université
PARIS-SACLAY

Homogeneous dynamics and S-adic quadratic forms

Dynamique homogène et formes quadratiques S-adiques

Thèse de doctorat de l'université Paris-Saclay

École doctorale de mathématiques Hadamard (EDMH) no. 574
Spécialité de doctorat: Mathématiques fondamentales
Unité de recherche : Laboratoire de mathématiques d'Orsay, UMR 8628 CNRS
Référent : Faculté des sciences d'Orsay

Thèse présentée et soutenue à Paris-Saclay, le 21/06/2021, par

Irving CALDERÓN

Composition du Jury

Emmanuel ULLMO Directeur de l'IHES	Président
Alexander GORODNIK Professeur à l'Université de Zurich	Rapporteur & Examinateur
Georges TOMANOV Professeur à l'Université Claude Bernard Lyon 1	Rapporteur & Examinateur
Nicolas BERGERON Professeur à l'ENS Paris	Examinateur
François MAUCOURANT Maître de conférences à l'Université de Rennes 1	Examinateur

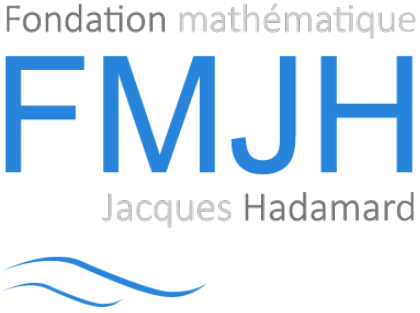
Direction de la thèse

Yves BENOIST Directeur de recherche au CNRS et l'Université Paris-Saclay	Directeur de thèse

Thèse de doctorat

NTT : 2021UPASM018


MATHEMATIQUES
ORSAY


Fondation mathématique
FMJH
Jacques Hadamard


FONDATION CFM
POUR LA RECHERCHE

Agradecimientos

Tout d'abord, je remercie mon directeur de thèse. Yves, merci pour tous ces après-midis dans ton bureau où tu m'as expliqué (souvent plus d'une fois) ce que je ne comprenais pas. Merci aussi d'avoir du mal à arrêter de parler, car grâce à cela j'ai appris sur une grande variété de sujets très intéressants. Mais au-delà de tous les théorèmes et preuves dont on a discuté, merci d'avoir partagé avec moi ta vision, ton enthousiasme et ta façon de faire des maths. C'est grâce à toi que je crois fermement qu'il vaut mieux connaître par coeur une preuve, et non pas cent énoncés, que les exemples sont presque plus importants que les théorèmes, et que le plus grand secret pour réussir dans les maths c'est le travail dur.

I warmly thank Alexander Gorodnik and Georges Tomanov for writing a report on my thesis, and for helping me to improve it with their valuable suggestions and remarks. Un grand merci aussi à Nicolas Bergeron, François Maucourant et Emmanuel Ullmo, je suis honoré d'avoir un jury aussi distingué.

En el plano personal, la primera persona a quien quiero agradecer es a Claudia, mi esposa. Gracias por depositar en mí tanta confianza al decidir emprender conmigo esta aventura lejos de casa, aún sabiendo que la incertidumbre era lo único seguro que nos esperaba. A pesar de que (en particular) en estos tres años mi mente se extraviaba frecuentemente, no perdiste la paciencia y siempre la guiaste de regreso a un lugar seguro con una gran sonrisa dibujada en tu rostro. Gracias por reconfortarme cuando mis ánimos andaban bajos, y por creer en mí, especialmente en los días en que me costaba hacerlo. Para mí, el cerrar hoy este ciclo marca uno de nuestros más grandes logros como equipo.

Esta estancia en Francia se la debo en gran medida a Ana y Pierre. Muchas gracias por motivarme a venir en primer lugar, por apoyar mis diversas candidaturas y por estar al pendiente de mí ya que estaba de este lado.

A mi hermano, Ayax: Gracias por escucharme siempre que lo necesito y por dejarme compartirte la poca experiencia que tengo. Me alegra que el mar que nos ha separado estos últimos cuatro años en realidad nos haya acercado más que nunca.

Gracias a mi mamá y a mi papá por su apoyo desde siempre. A pesar de que no entendían al inicio por qué quería estudiar matemáticas, eso no impidió que me alentaran y ayudaran de toda forma que estuviera en sus manos, y hasta de las que no lo estaban. Hoy sigo sin poder contestar completamente esas difíciles preguntas sobre mi futuro que me plantearon cuando empecé la carrera, pero espero que al tener en sus manos esta tesis se alegren de ver materializados el trabajo y los esfuerzos que he hecho en este camino al que difícilmente me hubiera lanzado sin sus palabras de aliento.

Ce n'est pas facile de s'habituer à un nouveau pays, surtout quand on s'y installe sans parler la langue. Cyril, merci d'avoir eu la patience de me parler super lentement quand je

suis arrivé en France, et pour le tas de mots et d'expressions que tu m'as apprises. Gabriel, merci de me faire sentir le bienvenue au LMO, me laissant travailler en el caos de ton bureau que j'ai fini par m'appropier, et de nous parler à Claudia et moi du SPF. Louise, merci d'avoir continué à m'inviter aux pauses thé, picnics et d'autres événements variés que tu organisais malgré ma très sporadique participation. C'était un plaisir d'apprendre et surtout de sécher avec Pierre-Louis, Timothée, Gabriel, Claudio, Oussama, Corentin, Juan, Frank, Antonio, Balthazar et tous les autres participants du groupe de travail hebdomadaire de Topologie et Dynamique d'Orsay.

Finalement, je remercie à la *Fondation CFM pour la recherche* de m'avoir permis de travailler dans ce projet dans des conditions excellentes grâce au généreux financement de ma bourse Jean-Pierre Aguilar.

21 de junio de 2021

Contents

Chapter 1

Introduction

Ma thèse a pour thème les formes quadratiques entières. Même si celles-ci ont été étudiées pendant plusieurs décennies, elles sont toujours au cœur de divers sujets de recherche actuels. Ma contribution consiste en deux nouveaux résultats. Le premier porte sur le problème de déterminer si deux formes quadratiques données sont équivalentes, et le deuxième donne des parties génératrices finies des groupes orthogonaux S-entiers. Une caractéristique importante de ces théorèmes est qu'ils sont effectifs, c'est-à-dire quantitatifs, et complètement explicites. Ces résultats, ainsi que les méthodes utilisées pour les prouver sont inspirés de l'article [LM16] de Li et Margulis.

Cette introduction est divisée en quatre sections. Dans les deux premières on parle de l'histoire des deux problèmes abordés, on présente les résultats originaux de Li et Margulis ainsi que les généralisations que j'ai obtenues. Après avoir beaucoup travaillé sur ce sujet, je me suis retrouvé avec moins de réponses que de questions. Certaines de ses questions sont rassemblées dans la troisième partie. La structure de la thèse est esquissée dans la quatrième section.

1.1 Équivalence de formes quadratiques

1.1.1 Classification des formes quadratiques entières

Pour motiver le premier problème qu'on traite, on va discuter maintenant de quelques concepts qui ont été développés pour tenter de classifier les formes quadratiques entières. On dit que les formes quadratiques Q_1 et Q_2 en d variables à coefficients dans un anneau commutatif $\mathcal{R}$ avec unité sont $\mathcal{R}$-équivalentes s'il existe $g \in GL(d, \mathcal{R})$ tel que $Q_1 \circ g = Q_2$. À ce jour, personne n'a réussi à classifier à $\mathbb{Z}$-équivalence près les formes quadratiques entières. L'histoire de ce problème est longue, donc on se limitera à évoquer de quelques développements clés.

Le cas des formes quadratiques binaires a été résolu par C.F. Gauss dans les *Disquisitiones Arithmeticae* [Gau65], où il décrit un algorithme qui, en partant d'une telle forme Q donne une suite de formes quadratiques binaires $\mathbb{Z}$-équivalentes à Q qui devient périodique. Le *cycle* de Q est la période de sa suite. Gauss montre que Q_1 et Q_2 sont $\mathbb{Z}$-équivalentes si et seulement si elles ont le même cycle – c.f. [CS99, Theorem 1, p. 356]. De plus, il caractérise les formes quadratiques qui peuvent apparaître dans un cycle en termes d'inégalités simples entre leurs coefficients, ce qui amène au concept de forme quadratique binaire réduite. Concrètement,

la forme quadratique entière $ax_1^2 + 2bx_1x_2 + cx_2^2$ est réduite -c.f. [CS99, p. 358-359] - si elle est définie positive ou négative et vérifie $|2b| < |a| < |c|$, ou bien si elle est indéfinie et

$$0 < b < \sqrt{b^2 - ac} < \min\{b + |a|, b + |c|\}.$$

Inspirés par ces travaux de Gauss, C. Hermite puis H. Minkowski étendent la notion de forme quadratique réduite à trois variables ou plus. Les propriétés souhaitées sont : toute forme quadratique entière doit être $\mathbb{Z}$-équivalente à une forme réduite et il doit y avoir une méthode aussi simple que possible pour déterminer si deux formes réduites sont $\mathbb{Z}$-équivalentes. C'est ainsi que la *Théorie de la réduction des formes quadratiques* est née. Voici son principal théorème de finitude. Dans l'énoncé on note δ_R le déterminant de la matrice d'une forme quadratique entière R en d variables dans la base canonique de $\mathbb{Z}^d$.

Théorème 1.1.1. *Soient d et N des entiers positifs. Il n'y a qu'un nombre fini de formes quadratiques entières réduites R en d variables avec $|\delta_R| = N$.*

La théorie de la réduction de formes quadratiques joue un rôle important dans cette thèse. On utilise la définition moderne de forme réduite en termes des sous-ensembles de Siegel de $GL(d, \mathbb{R})$.

Malgré les développements de la théorie de la réduction, la classification à $\mathbb{Z}$-équivalence près des formes quadratiques entières restait - et reste encore - inaccessible, donc les gens travaillant sur le sujet ont introduit d'autres notions d'équivalence, en espérant que celles-ci nous approchent de la $\mathbb{Z}$-classification. On va discuter brièvement deux telles équivalences.

La première est le *genre* : deux formes quadratiques entières sont du même genre si elles sont équivalentes sur $\mathbb{R}$ et sur $\mathbb{Z}_p$ pour tout nombre premier p[1]. Évidemment deux formes quadratiques $\mathbb{Z}$-équivalentes sont du même genre, mais la réciproque est fausse. Par exemple,

$$Q_1(x) = x_1^2 + 82x_2^2 \quad \text{et} \quad Q_2(x) = 2x_1^2 + 41x_2^2$$

ne sont pas $\mathbb{Z}$-équivalentes car $x_1^2 + 82x_2^2 = 2$ n'a pas de solution entière, mais Q_1 et Q_2 sont du même genre – c.f. [Cas78, p. 129]. Tout de même, le lien entre $\mathbb{Z}$-équivalence et genre est fort. Si Q_1 et Q_2 sont du même genre, alors elles sont presque $\mathbb{Z}$-équivalentes au sens suivante : elles sont $\mathbb{Z}^{(S)}$-équivalentes pour toute partie finie S de nombres premiers. Ici, $\mathbb{Z}^{(S)}$ est l'anneau des nombres rationnels dont le dénominateur n'est divisible par aucun $p \in S$. En fait, cette condition est une caractérisation alternative de *être du même genre* – c.f [Cas78, Theorem 1.4, p. 130].

Le *genre spinoriel* est une autre équivalence de formes quadratiques entières introduite par M. Eichler, plus fine que le genre et (parfois) plus grossière que la $\mathbb{Z}$-équivalence. Pour ne pas couper le fil de la discussion on ne donne pas ici la définition - voir [Cas78, Lemma 1.4, p. 201]. Grâce à elle on peut trouver le nombre de $\mathbb{Z}$-classes de formes quadratiques entières $\mathbb{R}$-isotropes en $d \geq 3$ variables. En effet, on sait que pour celles-ci, être du même genre spinoriel et être $\mathbb{Z}$-équivalentes revient au même - c.f. [Cas78, Theorem 1.3, p. 202]. De plus, J.H. Conway et N.A. Sloane décrivent dans [CS99, Chapter 15, Section 9, p. 388] une méthode

[1]Cette définition est sans doute motivée par le principe local-global pour des formes quadratiques rationnelles : deux telles formes sont $\mathbb{Q}$-équivalentes si et seulement si elles sont équivalentes sur $\mathbb{R}$ et sur $\mathbb{Q}_p$ pour tout p.

pratique pour calculer le nombre de genres spinoriels. Quant aux formes quadratiques $\mathbb{R}$-anisotropes, même s'il y a de bonnes méthodes pour les classer quand d est petit, Conway et Sloane - c.f. [CS99, p. 353] - pensent qu'on n'arrivera jamais à une classification générale car il y en a trop dès que $d > 24$.

