Amer. Math. Soc.*, 123 :178-199, 1966.

- [51] W. M. SCHMIDT. On heights of algebraic subspaces and diophantine approximations. *Ann. Math. (2)*, 85 :430-472, 1967.
- [52] W. M. SCHMIDT. Simultaneous approximation to algebraic numbers by rationals. *Acta Math.*, 125 :189-201, 1970.
- [53] Wolfgang M. SCHMIDT. *Diophantine approximation*. Tome 785. Springer, Cham, 1980.
- [54] Jean-Pierre SERRE. *Algèbres de Lie semi-simples complexes*. W. A. Benjamin, inc., New York-Amsterdam, 1966, viii+130 pp. (not consecutively paged).
- [55] Igor R. SHAFAREVICH. *Basic algebraic geometry 1. Varieties in projective space. Translated from the Russian by Miles Reid. 3rd ed.* Berlin : Springer, 3rd ed. Édition, 2013, pages xviii + 310.
- [56] Nimish A. SHAH. Equidistribution of expanding translates of curves and Dirichlet's theorem on Diophantine approximation. *Invent. Math.*, 177(3) :509-532, 2009.
- [57] C. L. SIEGEL. Approximation algebraischer Zahlen. Jahrbuch d. philos. Fakultät Göttingen 1921, 291-296 (1921). 1921.
- [58] Carl Ludwig SIEGEL. *Lectures on the geometry of numbers. Notes by B. Friedman. Rewritten by Komaravolu Chandrasekharan with the assistance of Rudolf Suter.* Berlin etc. : Springer-Verlag, 1989, pages x + 160.
- [59] V. G. SPRINDZHUK. Achievements and problems in diophantine approximation theory. *Russ. Math. Surv.*, 35(4) :1-80, 1980.
- [60] Axel THUE. Über Annäherungswerte algebraischer Zahlen. *J. Reine Angew. Math.*, 135 :284-305, 1909.
- [61] Pengyu YANG. Equidistribution of expanding translates of curves and Diophantine approximation on matrices. *Invent. Math.*, 220(3) :909-948, 2020.