1.1.2 Critère de $\mathbb{Z}$-équivalence

Après notre discussion de quelques outils pour classifier les formes quadratiques entières, on présente maintenant le problème proche, mais bien moins ambitieux, qu'on va aborder : Décider si deux formes quadratiques entières données Q_1 et Q_2 en d variables sont $\mathbb{Z}$-équivalentes. Voici une situation où ce *problème de $\mathbb{Z}$-équivalence* a une réponse facile, qui en plus motive notre approche du cas général. Si Q_1 et Q_2 sont toutes les deux définies positives ou négatives – c'est-à-dire $\mathbb{R}$-anisotropes –, l'ensemble des matrices g dans $GL(d, \mathbb{R})$ pour passer de Q_1 à Q_2 est compact, et on peut montrer facilement que pour toute telle g,

$$||g||_\infty \leq d \cdot d! ||Q_1||_\infty^{\frac{d-1}{2}} ||Q_2||_\infty^{\frac{1}{2}}, \tag{1.1}$$

où $||Q_i||_\infty$ est le maximum des valeurs absolues des coefficients de Q_i. Donc Q_1 et Q_2 sont $\mathbb{Z}$-équivalentes si et seulement si $Q_1 \circ \gamma = Q_2$ a une solution γ dans la partie **finie** de $GL(d, \mathbb{Z})$ déterminée par (1.1). Cette stratégie ne marche pas quand les Q_i sont $\mathbb{R}$-isotropes, car l'ensemble de matrices dans $GL(d, \mathbb{R})$ qui transforment Q_1 en Q_2 est non-borné. Il est étonnant que même dans ce cas on peut déterminer quand même si les Q_i sont $\mathbb{Z}$-équivalentes en cherchant γ tel que $Q_1 \circ \gamma = Q_2$ dans une partie finie de $GL(d, \mathbb{Z})$. Il s'agit d'un résultat de Siegel dans [Sie72].

Théorème 1.1.2. *Pour tout entier $d \geq 2$ il y a une fonction explicite M_d avec la propriété suivante : si les formes quadratiques entières Q_1 et Q_2 en d variables sont $\mathbb{Z}$-équivalentes, alors il y a $\gamma \in GL(d, \mathbb{Z})$ telle que*

$$||\gamma||_\infty \leq M_d(Q_1, Q_2)$$

et $Q_1 \circ \gamma = Q_2$.

Une fonction M_d comme dans le théorème précédant s'appelle *borne de $\mathbb{Z}$-équivalence*. Siegel établit l'existence de bornes de $\mathbb{Z}$-équivalence à l'aide de la théorie de la réduction de Hermite et Minkowski. Outre l'article original [Sie72] (écrit en allemand), on peut trouver un esquisse de la preuve du Théorème 1.1.2 dans le livre de Cassels [Cas78, Chapter 13, Section 12, p. 324]. Siegel ne donne pas M_d de façon explicite, mais S. Straumann montre dans son mémoire de master [Str99] que la méthode de Siegel donne

$$M_d(Q_1, Q_2) = \exp(A_d |\delta_{Q_1}|^{\frac{d^3+d^2}{2}}) \cdot \max\{||Q_1||_\infty, ||Q_2||_\infty\}^{\frac{d^3-d^2}{2}},$$

où δ_{Q_1} est comme dans le Théorème 1.1.1 et A_d est une constante qui ne dépend que de d [2].

Si l'on veut utiliser en pratique des bornes de $\mathbb{Z}$-équivalence, il faut trouver une M_d explicite qui ne croît pas trop vite. Le travail de Straumann montré qu'on peut prendre M_d

[2] Dans la suite on note $A_d, B_d, C_d, \ldots$ des constantes qui dépendent seulement de d.

exponentielle en $||Q_1||_\infty, ||Q_2||_\infty$. Dorénavant, on dira simplement que M_d est exponentielle ou polynomiale si elle a la propriété respective par rapport à $||Q_1||_\infty, ||Q_2||_\infty$.

On va discuter maintenant des contributions majeures à ce sujet en ordre chronologique. Pour les formes quadratiques binaires : on sait que M_2 ne peut pas être polynomiale car dans ce cas il y aurait une borne polynomiale de la norme de la plus petite solution d'une équation type Pell

$$au^2 - bv^2 = \pm 1, \tag{1.2}$$

avec $a, b \in \mathbb{Z}$. En effet, si $(u_0, v_0) \in \mathbb{Z}^2$ est solution de (1.2), alors

$$\gamma = \begin{pmatrix} u_0 & bv_0 \\ v_0 & au_0 \end{pmatrix} \in GL(2, \mathbb{Z})$$

transforme $Q_1(x) = ax_1^2 - bx_2^2$ en $Q_2(x) = \pm x_1^2 \mp abx_2^2$. Soit $\gamma_0 \in GL(2, \mathbb{Z})$ telle que $Q_1 \circ \gamma_0 = Q_2$ et $||\gamma_0||_\infty \leq M_2(Q_1, Q_2)$. La première colonne de γ_0 est une solution de 1.2 dont la taille est bornée par un polynôme en a et b. Le lecteur peut trouver dans l'article de J. Lagarias [Lag80, p. 486] une suite d'équations type Pell pour laquelle la plus petite solution croît plus vite que n'importe quel polynôme en a et b.

Pour les formes quadratiques en 3 variables il y a des bornes de $\mathbb{Z}$-équivalence polynomiales. R. Dietmann montre dans [Die03] qu'on peut prendre

$$M_3(Q_1, Q_2) = B_3||Q_1||_\infty^{510}(||Q_1||_\infty + ||Q_2||_\infty)^{207}.$$

Étant donné ce résultat, D. Masser conjecture dans [Mas02] qu'il y a des bornes de $\mathbb{Z}$-équivalence polynomiales dès que $d \geq 3$.

Conjecture 1.1.3. *Pour tout entier $d \geq 3$ il y a des constantes C_d, E_d avec la propriété suivante : si les formes quadratiques entières non-dégénérées Q_1 et Q_2 en d variables sont $\mathbb{Z}$-équivalentes, alors il y a $\gamma_0 \in GL(d, \mathbb{Z})$ telle que*

$$||\gamma_0||_\infty \leq C_d(||Q_1||_\infty + ||Q_2||_\infty)^{E_d}$$

et $Q_1 \circ \gamma_0 = Q_2$.

La prochaine grande contribution à cette histoire est due aussi a Dietmann, qui démontre dans [Die07, Theorem 3] la conjecture de Masser quitte à ajouter des hypothèses suplémentaires sur Q_1 et Q_2[3] qui lui permettent de trouver M_d en utilisant ses résultats pour les formes quadratiques ternaires. Pour $d \geq 6$ il obtient

$$M_d(Q_1, Q_2) = C_d \max\{||Q_1||_\infty, ||Q_2||_\infty\}^{E_d},$$

où E_d est un polynôme en d de terme principal $5^d d^{d+1}$. Cette borne de $\mathbb{Z}$-équivalence est améliorée par Li et Margulis dans [LM16, Theorem 1], où ils établissent la conjecture de Masser en toute généralité. Voici une version simplifiée de son énoncé.

Théorème 1.1.4. *Soient Q_1 et Q_2 des formes quadratiques entières non-dégénérées en $d \geq 3$ variables. Si Q_1 et Q_2 sont $\mathbb{Z}$-équivalentes, il y a $\gamma_0 \in GL(d, \mathbb{Z})$ telle que*

$$||\gamma_0||_\infty \leq C_d(||Q_1||_\infty ||Q_2||_\infty)^{\frac{13}{40}d^3}$$

et $Q_1 \circ \gamma_0 = Q_2$.

[3] Les coefficients de la diagonale principale de b_{Q_i} - la matrice de Q_i dans la base canonique de $\mathbb{Q}^d$ - ne sont pas tous pairs et $\det b_{Q_i}$ est sans facteurs cubiques et non divisible par 4.

1.1.3 La méthode de Li et Margulis

Les stratégies de Dietmann et de Li-Margulis pour traiter le problème de $\mathbb{Z}$-équivalence sont très différentes. D'un côté, Dietmann a une approche plutôt Théorie Analytique des Nombres, basé notamment sur la méthode du cercle de Hardy et Littlewood. Ceci est tout à fait naturel, vu qu'il s'est intéressé aux bornes de $\mathbb{Z}$-équivalence en raison de leur lien avec les bornes de résolubilité de l'équation diophantienne quadratique générale. En fait, ceci est le sujet principal de l'article [Mas02] où Masser énonce sa conjecture [Mas02].

Pour l'approche de Li et Margulis, il faut d'abord regarder le problème autrement, en profitant d'une dualité simple et très utile. Pour fixer les idées on va supposer que Q_1 et Q_2 sont de signature 2,1. Soit $P(x) = x_1^2 + x_2^2 - x_3^2$; on considère les groupes $G = GL(3, \mathbb{R}), H = O(P, \mathbb{R})$ et $\Gamma = GL(3, \mathbb{Z})$. On écrit $Q_i = P \circ g_i$ avec $g_i \in G$. Toute forme quadratique de signature 2,1 s'exprime comme $P \circ g$ avec $g \in G$, donc l'espace de toutes ces formes s'identifie à $H\backslash G$. Voici l'observation clé : une $\mathbb{Z}$-classe d'équivalence de formes quadratiques entières (de signature 2,1) est une Γ-orbite dans $H\backslash G$, qui correspond à une H-orbite dans l'espace $X = G/\Gamma$ des réseaux de $\mathbb{R}^3$ [4]. Trouver $\gamma_0 \in \Gamma$ qui transforme Q_1 en Q_2 équivaut à trouver $h_0 \in H$ qui envoie $g_2\mathbb{Z}^3$ sur $g_1\mathbb{Z}^3$. Il s'avère que la H-orbite Y de $g_2\mathbb{Z}^3$ est fermée et qu'elle admet une mesure H-invariante finie, ce qui permet à Li et Margulis de traiter le problème avec de puissants outils de dynamique homogène effective. L'action de H sur Y est presque mélangeante, et mieux encore, il y a une vitesse de mélange effective et uniforme, qui ne dépend pas de la H-orbite fermée, grâce à laquelle ils bornent la norme d'une matrice $h_0 \in H$ telle que $h_0 g_2 \mathbb{Z}^3 = g_1 \mathbb{Z}^3$ en fonction de $||g_1||_\infty, ||g_2||_\infty$ et du volume de Y.

Pour finir la discussion du Théorème 1.1.4 on va signaler les deux outils techniques principales de la preuve. Premièrement, la récurrence effective des flots unipotents – un résultat de Kleinbock et Margulis [KM98] – qui donne une estimation du volume de la H-orbite Y évoqué ci-dessus. Deuxièmement, la borne de Kim et Sarnak [Kim03, Appendix 2] pour la conjecture de Ramanujan-Petersson pour $\mathbf{SL}(2)$ sur $\mathbb{Q}$, un important résultat de la théorie des représentations automorphes, qui prescrit la vitesse de mélange uniforme pour l'action de H dans des H-orbites fermées dans X.

1.1.4 Critère de $\mathbb{Z}_S$-équivalence

Le premier objectif de ma thèse est d'obtenir un analogue du Théorème 1.1.4 pour le *problème de $\mathbb{Z}_S$-équivalence*. Pour l'énoncer on a besoin des nouvelles définitions. Si $S_f = \{p_1, \ldots, p_k\}$ est un ensemble fini de nombres premiers, on pose $S = S_f \cup \{\infty\}$. L'anneau des S-entiers $\mathbb{Z}_S$ est formé des nombres rationnels dont le dénominateur est un produit de puissances d'éléments de S_f. On note p_S le produit des nombres premiers dans S_f. Pour $S = \{\infty\}$ on pose $\mathbb{Z}_S = \mathbb{Z}$ et $p_S = 1$. Étant données des formes quadratiques entières Q_1 et Q_2 en d variables, cette fois-ci on veut déterminer si elles sont $\mathbb{Z}_S$-équivalentes en cherchant une solution γ de $Q_1 \circ \gamma = Q_2$ dans une partie finie de $GL(d, \mathbb{Z}_S)$. D'après le Théorème 1.1.4, pour $S = \{\infty\}$ une telle partie est définie par une inégalité de la forme $||\gamma||_\infty \leq M$. Elle est finie car tout coefficient d'une solution $\gamma \in GL(d, \mathbb{Z})$ est un entier dont la valeur absolue est au plus M. Mais $|x| \leq M$ a une infinité de solutions dans $\mathbb{Z}_S$ dès que S_f est non-vide,

[4] D'autres auteurs ont exploité la dualité entre Γ-orbites de formes quadratiques et H-orbites de réseaux de $\mathbb{R}^d$. Par exemple, Eichler l'utilise pour définir le genre spinoriel.

donc l'inegalité $||\gamma||_\infty \leq M$ ne suffit pas. On contourne cette petite difficulté comme suit : rappelons que chaque $t \in \mathbb{Z}_S$ s'écrit

$$t = \frac{n}{p_1^{a_1} \cdots p_k^{a_k}},$$

avec $n \in \mathbb{Z}$ et $a_1, \ldots, a_k \in \mathbb{N}$. Si on impose des bornes supérieures pour $|t|$ ainsi que pour chaque a_i, il n'y a qu'un nombre fini de solutions dans $\mathbb{Z}_S$ du système résultant. Pour $\gamma \in M_d(\mathbb{Q})$, soient $||\gamma||_p$ le maximum des valeurs absolues p-adiques des coefficients de γ et

$$||\gamma||_S = \max_{\nu \in S} ||\gamma||_\nu.$$

Alors $||\gamma||_S \leq M$ définit une partie finie de $GL(d, \mathbb{Z}_S)$. Voici la généralisation du Théorème 1.1.4 que j'ai obtenue.

Théorème 1.1.5. *Soient Q_1 et Q_2 des formes quadratiques entières non-dégénérées en $d \geq 3$ variables et soit S_f un ensemble fini de nombres premiers impairs. Si Q_1 et Q_2 sont $\mathbb{Z}_S$-équivalentes, alors il y a $\gamma_0 \in GL(d, \mathbb{Z}_S)$ telle que*

$$||\gamma_0||_S \leq F_d p_S^{19d^6} (||Q_1||_\infty ||Q_2||_\infty)^{2d^3}$$

et $Q_1 \circ \gamma_0 = Q_2$.

On peut se passer de l'hypothèse $2 \notin S$. En fait, la même preuve fonctionne, mais il y a des endroits avec plus de cas à considérer[5]. Dans le Théorème 1.1.4, où $S = \{\infty\}$, le cas facile est quand les Q_i sont $\mathbb{R}$-anisotropes – c.f. (1.1). Pour S géneral, le cas facile est quand les Q_i sont $\mathbb{Q}_\nu$-anisotropes[6] pour chaque $\nu \in S$, car tout $g \in GL(d, \mathbb{Q})$ pour passer de Q_1 à Q_2 vérifie

$$||g||_S \leq d \cdot d! ||Q_1||_\infty^{\frac{d-1}{2}} ||Q_2||_\infty^{\frac{1}{2}}.$$

Le cas intéressant - quand Q_1 et Q_2 sont $\mathbb{Q}_\nu$-isotropes pour au moins un $\nu \in S$ - est traité par le Théorème 5.1.1 et le Théorème 5.1.2 quand les Q_i sont respectivement $\mathbb{R}$-isotropes et $\mathbb{R}$-anisotropes.

Li et Margulis traitent le cas $S = \{\infty\}$ en étudiant l'action d'un groupe orthogonal réel H sur l'espace X des réseaux de $\mathbb{R}^d$. On adapte leur stratégie comme suit : supposons que Q_1 et Q_2 sont $\mathbb{Z}_S$-équivalentes. On veut contrôler $||\gamma_0||_\nu, \nu \in S$ d'une $\gamma_0 \in GL(d, \mathbb{Z}_S)$ qui transforme Q_1 en Q_2. Il est donc naturel de considérer les Q_i comme forme quadratique sur chaque $\mathbb{Q}_\nu, \nu \in S$. Soit P_ν le représentant *standard* de la $\mathbb{Q}_\nu$-classe d'équivalence des Q_i. Pour faire d'une pierre deux coups on considère Q_1 et Q_2 sur $\mathbb{Q}_S = \prod_{\nu \in S} \mathbb{Q}_\nu$ grâce au plongement diagonal $\mathbb{Q} \to \mathbb{Q}_S$, donc les Q_i sont $\mathbb{Q}_S$-équivalentes à $P = (P_\nu)_{\nu \in S}$. On considère les groupes

$$G_S = GL(d, \mathbb{Q}_S) = \prod_{\nu \in S} GL(d, \mathbb{Q}_\nu), \qquad H_S = O(P, \mathbb{Q}_S) = \prod_{\nu \in S} O(P_\nu, \mathbb{Q}_\nu),$$

[5] La différence entre 2 et $p > 2$ vient du fait que $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2$ est d'ordre 8, tandis que $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ est d'ordre 4. Ceci entraîne qu'il y a plus de classes d'équivalence de formes quadratiques sur $\mathbb{Q}_2$ que sur $\mathbb{Q}_p$.

[6] Par convention $\mathbb{Q}_\infty = \mathbb{R}$.

et on prend $g_1, g_2 \in G_S$ telles que $Q_i = P \circ g_i$. Quel espace joue ici le rôle de X ? On remarque que la copie diagonale de $\mathbb{Z}_S$ dans $\mathbb{Q}_S$ est un réseau dans $\mathbb{Q}_S$, donc $\mathbb{Z}_S^d$ est un réseau dans $\mathbb{Q}_S^d$. L'action de G_S sur l'espace X_S des réseaux de $\mathbb{Q}_S^d$ est transitive et le stabilisateur de $\mathbb{Z}_S^d$ est le plongement diagonal Γ_S de $GL(d, \mathbb{Z}_S)$ dans G_S, donc X_S s'identifie à G_S/Γ_S. Trouver une $\gamma_0 \in GL(d, \mathbb{Z}_S)$ qui transforme Q_1 en Q_2 équivaut à trouver $h_0 \in H_S$ qui envoie $g_2\mathbb{Z}_S^d$ sur $g_1\mathbb{Z}_S^d$. Heureusement, le cadre dynamique est aussi bon que dans le cas $S = \{\infty\}$: l'orbite $Y = H_S g_2 \mathbb{Z}_S^d$ est fermée dans X_S, de volume H_S-invariant fini et l'action de H_S sur Y est presque mélangeante. On peut donc traiter le problème avec des outils de dynamique homogène. On donnera la borne de $||h_0||_S$ en fonction des $||g_i||_S$ et du volume de Y - c.f Proposition 5.2.2 et Proposition 5.2.3.

Les deux ingrédients techniques principaux de la preuve du Théorème 1.1.5 ressemblent à ceux utilisés par Li et Margulis pour $S = \{\infty\}$. Pour estimer le volume de Y on applique une version S-adique, due à Kleinbock et Tomanov [KT07], de la récurrence effective des flots unipotents. Quant à la vitesse effective et uniforme de mélange pour l'action de H_S sur des H_S-orbites fermées dans X_S, elle est aussi déduite de la borne de Kim-Sarnak [Kim03, Appendix 2] pour la conjecture de Ramanujan-Petersson pour $\mathbf{SL}(2)$ sur $\mathbb{Q}$ quand les Q_i sont $\mathbb{R}$-isotropes, et quand elles sont $\mathbb{R}$-anisotropes, d'une reformulation dans le langage de la théorie de représentations [Lub94, Theorem 2.14, p. 158] d'un célèbre théorème de Deligne [Lub94, Theorem 1.2, p. 148] sur les formes modulaires, et de la correspondance de Jacquet-Langlands [Lub94, Theorem 3.4, p. 163].

1.2 Le groupe des unités d'une forme quadratique

1.2.1 Les résultats classiques de Siegel

Il est probable que la motivation de beaucoup de celles et ceux qui ont étudié les formes quadratiques entières vienne des liens de celles-ci avec la théorie des nombres. Par exemple, pour comprendre les corps de nombres quadratiques $K = \mathbb{Q}[\sqrt{D}]$ il faut étudier les formes quadratiques $Q(x) = x_1^2 - Dx_2^2$. Le groupe des unités $\mathcal{O}_K^\times$ de l'anneau d'entiers de K est fortement lié au groupe orthogonal entier $O(Q, \mathbb{Z})$, c'est pour cela qu'on appelle parfois $O(Q, \mathbb{Z})$ le groupe des unités de Q. Dans l'article clé [Sie39] de 1939, Siegel étudie le groupe des unités des formes quadratiques en $d \geq 3$ variables. Deux de ses résultats sont extrêmement importants pour cette thèse. Le premier est [Sie39, Satz 11, p. 230].

Théorème 1.2.1. *Pour toute forme quadratique entière non-dégénérée Q en $d \geq 3$ variables, le groupe $O(Q, \mathbb{Z})$ est de type fini.*

Li et Margulis ont démontré dans [LM16] une version effective du Théorème 1.2.1, qu'on généralise au groupe des S-unités $O(Q, \mathbb{Z}_S)$ de Q, pour tout S. On va présenter ces résultats dans la sous-section suivante. Le deuxième théorème de Siegel qui nous concerne est [Sie39, Satz 12, p. 233].

Théorème 1.2.2. *Soit Q une forme quadratique entière non-dégénérée en $d \geq 3$ variables. Le groupe $O(Q, \mathbb{Z})$ des unités de Q est un réseau dans $O(Q, \mathbb{R})$.*

Le rôle du Théorème 1.2.2 dans ma thèse est le suivant : Soit $H \curvearrowright X$ le système dynamique utilisé par Li et Margulis pour le problème de $\mathbb{Z}$-équivalence. Le fait crucial que

les H-orbites fermées dans X sont de volume H-invariant fini vient[7] du Théorème 1.2.2. Plus généralement, la copie diagonale de $O(Q,\mathbb{Z}_S)$ dans $O(Q,\mathbb{Q}_S)$ est un réseau dans $O(Q,\mathbb{Q}_S)$, ce qui implique que les H_S-orbites fermées dans X_S sont de volume H_S-invariant fini.

Les preuves des théorèmes 1.2.1 et 1.2.2 se basent sur la théorie de la réduction de Hermite et Minkowski, qui a été affinée par Siegel lui même. A. Borel et Harish-Chandra ont poussé ces idées plus encore dans son papier [BH62] de 1962 où, inspirés par les exemples classiques $SL(d,\mathbb{Z}) \subset SL(d,\mathbb{R})$ et $O(Q,\mathbb{Z}) \subset O(Q,\mathbb{R})$ de réseaux dans groupes de Lie réels semisimples, ils introduisent la notion de sous-groupe arithmétique d'un groupe algébrique linéaire $\mathbf{G}$ défini sur $\mathbb{Q}$. Par analogie avec les formes quadratiques, ils développent une théorie de la réduction par rapport à un sous-groupe arithmétique, grâce à laquelle ils généralisent le Théorème 1.2.1 – tout sous-groupe arithmétique est de type fini – ainsi que le Théorème 1.2.2 en explicitant la condition sur $\mathbf{G}$ qui garantit que le volume de $\mathbf{G}_\mathbb{R}/\mathbf{G}_\mathbb{Z}$ est fini. Ils démontrent aussi – presque au même temps que G.D. Mostow et T. Tamagawa [MT62] – la *conjecture de Godement*, qui donne une condition nécessaire et suffisante sur $\mathbf{G}$ pour que $\mathbf{G}_\mathbb{R}/\mathbf{G}_\mathbb{Z}$ soit compact. Peu après, Borel étend ces résultats aux groupes S-arithmétiques dans [Bor63].

1.2.2 Petits générateurs des groupes orthogonaux S-entiers

Dans le papier [LM16], Li et Margulis déduisent du Théorème 1.1.4 plusieurs résultats intéressants sur les formes quadratiques entières. L'un d'entre eux, que je trouve particulièrement joli est une version effective [LM16, Theorem 2] du fait que $O(Q,\mathbb{Z})$ est de type fini.

Théorème 1.2.3. *Soit Q une forme quadratique entière non-dégénérée en $d \geq 3$ variables. Le groupe $O(Q,\mathbb{Z})$ est engendré par la famille de ses éléments γ tels que*

$$||\gamma||_\infty \leq J_d ||Q||_\infty^{d^7+3d^4}.$$

La preuve repose sur le Théorème 1.1.4 ainsi que des améliorations effectives de résultats classiques de la théorie de la réduction de formes quadratiques entières.

J'obtiens par analogie une version effective du fait que $O(Q,\mathbb{Z}_S)$ est de type fini, pour tout partie finie S_f de nombres premiers. Pour ce faire j'utilise la théorie de la réduction effective des formes quadratiques sur $\mathbb{Q}_S$ et le Théorème 1.1.5.

Théorème 1.2.4. *Soit Q une forme quadratique entière non-dégénérée en $d \geq 3$ variables. Pour toute partie finie S_f de nombres premiers, le groupe $O(Q,\mathbb{Z}_S)$ est engendré par ses éléments γ dont*

$$||\gamma||_S \leq L_d p_S^{20d^7} ||Q||_\infty^{4d^6}.$$

1.3 Quelques problèmes ouverts

Comme on a vu, le problème qui motive cette thèse est celui de déterminer si deux formes quadratiques entières en d variables données Q_1 et Q_2 sont $\mathbb{Z}$-équivalentes. On peut le reformuler de façon plus géométrique comme suit : les espaces quadratiques $(\mathbb{Z}^d, Q_1)$ et

[7] Car les H-orbites fermées sont obtenues à partir de formes quadratiques entières – c.f. Lemme 6.1.2

$(\mathbb{Z}^d, Q_2)$ sont-ils isométriques ? Mais que fait-on si Q_1 est en d_1 variables et Q_2 en $d_2 < d_1$? Décider si Q_1 représente Q_2 - c'est-à-dire qu'il y a un plongement isométrique $(\mathbb{Z}^{d_2}, Q_2) \hookrightarrow (\mathbb{Z}^{d_1}, Q_1)$ - est aussi intéressant. Li et Margulis donnent une borne [LM16, Theorem 4] pour ce *problème de $\mathbb{Z}$-représentation* de formes quadratiques, encore une autre application de leur Théorème 1.1.4. Par manque de temps je n'ai pas mis dans la thèse la généralisation S-adique naturelle.

On sait que les groupes $O(Q, \mathbb{Z}_S)$ sont de présentation finie - c.f. [PR94, Théorème 5.11, p. 272] -, et maintenant qu'on a des parties génératrices finies $\mathscr{G}_S^Q$ de ces groupes grâce aux théorèmes 1.2.3 et 1.2.4, il serait souhaitable de donner explicitement des relations sur $\mathscr{G}_S^Q$ définissant $O(Q, \mathbb{Z}_S)$.

Le programme de rendre effectifs des résultats classiques sur les groupes orthogonaux S-entiers peut aussi s'étendre aux sous-groupes S-arithmétiques d'autres $\mathbb{Q}$-groupes classiques, tels que les groupes unitaires. Quelques auteurs ont déjà exploré cette voie. Par exemple, T. Chinburg et M. Stover trouvent dans le papier récent [CS14] des petits générateurs du groupe de S-unités de $\mathbb{Q}$-algèbres centrales simples. Voir aussi - même si ses résultats ne sont pas effectifs – l'approche algorithmique au sujet proposé par F. Grunewald et D. Segal dans [GS80] pour les groupes arithmétiques et dans [GS85] pour les groupes S-arithmétiques.

1.4 Structure de la thèse

La première partie est formée de deux chapitres préliminaires. Au Chapitre 3 on rappelle la classification des formes quadratiques à coefficients dans $\mathbb{R}$ et $\mathbb{Q}_p$, et on fixe un représentant de chaque classe d'équivalence, qu'on appellera *forme quadratique standard*. Ceci est un concept important auquel on fera référence dans tous les chapitres. Puis, on révise la théorie de représentations unitaires de $SL(2, \mathbb{Q}_\nu)$ au Chapitre 4. Ici, le résultat important est la décroissance effective des coefficients des représentations unitaires presque L^k, qui plus loin nous permet d'établir la vitesse de mélange effective pour le système dynamique sous-jacent au problème de $\mathbb{Z}_S$-équivalence.

La deuxième partie est dédiée à la preuve de la borne pour le problème de $\mathbb{Z}_S$-équivalence, qui s'étale du Chapitre 5 au Chapitre 8. Au Chapitre 5 on traduit le problème arithmétique de $\mathbb{Z}_S$-équivalence à un problème dynamique sur l'action d'un groupe orthogonal S-adique H_S sur l'espace X_S des réseaux de $\mathbb{Q}_S^d$: étant donnés des points y_2, y_1 dans une H_S-orbite fermée Y dans X_S, on borne la S-norme $||h_0||_S$ de la plus petite $h_0 \in H_S$ qui envoie y_2 sur y_1. Ceci est accompli dans la Proposition 5.2.2 au Chapitre 6 quand H_∞ est non-compact, et dans la Proposition 5.2.3 au Chapitre 7 quand H_∞ est compact. La borne pour $||h_0||_S$ fait intervenir le volume de Y, c'est pourquoi on donne au Chapitre 8 une borne supérieure de ce volume en fonction du déterminant de Q quand l'orbite Y vient d'une forme quadratique entière Q.

Ayant établi notre borne de $\mathbb{Z}_S$-équivalence, on en déduit au Chapitre 9 le Théorème 1.2.4 sur la partie génératrice explicite de $O(Q, \mathbb{Z}_S)$. On traite le cas des formes quadratiques $\mathbb{R}$-isotropes et $\mathbb{R}$-anisotropes respectivement au Théorème 9.0.2 et Théorème 9.0.3.

Les calculs qui donnent les constantes explicites dans nos énoncés sont rassemblées dans deux appendices à la fin de la thèse. À l'Appendice B on donne des estimés du volume de petites boules dans un groupe orthogonal réel, ainsi qu'une formule du volume dans le cas

p-adique. Puis, on démontre des améliorations effectives, avec des constantes explicites, de résultats de la théorie de la réduction de formes quadratiques réels à l'Appendice B. Enfin on liste les constantes de nos énoncés à l'Appendice C.

Chapter 2

Introduction

The topic of my thesis is integral quadratic forms. Even though they have been studied for centuries, they are still at the heart of diverse subjects of contemporary research. The highlight is two new results, one concerning the problem of deciding if two given quadratic forms are equivalent, and the other on the finite generation of S-integral orthogonal groups. An important feature of this new theorems is that they are effective—i.e. quantitative—and completely explicit. The results of my thesis, as well as the methods used to establish them are inspired by the article [LM16] of Li and Margulis. In fact my two main theorems generalize two of their theorems in that paper.

This introduction is divided into four sections. The first two present some history of the problems addressed, the original results of Li and Margulis, and the generalizations I obtained. After spending a long time working on this topic I ended up with less answers than questions, some of which are discussed in the third section. Finally, the structure of the thesis is sketched in the fourth section.

2.1 Equivalence of quadratic forms

2.1.1 Classification of integral quadratic forms

To motivate the first problem we address let's discuss some ideas and concepts developed to attempt to classify integral quadratic forms. We say that two quadratic forms Q_1 and Q_2 in d variables with coefficients in a commutative ring $\mathcal{R}$ with unit are $\mathcal{R}$-equivalent if $Q_1 = Q_2 \circ g$ for some $g \in GL(d, \mathcal{R})$. The classification of integral quadratic forms is an unsolved hard problem with a long history.

C.F. Gauss treats the binary case in *Disquisitiones Arithmeticae* [Gau65], where he comes up with a procedure that, starting from a binary integral quadratic form Q, produces a sequence of them equivalent to the original one that is eventually periodic. He associates to Q its period or *cycle* of quadratic forms, and shows that Q_1 and Q_2 are $\mathbb{Z}$-equivalent[1] if and only if they have the same cycle—see [CS99, Theorem 1, p. 356]. He also characterizes the quadratic forms of the cycle in terms of simple inequalities between the coefficients, which leads to the notion of reduced binary quadratic form. We say that the integral quadratic

[1] In fact *properly equivalent*, which a matrix in $SL(2, \mathbb{Z})$ takes Q_1 to Q_2.

form $ax_1^2 + 2bx_1x_2 + cx_2^2$ is reduced—see [CS99, p. 358-359]—if it is positive definite and $|2b| \leq a \leq c$, or if it is indefinite and

$$0 < b < \sqrt{b^2 - ac} < \min\{b + |a|, b + |c|\}.$$

Inspired by the work of Gauss for the binary case, C. Hermite and later H. Minkowski, generalize the notion of reduced to quadratic forms to 3 or more variables. The leading principles are: every integral quadratic form should be $\mathbb{Z}$-equivalent to a reduced one, and there should be a way to figure out if two reduced quadratic forms are $\mathbb{Z}$-equivalent. That is how the *Reduction Theory of quadratic forms* was born. Here is the main finiteness result of the theory. In the statement, δ_R is the determinant of the matrix of the integral quadratic form R in d variables in the canonical basis of $\mathbb{Z}^d$.

Theorem 2.1.1. *Let d and N be positive integers. There are only finitely many reduced integral quadratic forms R in d variables with $|\delta_R| = N$.*

Reduction theory will play an important role in this work. I use the modern definition in terms of Siegel subsets of $GL(d, \mathbb{R})$.

Even with the advances in reduction theory, a complete classification of integral quadratic forms was—and still is—out of reach, so mathematicians started to search for new ideas, introducing new notions of equivalence of integral quadratic forms, hoping they would shed some light on the hard problem of $\mathbb{Z}$-classification. Let's discuss briefly two of them.

The first is the *genus*: we say that two integral quadratic forms in d variables are in the same genus if they are $\mathbb{R}$ and $\mathbb{Z}_p$-equivalent for any prime p[2]. Two $\mathbb{Z}$-equivalent integral quadratic forms are in the same genus, but the converse is false. For example,

$$Q_1(x) = x_1^2 + 82x_2^2 \quad \text{and} \quad Q_2(x) = 2x_1^2 + 41x_2^2$$

are not $\mathbb{Z}$-equivalent because $x_1^2 + 82x_2^2 = 2$ has no integral solutions, but they are in the same genus—see [Cas78, p. 129]. Nonetheless, quadratic forms in the same genus are almost $\mathbb{Z}$-equivalent in the following sense: they are $\mathbb{Z}^{(S)}$-equivalent for any a finite set S of primes, where $\mathbb{Z}^{(S)}$ is the subring of $\mathbb{Q}$ of rational numbers whose denominator is not divisible by any $p \in S$. In fact, this last condition is an alternative definition of genus—see [Cas78, Theorem 1.4, p. 130].

The second equivalence of quadratic forms we'll discuss is the *spinor genus*, introduced by M. Eichler. It is finer than the genus but (sometimes) coarser than $\mathbb{Z}$-equivalence. To avoid a big detour we won't define it here—see [Cas78, Lemma 1.4, p. 201]—, but to emphasize its importance we mention two facts: for $\mathbb{R}$-isotropic integral quadratic forms in at least 3 variables, a spinor genera is the same as a $\mathbb{Z}$-equivalence class—see [Cas78, Theorem 1.3, p. 202]. Second, J.H. Conway and N.A. Sloane describe in [CS99, Chapter 15, Section 9, p. 388] a practical way to compute the number of spinor genera. It is then possible to determine the number of $\mathbb{Z}$-equivalence classes of $\mathbb{R}$-isotropic integral quadratic forms in $d \geq 3$ variables. As for $\mathbb{R}$-anisotropic integral quadratic forms, even though there are reasonable methods to classify them for small d, Conway and Sloane [CS99, p. 353] believe there is no hope of an explicit classification since there are too many $\mathbb{Z}$-equivalence classes as soon as $d > 24$.

[2]This definition is undoubtedly motivated by the local-global principle for rational quadratic forms: two such quadratic forms are $\mathbb{Q}$-equivalent if and only if they are $\mathbb{R}$-equivalent and $\mathbb{Q}_p$-equivalent for any prime p.

2.1.2 Criterion of $\mathbb{Z}$-equivalence

After our brief discussion concerning the classification of integral quadratic forms, we present the less ambitious related problem we'll treat: Given integral quadratic forms Q_1 and Q_2 in d variables, decide if they are $\mathbb{Z}$-equivalent. We'll refer to this as the *problem of $\mathbb{Z}$-equivalence.* Here is a situation for which there is an easy solution to this problem, and which motivates our approach to the general case: When Q_1 and Q_2 are positive or negative definite—$\mathbb{R}$-anisotropic for short—, one can show with elementary arguments that any $g \in GL(d,\mathbb{R})$ taking Q_1 to Q_2 verifies

$$||g||_\infty \leq d \cdot d! ||Q_1||_\infty^{\frac{d-1}{2}} ||Q_2||_\infty^{\frac{1}{2}}, \tag{2.1}$$

where $||Q_i||_\infty$ is the maximum of the absolute values of the coefficients of Q_i. So, Q_1 and Q_2 are $\mathbb{Z}$-equivalent if and only if $Q_1 \circ \gamma = Q_2$ has a solution γ in the **finite** subset of $GL(d,\mathbb{Z})$ determined by (2.1).

This naive strategy doesn't work for $\mathbb{R}$-isotropic quadratic forms because the subset of matrices in $GL(d,\mathbb{R})$ taking Q_1 to Q_2 is unbounded. Surprisingly, C.L. Siegel shows in [Sie72] that even when the quadratic forms are $\mathbb{R}$-isotropic, one can restrict the search of a $\gamma \in GL(d,\mathbb{Z})$ that takes Q_1 to Q_2 to a finite subset of $GL(d,\mathbb{Z})$.

Theorem 2.1.2. *For any $d \geq 2$ there is an explicit real-valued function M_d with the following property: if the integral quadratic forms Q_1 and Q_2 in d variables are $\mathbb{Z}$-equivalent, there is $\gamma \in GL(d,\mathbb{Z})$ with*

$$||\gamma||_\infty \leq M_d(Q_1, Q_2)$$

such that $Q_1 \circ \gamma = Q_2$.

A function M_d as in Theorem 2.1.2 is a *search bound* for the problem of $\mathbb{Z}$-equivalence. Siegel uses the reduction theory of Hermite and Minkowski to prove the existence of search bounds for the problem of $\mathbb{Z}$-equivalence. Apart from the original article [Sie72] (written in german), one can find a sketch of the proof of Theorem 2.1.2 in the book of Cassels [Cas78, Chapter 13, Section 12, p. 324]. Siegel doesn't give an explicit formula for M_d, but S. Straumann shows in his master dissertation [Str99] that Siegel's ideas yield[3]

$$M_d(Q_1, Q_2) = \exp(A_d |\delta_{Q_1}|^{\frac{d^3+d^2}{2}}) \cdot \max\{||Q_1||_\infty, ||Q_2||_\infty\}^{\frac{d^3-d^2}{2}},$$

where δ_{Q_1} is as in Theorem 2.1.1 and A_d is a constant depending only on d. [4]

Once we know there are search bounds for the problem of $\mathbb{Z}$-equivalence, it is natural to look for an M_d that grows as slow as possible. Straumann's work shows that the search bound of Siegel is exponential in $||Q_1||_\infty, ||Q_2||_\infty$. In the sequel we'll simply say that M_d is exponential or polynomial when it has the respective property with respect to $||Q_1||_\infty, ||Q_2||_\infty$.

Now we'll discuss the main contribution to this problem in chronological order. It is known that M_2 can't be polynomial, because that would imply a polynomial bound for the smallest solution for Pell-like equations

$$au^2 - bv^2 = \pm 1, \tag{2.2}$$

[3] Recall that δ_{Q_1} is the determinant of the matrix of Q_1 in the canonical basis of $\mathbb{Z}^d$

[4] In the sequel we'll use $A_d, B_d, C_d, \ldots$ to denote constants that depend only on d.

with $a, b \in \mathbb{Z}$. Indeed, if $(u_0, v_0) \in \mathbb{Z}^2$ a solution of (2.2), then

$$\gamma_0 = \begin{pmatrix} u_0 & bv_0 \\ v_0 & au_0 \end{pmatrix} \in GL(2, \mathbb{Z})$$

takes $Q_1(x) = ax_1^2 - bx_2^2$ to $Q_2(x) = \pm x_1^2 \mp abx_2^2$. If M_2 is polynomial, the first column of a $\gamma_0 \in GL(2, \mathbb{Z})$ taking Q_1 to Q_2 would be a solution of (2.2) with norm bounded by a polynomial in a, b. An example of a family of Pell-like equations where the minimal solution grows faster than any polynomial in a, b can be found in the article [Lag80, p. 486] de J. Lagarias.

The situation is quite different for quadratic forms in 3 variables. R. Dietmann proves in [Die03] that one can take

$$M_3(Q_1, Q_2) = B_3 ||Q_1||_\infty^{510} (||Q_1||_\infty + ||Q_2||_\infty)^{207},$$

a polynomial search bound. D. Masser conjectures in his survey article [Mas02] this phenomenon is valid more generally for quadratic forms in 3 or more variables.

Conjecture 2.1.3. *For any integer $d \geq 3$ there are constants C_d, E_d with the following property: If the non-degenerate integral quadratic forms in d variables Q_1 and Q_2 are $\mathbb{Z}$-equivalent, there is $\gamma_0 \in GL(d, \mathbb{Z})$ with*

$$||\gamma_0||_\infty \leq C_d (||Q_1||_\infty + ||Q_2||_\infty)^{E_d},$$

such that $Q_2 = Q_1 \circ \gamma_0$.

The next major advance in this story is also made by Dietmann, who establishes Masser's Conjecture when δ_{Q_1}—the determinant of the matrix of Q_1 in the standard basis of $\mathbb{Q}^d$—is cube-free, not divisible by 4 and that not all entries in the main diagonal of the matrix of Q_1 are even [Die07, Theorem 3]. These assumptions allow him to extend his methods for ternary quadratic forms. When $d \geq 6$ he obtains

$$M_d(Q_1, Q_2) = C_d \max\{||Q_1||_\infty, ||Q_2||_\infty\}^{E_d},$$

where E_d is polynomial in d with leading term $5^d d^{d+1}$.

Li and Margulis establish Masser's Conjecture in full generality in [LM16, Theorem 1], improving the search bounds of Dietmann. Here is a simplified version of their result.

Theorem 2.1.4. *Let Q_1 and Q_2 be non-degenerate integral quadratic forms in $d \geq 3$ variables. If Q_1 and Q_2 are $\mathbb{Z}$-equivalent, there is $\gamma_0 \in GL(d, \mathbb{Z})$ with*

$$||\gamma_0||_\infty \leq C_d (||Q_1||_\infty ||Q_2||_\infty)^{\frac{13}{40} d^3}$$

such that $Q_1 \circ \gamma_0 = Q_2$.

2.1.3 The methods of Li and Margulis

The strategies of Dietmann and Li-Margulis to tackle the problem of $\mathbb{Z}$-equivalence are very different. On the one hand, Dietmann relies mostly on tools from analytic number theory, such as the Circle Method of Hardy and Littlewood. This approach is natural considering that his interest on search bounds for the $\mathbb{Z}$-equivalence of integral quadratic forms comes from its connection to search bounds to decide the solvability of the general quadratic diophantine equation. In fact, this is the central topic of the survey [Mas02] where Masser formulates its conjecture.

Now we'll motivate the approach of Li and Margulis. To start, one has to change the point of view of the problem by taking advantage of a simple, yet extremely important duality phenomenon. Suppose we are dealing with quadratic forms Q_1 and Q_2 of signature $2,1$. Let $P(x) = x_1^2 + x_2^2 - x_3^2$ and consider the groups $G = GL(3,\mathbb{R})$, $H = O(P,\mathbb{R})$ and $\Gamma = GL(3,\mathbb{Z})$. We write Q_i as $P \circ g_i$ for $g_1, g_2 \in G$. Since any quadratic form of signature 2,1 is of the form $P \circ g$ with $g \in G$, the space of all such quadratic forms is naturally identified with $H\backslash G$. Here is the important observation: a $\mathbb{Z}$-equivalence class of integral quadratic forms (of signature 2,1) is a Γ-orbit in $H\backslash G$, which corresponds naturally to an H-orbit on the space $X = G/\Gamma$[5], which identifies with the space of lattices of $\mathbb{R}^3$. Finding $\gamma_0 \in GL(3,\mathbb{Z})$ transforming Q_1 to Q_2 is equivalent to finding an $h_0 \in H$ moving the lattice $g_2\mathbb{Z}^3$ to $g_1\mathbb{Z}^3$. It turns out that the H-orbit Y of $g_2\mathbb{Z}^3$ is closed in X and admits a finite H-invariant measure, which enables Li and Margulis to tackle the problem with the powerful machinery of homogeneous dynamics, more specifically, effective homogeneous dynamics. The action of H on Y is nearly mixing, and moreover, there is an effective mixing speed that Li and Margulis use to show there is an h_0 moving $g_2\mathbb{Z}^3$ to $g_1\mathbb{Z}^3$ of norm bounded by a function of $||g_1||_\infty, ||g_2||_\infty$ and the volume of Y.

To close the discussion of Theorem 2.1.4, let us mention the two main technical ingredients of its proof. First, an estimation of the volume of Y that is deduced from the effective recurrence of unipotent flows of Kleinbock and Margulis [KM98]. Secondly, the Kim-Sarnak bound [Kim03, Appendix 2] for the Ramanujan-Petersson Conjecture for $\mathbf{SL}(2)$ over $\mathbb{Q}$, a profound result on the theory of automorphic representations, which yields a uniform effective mixing speed for the action of H on closed H-orbits in X.

2.1.4 Criterion of $\mathbb{Z}_S$-equivalence

The first objective of my thesis is to obtain a result analogous to Theorem 2.1.4 for the slightly more general problem of $\mathbb{Z}_S$-equivalence of integral quadratic forms. If $S_f = \{p_1, \dots, p_k\}$ is a finite set of primes, we set $S = \{\infty\} \cup S_f$. The ring of S-integers $\mathbb{Z}_S$ consists of the rational numbers with denominator a product of powers of the primes in S_f. The product of the elements of S_f will be denoted by p_S. By convention $\mathbb{Z}_S = \mathbb{Z}$ and $p_S = 1$ when $S = \{\infty\}$. Given two integral quadratic forms in d variables Q_1 and Q_2, this time we want to decide if Q_1 and Q_2 are $\mathbb{Z}_S$-equivalent by searching a solution γ of $Q_1 \circ \gamma = Q_2$ in an explicit finite subset of $GL(d,\mathbb{Z}_S)$. In Theorem 2.1.4, an inequality of the form $||\gamma||_\infty \leq M$ determines a *search subset* of $GL(d,\mathbb{Z})$, which is finite because an entry of any such γ is an integer with

[5]Before Li and Margulis, other authors have exploited the duality between Γ-orbits of quadratic forms and H-orbits of lattices of $\mathbb{R}^d$. For example, Eichler uses it to define spinor genera.

absolute value at most M. But $|x| \leq M$ has infinite solutions in $\mathbb{Z}_S$ when S_f is non-empty, hence the inequality $||\gamma||_\infty \leq M$ is not enough. We'll proceed as follows: Recall that any $t \in \mathbb{Z}_S$ is of the form

$$t = \frac{n}{p_1^{a_1} \cdots p_k^{a_k}}$$

with $n \in \mathbb{Z}$ and $a_1, \ldots, a_k \in \mathbb{N}$. If in addition to an upper bound for $|t|$ we impose an upper bound on each a_i, the resulting system has finitely many solutions in $\mathbb{Z}_S$. For $\gamma \in M_d(\mathbb{Q})$, let $||\gamma||_p$ be the maximum of the p-adic absolute values of the entries of γ, and let

$$||\gamma||_S = \max_{\nu \in S} ||\gamma||_\nu.$$

Then $||\gamma||_S \leq M$ defines a finite subset of $GL(d, \mathbb{Z}_S)$. Here is our result.

Theorem 2.1.5. *Let Q_1 and Q_2 be non-degenerate integral quadratic forms in $d \geq 3$ variables and let S_f be a finite set of odd primes. If Q_1 and Q_2 are $\mathbb{Z}_S$-equivalent, there is $\gamma_0 \in GL(d, \mathbb{Z}_S)$ with*

$$||\gamma_0||_S \leq F_d p_S^{19d^6} (||Q_1||_\infty ||Q_2||_\infty)^{2d^3}$$

such that $Q_1 \circ \gamma_0 = Q_2$.

The assumption $2 \notin S$ is not essential. In fact the proof we give works also, but at certain points there are more cases to consider[6]. Recall that the *easy case* of Theorem 2.1.4, where $S = \{\infty\}$, is when Q_1 and Q_2 are $\mathbb{R}$-anisotropic. For general S, the easy case is when Q_1 and Q_2 are $\mathbb{Q}_\nu$-anisotropic[7] for every $\nu \in S$, because any $g \in GL(d, \mathbb{Q})$ taking Q_1 to Q_2 verifies

$$||g||_S \leq d \cdot d! ||Q_1||_\infty^{\frac{d-1}{2}} ||Q_2||_\infty^{\frac{1}{2}}.$$

The interesting case is when Q_1 and Q_2 are isotropic over $\mathbb{Q}_\nu$ for some $\nu \in S$, which is covered by Theorem 5.1.1 and Theorem 5.1.2 when Q_1 and Q_2 are $\mathbb{R}$-isotropic and $\mathbb{R}$-anisotropic, respectively.

Li and Margulis address the case $S = \{\infty\}$ by studying the action of a real orthogonal group H on the space X of lattices of $\mathbb{R}^d$. We adapt their strategy for general S in the following way: Suppose that Q_1 and Q_2 are $\mathbb{Z}_S$-equivalent. We need to control $||\gamma||_\nu$ for any $\nu \in S$ of some $\gamma \in GL(d, \mathbb{Z}_S)$ taking Q_1 to Q_2, so we'll consider the quadratic forms Q_1 and Q_2 over every $\mathbb{Q}_\nu$. Let P_ν be a *standard* representative of the $\mathbb{Q}_\nu$-equivalence class of Q_1 and Q_2. To do the job in one shot, we'll think the Q_i's as quadratic forms over $\mathbb{Q}_S = \prod_{\nu \in S} \mathbb{Q}_\nu$ via the diagonal embedding $\mathbb{Q} \to \mathbb{Q}_S$, so they are $\mathbb{Q}_S$-equivalent to $P = (P_\nu)_{\nu \in S}$. Consider the groups

$$G_S = GL(d, \mathbb{Q}_S) = \prod_{\nu \in S} GL(d, \mathbb{Q}_\nu), \qquad H_S = O(P, \mathbb{Q}_S) = \prod_{\nu \in S} O(P_\nu, \mathbb{Q}_\nu),$$

and take $g_1, g_2 \in G_S$ such that $Q_i = P \circ g_i$. What replaces X in this context? Note that diagonal copy of $\mathbb{Z}_S$ in $\mathbb{Q}_S$ is a lattice in $\mathbb{Q}_S$, hence $\mathbb{Z}_S^d$ is a lattice in $\mathbb{Q}_S^d$. The group G_S

[6] The difference between 2 and $p > 2$ comes from the fact that $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2$ has order 8 while $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ has order 4. As a result, there are more equivalence classes of quadratic forms over $\mathbb{Q}_2$ than over $\mathbb{Q}_p$.

[7] Where $\mathbb{Q}_\infty$ stands for $\mathbb{R}$.

acts transitively on the space X_S of lattices of $\mathbb{Q}_S^d$, and the stabilizer of $\mathbb{Z}_S^d$ is the diagonal copy Γ_S of $GL(d,\mathbb{Z}_S)$ in G_S. Finding $\gamma_0 \in GL(d,\mathbb{Z}_S)$ taking Q_1 to Q_2 amounts to finding $h_0 \in H_S$ moving $g_2\mathbb{Z}_S^d$ to $g_1\mathbb{Z}_S^d$. Happily for us, the dynamical setting is as good as in the case $S = \{\infty\}$: the orbit $Y = H_S g_2 \mathbb{Z}_S$ is closed in X_S, it admits a finite H_S-invariant measure, and the action of H_S on Y is almost mixing, so we are also able to address the problem with homogeneous dynamics. We'll bound $||h_0||_S$ in terms of $||g_i||_S$ and the volume of Y—see propositions 5.2.2 and 5.2.3.

The two main technical ingredients to prove Theorem 2.1.5 are very similar to those used by Li and Margulis for $S = \{\infty\}$. To estimate the volume of Y we'll apply the effective S-adic recurrence of unipotent flows of Kleinbock and Tomanov [KT07]. The uniform effective mixing speed for the action of H_S on closed H_S-orbits in X_S will be deduced also from Kim-Sarnak's bound [Kim03, Appendix 2] for the Ramanujan-Petersson conjecture for $\mathbf{SL}(2)/\mathbb{Q}$ when the Q_i's are $\mathbb{R}$-isotropic, and when they are $\mathbb{R}$-anisotropic, from Deligne's theorem on holomorphic modular forms [Lub94, Theorem 1.2, p. 148] in its representation theoretic version [Lub94, Theorem 2.14, p. 158], and the classical Jacquet-Langlands Correspondence [Lub94, Theorem 3.4, p. 163].

2.2 The group of units of a quadratic form

2.2.1 The classical results of Siegel

It is likely that the interest of many that have worked with quadratic forms comes from their connection with Number Theory. For example, to understand quadratic number fields $K = \mathbb{Q}[\sqrt{D}]$ one must study the binary quadratic forms $Q(x) = x_1^2 - Dx_2^2$. The group of units $\mathcal{O}_K^\times$ of the ring of integers of K is intimately related to the integral orthogonal group $O(Q,\mathbb{Z})$, for this reason some people refer to $O(Q,\mathbb{Z})$ as the *group of units* of Q. In the milestone paper [Sie39] of 1939, Siegel undertakes the investigation of the group of units of integral quadratic forms in 3 or more variables, obtaining two results of the utmost importance for this thesis. The first one is [Sie39, Satz 11, p. 230].

Theorem 2.2.1. *For any non-degenerate integral quadratic form Q in $d \geq 3$ variables, the group $O(Q,\mathbb{Z})$ is finitely generated.*

Li and Margulis obtain in [LM16] an effective version of Theorem 2.2.1, which we extend to the group of S-units $O(Q,\mathbb{Z}_S)$ of Q, for any S. These result are discussed in the next subsection. The second important theorem of Siegel is [Sie39, Satz 12, p. 233].

Theorem 2.2.2. *For any non-degenerate integral quadratic form Q in $d \geq 3$ variables, the group $O(Q,\mathbb{Z})$ is a lattice in $O(Q,\mathbb{R})$.*

The role played by Theorem 2.2.2 in this work is the following: Consider again the dynamical system $H \curvearrowright X$ used by Li and Margulis for the problem of $\mathbb{Z}$-equivalence. The key fact that H-orbits in X admit a finite H-invariant measure comes[8] from Theorem 2.2.2. More generally, the diagonal copy of $O(Q,\mathbb{Z}_S)$ in $O(Q,\mathbb{Q}_S)$ is a lattice in $O(Q,\mathbb{Q}_S)$, and that's why closed H_S-orbits in X_S admit finite H_S-invariant measures.

[8] Because closed H-orbits come from integral quadratic forms—see Lemma 6.1.2.

The proofs of theorems 2.2.1 and 2.2.2 rely heavily on the reduction theory of Hermite and Minkowski, which was polished by Siegel himself. A. Borel and Harish-Chandra pushed further these ideas in their 1962 article [BH62] where, based classical examples of lattices in semisimple real Lie groups, such as $SL(d,\mathbb{Z}) \subset SL(d,\mathbb{R})$ and $O(Q,\mathbb{Z}) \subset O(Q,\mathbb{R})$, they introduce the notion of arithmetic subgroup of a linear algebraic $\mathbb{Q}$-group $\mathbf{G}$. They develop, by analogy with quadratic forms, a reduction theory for arithmetic groups which is used to generalize Theorem 2.2.1— arithmetic groups are finitely generated—and Theorem 2.2.2—obtaining a condition on $\mathbf{G}$ for $\mathbf{G}_{\mathbb{R}}/\mathbf{G}_{\mathbb{Z}}$ to have finite volume. They also establish—at almost the same time as G.D. Mostow and T. Tamagawa [MT62]—*Godement's Conjecture*, which gives necessary and sufficient conditions on a $\mathbb{Q}$-group $\mathbf{G}$ for $\mathbf{G}_{\mathbb{R}}/\mathbf{G}_{\mathbb{Z}}$ to be compact. The extension—by Borel—of these results to S-arithmetic groups came shortly after in [Bor63].

2.2.2 Small generators of S-integral orthogonal groups

In the article [LM16], Li and Margulis deduce several interesting results on integral quadratic forms from Theorem 2.1.4. One that I find particularly beautiful is an effective version [LM16, Theorem 2] on the finite generation of $O(Q,\mathbb{Z})$.

Theorem 2.2.3. *Let Q be a non-degenerate integral quadratic form in $d \geq 3$ variables. The group $O(Q,\mathbb{Z})$ is generated by its elements γ with*

$$||\gamma||_\infty \leq J_d ||Q||_\infty^{d^7+3d^4}.$$

The proof is based on Theorem 2.1.4 and effective refinements of classical results on reduction theory of integral quadratic forms.

Following their lead, I obtain an effective finite generation of $O(Q,\mathbb{Z}_S)$ for any finite set S_f of primes from effective results on reduction theory of quadratic forms over $\mathbb{Q}_S$ and Theorem 2.1.5.

Theorem 2.2.4. *Let Q be a non-degenerate integral quadratic forms in $d \geq 3$ variables. For any finite set S_f of primes, the group $O(Q,\mathbb{Z}_S)$ is generated by its elements γ with*

$$||\gamma||_S \leq L_d p_S^{20d^7} ||Q||_\infty^{4d^6}.$$

2.3 Some interesting further problems

The main motivation of this thesis is the problem of deciding if two given integral quadratic forms Q_1 and Q_2 in d variables are $\mathbb{Z}$-equivalent. It can be reformulated in a more geometric way as: are the quadratic spaces $(\mathbb{Z}^d, Q_1)$ and $(\mathbb{Z}^d, Q_2)$ isometric? But what if Q_1 has d_1 variables and Q_2 has $d_2 < d_1$ variables? An equally interesting problem is to decide if Q_1 *represents* Q_2, which means there is an isometric embedding $(\mathbb{Z}^{d_2}, Q_2) \hookrightarrow (\mathbb{Z}^{d_1}, Q_1)$. Li and Margulis obtain an effective search bound [LM16, Theorem 4] for this problem, which is yet another application of Theorem 2.1.4. Due to time constraints I didn't include here the natural S-adic generalization.

It is known that the groups $O(Q,\mathbb{Z}_S)$ are finitely presented— see [PR94, Theorem 5.11, p. 272]—, and now that we have explicit generating sets $\mathscr{G}_S^Q$ of them thanks to theorems 2.2.3 and 2.2.4, it would be nice to give a set of relations on $\mathscr{G}_S^Q$ that defines $O(Q,\mathbb{Z}_S)$.

The program of making effective classical results on S-integral orthogonal groups could also be extended to S-arithmetic groups of other classical $\mathbb{Q}$-groups, such as unitary groups. Some have already explored this line of research, like T. Chinburg and M. Stover who give in the recent article [CS14] small generators of the group of S-units of central simple $\mathbb{Q}$-algebras. Although not effective, we mention also the algorithmic approach to the topic by F. Grunewald and D. Segal, who treat arithmetic groups in [GS80] and S-arithmetic groups in [GS85].

2.4 Structure of the thesis

The first part consists of two chapters that set the stage. In Chapter 3 we recall the classification of quadratic forms over $\mathbb{R}$ and $\mathbb{Q}_p$, and we fix a representative in each equivalence class, which we'll call *standard quadratic forms*. We make reference to them in every chapter of the thesis. In Chapter 4 we review part of the theory of unitary representations of $SL(2, \mathbb{Q}_\nu)$, with emphasis on the effective decay speed of coefficients of *almost* L^k unitary representations. This is the technical tool behind the effective mixing speed for the dynamical system of $\mathbb{Z}_S$-equivalence.

The second—and biggest—part of the thesis is devoted to the proof of our search bound for the $\mathbb{Z}_S$-equivalence problem, which spreads through chapters 5 to 8. In Chapter 5 we translate the arithmetic problem of $\mathbb{Z}_S$-equivalence into a dynamical one in terms of the action of an S-adic orthogonal group H_S on the space X_S of lattices of $\mathbb{Q}_S^d$: given points y_2, y_1 in a closed H_S-orbit Y in X_S, we bound $||h_0||_S$ for an $h_0 \in H_S$ moving y_2 to y_1. This is done in Proposition 5.2.2 when H_∞ is non-compact, and in Proposition 5.2.3 when H_∞ is compact. We prove these propositions in Chapter 6 and Chapter 7, respectively. The bound of $||h_0||_S$ involves the volume of the orbit Y, so in Chapter 8 we obtain an upper bound of it in terms the determinant of Q when Y comes from an integral quadratic form Q.

Having established our search bound for $\mathbb{Z}_S$-equivalence, we use it in Chapter 9 to prove Theorem 2.2.4 on the effective finite generation of $O(Q, \mathbb{Z}_S)$. We handle $\mathbb{R}$-isotropic quadratic forms in Theorem 9.0.2, leaving the $\mathbb{R}$-anisotropic ones to Theorem 9.0.3.

The computations that give the explicit constants in our statements are gathered in two appendices at the end of the thesis. In Appendix A we estimate the volume of small balls in orthogonal groups with coefficients in $\mathbb{Q}_\nu$. For real orthogonal groups we obtain upper and lower bounds in Lemma A.2.1, and in the p-adic case we prove a formula for the exact volume in Lemma A.2.11. In Appendix B we prove effective versions of classical results on reduction theory of real quadratic forms with explicit constants. For commodity of reference we list the constants in our statements in Appendix C.

Chapter 3

Quadratic forms over $\mathbb{Q}_\nu$

In this first chapter we present the main object of study of this work: quadratic forms. After giving the basic definitions in Section 3.1, we specialize to the case of quadratic forms over a completion $\mathbb{Q}_\nu$ of $\mathbb{Q}$, recalling (without proof) the classification of these. For future reference, we choose a representative in each equivalence class, which we call *standard quadratic forms*. This is done in Section 3.2 for real quadratic forms and in Section 3.3 for p-adic quadratic forms. We prove a bound on the size of a matrix relating a quadratic form to its standard form in Lemma 3.2.2 and Proposition 3.3.4. In Section 3.4 we introduce the *Spin* group of a quadratic form, which is the universal covering of the respective special orthogonal group. We conclude with a discussion in Section 3.5 of the relation between $SL(2, \mathbb{Q}_\nu)$ and isotropic quadratic forms on $\mathbb{Q}_\nu^3$.

3.1 Basic definitions

A quadratic form in d variables is an homogeneous polynomial of degree 2

$$Q(x) = \sum_{i,j=1}^{d} a_{ij} x_i x_j,$$

with coefficients in a commutative ring $\mathcal{R}$ with unit. We say that Q is *isotropic* if there is $v \in \mathcal{R}^d - \{0\}$ such that $Q(v) = 0$, and that Q is *anisotropic* if there is no such v. Let Q, Q_1, and Q_2 be quadratic forms in d variables with coefficients in $\mathcal{R}$. Q_1 and Q_2 are $\mathcal{R}$-*equivalent*, denoted $Q_1 \underset{\mathcal{R}}{\sim} Q_2$, if they coincide up to a base-change of $\mathcal{R}^d$. In other words, $Q_1 \underset{\mathcal{R}}{\sim} Q_2$ if there exists $g \in GL(d, \mathcal{R})$—the group of $d \times d$ matrices whose determinant is invertible in $\mathcal{R}$—such that $Q_2(x) = Q_1 \circ g(x)$. Q is non-degenerate if it is not $\mathcal{R}$-equivalent to a quadratic form in less than d variables.

Suppose that 2 is invertible in $\mathcal{R}$. Let's recall the correspondence between quadratic forms in d variables and symmetric bilinear forms on $\mathcal{R}^d$. Q defines a symmetric bilinear form $\langle \cdot, \cdot \rangle_Q$ on $\mathcal{R}^d$ by the formula

$$\langle x, y \rangle_Q = \frac{1}{2}(Q(x+y) - Q(x) - Q(y)).$$

Conversely, if $\langle\cdot,\cdot\rangle$ is a symmetric bilinear form on $\mathcal{R}^d$, $x \mapsto \langle x, x\rangle$ defines a quadratic form. We denote by b_Q the matrix $(\langle e_i, e_j\rangle_Q)_{i,j}$ of $\langle\cdot,\cdot\rangle_Q$ with respect to the standard basis $e_1, \cdots, e_d$ of $\mathcal{R}^d$, and we define $\delta_Q = \det b_Q$.

Now, a quick remainder of the possible absolute values on $\mathbb{Q}$, which are maps $|\cdot| : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ such that for any $s, t \in \mathbb{Q}$:

(i) $|s| = 0 \Leftrightarrow s = 0$,

(ii) $|st| = |s| \cdot |t|$,

(iii) $|s + t| \leq |s| + |t|$.

An absolute value on $\mathbb{Q}$ is said to be trivial if it induces the discrete topology on $\mathbb{Q}$. Two absolute values on $\mathbb{Q}$ are equivalent if their topologies on $\mathbb{Q}$ coincide. Besides the standard absolute value, that we'll denote by $|\cdot|_\infty$, there is an absolute value $|\cdot|_p$ for each prime number p uniquely determined by:

$$|n|_p = \begin{cases} 1 & \text{if } n \in \mathbb{Z} - p\mathbb{Z}, \\ p^{-1} & \text{if } n = p. \end{cases}$$

The completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$ and $|\cdot|_p$ are respectively $\mathbb{R}$ and the field of p-adic numbers $\mathbb{Q}_p$. The absolute values $|\cdot|_\infty$ and $|\cdot|_p$ exhaust all the possible equivalence classes of non-trivial absolute values on $\mathbb{Q}$ according to Ostrowski's Theorem—see [Kob84, Theorem 1, p. 3]. For this reason, we'll say that ∞ is also a prime number. We'll use the symbol ν to refer to a prime number, possibly ∞, and p for finite primes. Let $||\cdot||_\nu$ be the norm on the space of $d \times d$ matrices $M_d(\mathbb{Q}_\nu)$ of the maximum of the ν-absolute value of the entries. If Q is a quadratic form on $\mathbb{Q}_\nu^d$ we define $||Q||_\nu = ||b_Q||_\nu$.

3.2 Real quadratic forms

Let's review the classification of quadratic forms over $\mathbb{Q}_\nu$, starting with the familiar case of real quadratic forms. A non-degenerate real quadratic form R on $\mathbb{R}^d$ is $\mathbb{R}$-equivalent to a diagonal quadratic form. The next classical lemma says a bit more—see [BO07, Fact 5.1].

Lemma 3.2.1. *Let R be a non-degenerate quadratic form on $\mathbb{R}^d$. There is $k \in O(d, \mathbb{R})$ such that $R \circ k$ is diagonal.*

Suppose that R is $\mathbb{R}$-equivalent to $R'(x) = a_1 x_1^2 + \cdots + a_d x_d^2$. Permuting the variables if necessary we may assume that $a_1, \ldots, a_p > 0$ and $a_{p+1}, \ldots, a_d < 0$. A suitable diagonal matrix takes R' to

$$Q_{p,q}(x) = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2,$$

where $p + q = d$. Any non-degenerate quadratic form on $\mathbb{R}^d$ is equivalent to exactly one $Q_{p,q}$ with $p + q = d$. We'll refer to these as the *standard quadratic forms on* $\mathbb{R}^d$.

We write R as $P \circ g$ with P standard and $g \in GL(d, \mathbb{R})$. The next lemma says that we can choose g with norm controlled by the size of the coefficients of R—see also [LM16, Lemma 1].

Lemma 3.2.2. *We can write any non-degenerate quadratic form R on $\mathbb{R}^d$ as $P \circ g_\infty$, where P is a standard quadratic form on $\mathbb{R}^d$ and $g_\infty \in GL(d, \mathbb{R})$ verifies*

$$||g_\infty||_\infty \leq d||R||_\infty^{\frac{1}{2}}.$$

Proof. We start by proving an auxiliary inequality. Consider $k \in O(d, \mathbb{R})$ and $A \in M_d(\mathbb{R})$. For any $1 \leq i, j \leq d$ we have

$$\begin{aligned}\left|\sum_{\ell=1}^{d} k_{i\ell}A_{\ell j}\right|_\infty &\leq \left(\sum_{\ell=1}^{d} k_{i\ell}^2\right)^{\frac{1}{2}} \left(\sum_{\ell=1}^{d} A_{\ell j}^2\right)^{\frac{1}{2}} \\ &\leq \sqrt{d} \cdot ||A||_\infty.\end{aligned}$$

This proves that $||kA||_\infty \leq \sqrt{d} \cdot ||A||_\infty$.

We pass to quadratic forms. By Lemma 3.2.1 there is $k \in O(d, \mathbb{R})$ such that

$$R'(x) = R \circ k(x) = a_1 x_1^2 + \cdots a_d x_d^2.$$

We assume further that $a_1, \ldots, a_p$ are positive, and the rest are negative—permutation matrices are in $O(d, \mathbb{R})$. Note that

$$||R'||_\infty = ||b_{R'}||_\infty = ||{}^t k b_R k||_\infty \leq d||R||_\infty.$$

Consider

$$g'_\infty = diag(\sqrt{|a_1|_\infty}, \ldots, \sqrt{|a_d|_\infty}),$$

and $g_\infty = g'_\infty k^{-1}$. Then g_∞ takes $x_1^2 + \cdots + x_p^2 - \cdots - x_d^2$ to R and

$$||g_\infty||_\infty \leq \sqrt{d}\,||g'_\infty||_\infty = \sqrt{d}\,||R'||_\infty^{\frac{1}{2}} \leq d||R||_\infty^{\frac{1}{2}}.$$

□

3.3 p-adic quadratic forms

We move to the p-adic world. Let's discuss first quadratic forms in one variable. For $a, b \in \mathbb{Q}_p^\times$, ax_1^2 is $\mathbb{Q}_p$-equivalent to bx_1^2 if and only if a/b is a square in $\mathbb{Q}_p^\times$. The $\mathbb{Q}_p$-equivalence classes of non-degenerate quadratic forms in one variable are thus parametrized by $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$. The characterization of squares in $\mathbb{Q}_p^\times$ follows easily from the next lemma—see [Ser95, p. 34].

Lemma 3.3.1. *Let p be a prime number. A $t \in \mathbb{Z}_p^\times$ is a square in $\mathbb{Z}_p$ if an only if $t \mod p$ is a square in $\mathbb{F}_p^\times$ when $p > 2$, or $t \equiv 1 \mod 8$ when $p = 2$.*

The group $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$ and

$$\mathcal{C}_2 = \{\pm 1, \pm 3, \pm 2, \pm 6\} \subseteq \mathbb{Q}_2^\times$$

is a system of representatives. When $p > 2$, $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \simeq (\mathbb{Z}/2\mathbb{Z})^2$. We fix the system of representatives

$$\mathcal{C}_p = \{1, \mathtt{n}_p, p, p\mathtt{n}_p\} \subseteq \mathbb{Q}_p^\times,$$

where $\mathtt{n}_p$ is an integer that is not a square in $\mathbb{Z}/p\mathbb{Z}$.

Now we recall the classification of p-adic quadratic forms in $d \geq 2$ variables. We focus in the diagonal case since any non-degenerate quadratic form on $\mathbb{Q}_p^d$ is $\mathbb{Q}_p$-equivalent to a diagonal one. The next lemma is a p-adic analog of Lemma 3.2.1—see [BO07, Fact 5.4]:

Lemma 3.3.2. *Let p be a prime and let R be a non-degenerate quadratic form on $\mathbb{Q}_p^d$. There is $k \in GL(d, \mathbb{Z}_p)$ such that $R \circ k$ is diagonal.*

There are two invariants that classify p-adic quadratic forms. The *discriminant* $\delta(R)$ of $R(x) = a_1x_1^2 + \cdots + a_dx_d^2$ is the projection of $a_1 \cdots a_d$ in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$, and its *epsilon invariant* is

$$\varepsilon(R) = \prod_{i<j}(a_i, a_j)_p,$$

where $(a, b)_p$ is the *Hilbert symbol*:

$$(a, b)_p = \begin{cases} 1 & \text{if } x_1^2 - ax_2^2 - bx_3^2 \text{ is isotropic,} \\ -1 & \text{if } x_1^2 - ax_2^2 - bx_3^2 \text{ is anisotropic.} \end{cases}$$

These two invariants‘ classify p-adic quadratic forms—see [Ser95, p. 70].

Theorem 3.3.3. *Two non-degenerate diagonal quadratic forms R_1 and R_2 on $\mathbb{Q}_p^d$ are $\mathbb{Q}_p$-equivalent if and only if $\delta(R_1) = \delta(R_2)$ and $\varepsilon(R_1) = \varepsilon(R_2)$.*

For any prime $p > 2$, the number of $\mathbb{Q}_p$-equivalence classes of non-degenerate quadratic forms in d variables with coefficients in $\mathbb{Q}_p$ is 4 if $d = 1$, 7 if $d = 2$ and 8 if $d \geq 3$—all the combinations of $\delta(R)$ and $\varepsilon(R)$ are realized. As for non-degenerate quadratic forms in d variables with coefficients in $\mathbb{Q}_2$, there are respectively 8, 15 and 16 $\mathbb{Q}_2$-equivalence classes if $d = 1, d = 2$ and $d \geq 3$. See [Ser95, Corollaire, p. 71].

3.3.1 Standard p-adic quadratic forms

Now we give the list of representatives of the $\mathbb{Q}_p$-equivalence classes of quadratic forms we'll be working with. A big difference between the real and the p-adic case is that in the latter there are anisotropic quadratic forms only when $d \leq 4$—see [Ser95, Théorème 6, p. 66]. We treat separately $p = 2$ and $p > 2$. Suppose first that $p > 2$. Any anisotropic quadratic form over $\mathbb{Q}_p$ is equivalent to exactly one of the following table. We'll call these *standard anisotropic quadratic forms over $\mathbb{Q}_p$*.

$d = 1$	$d = 2$	$d = 3$	$d = 4$
x_1^2	$x_1^2 - \mathtt{n}_p x_2^2$	$x_1^2 - \mathtt{n}_p x_2^2 + px_3^2$	$x_1^2 - \mathtt{n}_p x_2^2 + px_3^2 - p\mathtt{n}_p x_4^2$
$\mathtt{n}_p x_1^2$	$px_1^2 - p\mathtt{n}_p x_2^2$	$x_1^2 - \mathtt{n}_p x_2^2 + p\mathtt{n}_p x_3^2$	
px_1^2	$x_1^2 - px_2^2$	$x_1^2 + px_2^2 - p\mathtt{n}_p x_3^2$	
$p\mathtt{n}_p x_1^2$	$\mathtt{n}_p x_1^2 - p\mathtt{n}_p x_2^2$	$\mathtt{n}_p x_1^2 + px_2^2 - p\mathtt{n}_p x_3^2$	
	$x_1^2 - p\mathtt{n}_p x_2^2$		
	$\mathtt{n}_p x_1^2 - px_2^2$		

As for isotropic quadratic forms, we define the standard ones as either a direct sum of hyperbolic planes

$$x_1^2 - x_2^2 + \cdots + x_{2m-1}^2 - x_{2m}^2,$$

or a direct sum of hyperbolic planes and a standard anisotropic quadratic form. For example, there are 7 standard isotropic quadratic forms on $\mathbb{Q}_p^4$:

$$x_1^2 - x_2^2 + x_3^2 - x_4^2 \quad \text{and} \quad x_1^2 - x_2^2 + P(x_3, x_4),$$

with $P(x_3, x_4)$ anisotropic standard on $\mathbb{Q}_p^2$. For any prime $p > 2$ and any $d \geq 1$, every non-degenerate quadratic form on $\mathbb{Q}_p^d$ is $\mathbb{Q}_p$-equivalent to a unique standard quadratic form. For $p = 2$, we define the standard anisotropic quadratic forms in one variable as mx_1^2 with $m \in \mathcal{C}_2$, in two variables as $m_1x_1^2 - m_2x_2^2$ with $m_1 \neq m_2$ in $\mathcal{C}_2$, in three variables $m(x_1^2+x_2^2+x_3^2)$ with $m \in \mathcal{C}_2$ and $x_1^2 + x_2 + x_3^2 + x_4^2$ in four variables. Here we were less careful, there are different $\mathbb{Q}_2$-equivalent standard binary quadratic forms, but this won't cause troubles in the proofs. Standard isotropic quadratic forms are also direct sums of hyperbolic planes, or sums of hyperbolic planes and a standard anisotropic quadratic form.

The next result is analogous to Lemma 3.2.2.

Proposition 3.3.4. *Consider a prime number $p > 2$. We can write any non-degenerate quadratic form R on $\mathbb{Q}_p^d$ as $P \circ g$ for a standard quadratic form P and some $g \in GL(d, \mathbb{Q}_p)$ with*

$$||g||_p \leq \sqrt{p} \cdot ||R||_p^{\frac{1}{2}}.$$

Remark 3.3.5. *The ideas we'll use to prove Proposition 3.3.4 give a similar statement for $p = 2$, but with we might need to replace $\sqrt{p}$ by a bigger constant. Probably $2\sqrt{2}$ is enough.*

Let's see that it suffices to prove Proposition 3.3.4 for a particular kind of diagonal quadratic forms. Consider a non-degenerate quadratic form R on $\mathbb{Q}_p^d$. By Lemma 3.3.2 there is $k \in GL(d, \mathbb{Z}_p)$ such that

$$R'(x) = R \circ k(x) = a_1x_1^2 + \cdots + a_dx_d^2.$$

Write a_i as $p^{2m_i}u_i$, with $u_i \in \mathbb{Z}_p^\times \cup p\mathbb{Z}_p^\times$ and let $g = \text{diag}\,(p^{m_1}, \ldots, p^{m_d})$. Then gk^{-1} takes

$$R''(x) = u_1x_1^2 + \ldots + u_dx_d^2$$

to R and

$$||gk^{-1}||_p \leq \sqrt{p}\,||R'||_p^{\frac{1}{2}} = \sqrt{p}\,||R||_p^{\frac{1}{2}}.$$

It suffices then to prove the result for R''. We'll call *almost standard* a quadratic form $b_1x_1^2 + \cdots + b_dx_d^2$ with $b_i \in \mathbb{Z}_p^\times \cup p\mathbb{Z}_p^\times$. Proposition 3.3.4 follows then from the next lemma.

Lemma 3.3.6. *Consider a prime number $p > 2$. We can write any almost standard quadratic form R on $\mathbb{Q}_p^d$ as $P \circ g$ for a standard quadratic form P and some $g \in GL(d, \mathbb{Q}_p)$ with coefficients in $\mathbb{Z}_p$.*

We'll prove Lemma 3.3.6 by induction on d: we treat first the case $d = 2$, then $d = 3$ and finally $d \geq 4$.

3.3.2 Binary quadratic forms

Lemma 3.3.7. *Let $p > 2$ be a prime number. We can write any almost standard quadratic form R on $\mathbb{Q}_p^2$ as $P \circ g$ for a standard quadratic form P and a non-singular $g \in M_2(\mathbb{Z}_p)$.*

We'll use two auxiliary results to prove Lemma 3.3.7.

Lemma 3.3.8. *Let $p > 2$ be a prime number and let $a \in \mathbb{Q}_p^\times$. There is $v = (t_1, t_2) \in \mathbb{Q}_p^2$ such that $t_1^2 - t_2^2 = a$ and*

$$||v||_p \leq \sqrt{p} \cdot |a|_p^{\frac{1}{2}}.$$

Proof. We'll first prove the result for $a \in \mathcal{C}_p$. If $a = 1$, then $(t_1, t_2) = (1, 0)$ works. For $a = \mathtt{n}_p$, we consider two cases: if $p = 4m + 3$, we choose $\mathtt{n}_p = -1$ and $(t_1, t_2) = (0, 1)$. When $p = 4m + 1$, consider the map $\mathbb{Z} \to \mathbb{F}_p, s \mapsto s^2 + \mathtt{n}_p$. Note that p never divides $s^2 + \mathtt{n}_p$, so this function takes $\frac{p+1}{2}$ values in $\mathbb{F}_p^\times$. We can then choose $t_2 \in \mathbb{Z}$ such that $u = \mathtt{n}_p + t_2^2$ is a square in $\mathbb{Z}_p^\times$, and set $t_1 = \sqrt{u}$. Finally, if $a \in \{p, p\mathtt{n}_p\}$, then $u = a + 1$ is a square in $\mathbb{Z}_p^\times$ by Lemma 3.3.1, so $(t_1, t_2) = (\sqrt{u}, 1)$ does the job.

For the general case, we write $a \in \mathbb{Q}_p^\times$ as cs^2 with $c \in \mathcal{C}_p$ and $s \in \mathbb{Q}_p^\times$. Consider $v' = (t_1', t_2') \in \mathbb{Q}_p^2$ such that $(t_1')^2 - (t_2')^2 = c$ and $||v'||_p \leq \sqrt{p} \cdot |c|_p^{\frac{1}{2}}$. Then $(t_1, t_2) = sv'$ works. □

Lemma 3.3.9. *Consider a prime $p > 2$ and an anisotropic standard quadratic form P on $\mathbb{Q}_p^2$. For any $v \in \mathbb{Q}_p^2$ we have*

$$|P(v)|_p^{\frac{1}{2}} \leq ||v||_p \leq (p|P(v)|_p)^{\frac{1}{2}}.$$

Proof. We write $P(x) = a_1x_1^2 + a_2x_2^2$, and let $v = (t_1, t_2) \in \mathbb{Q}_p^2$. Consider first the case $|a_1|_p = 1$ and $|a_2|_p = p^{-1}$. Note that $|a_1t_1^2|_p \neq |a_2t_2^2|_p$ since they are even and odd powers of p, respectively. Then

$$|P(v)|_p = \max\{|t_1|_p^2, p^{-1}|t_2|_p^2\}.$$

If $|t_1|_p^2 > p^{-1}|t_2|_p^2$, then $|t_1|_p \geq |t_2|_p$. It follows that

$$||v||_p = |t_1|_p = |P(v)|_p^{\frac{1}{2}}.$$

When $|t_1|_p^2 < p^{-1}|t_2|_p^2$, necessarily $|t_1|_p < |t_2|_p$. Hence

$$||v||_p = |t_2|_p = \sqrt{p}\,|P(v)|_p^{\frac{1}{2}}.$$

Suppose now that $|a_1|_p = |a_2|_p = 1$. If $|t_1|_p \neq |t_2|_p$, then $|P(v)|_p = \max\{|t_1^2|_p, |t_2^2|_p\} = ||v||_p^2$. Assume now that $|t_1|_p = |t_2|_p$. Leaving aside the easy case $t_1 = t_2 = 0$, we can write $t_i = p^{-m}u_i$ for some $m \in \mathbb{Z}$ and $u_i \in \mathbb{Z}_p^\times$, so

$$P(v) = p^{-2m}(a_1u_1^2 + a_2u_2^2).$$

Since P is anisotropic, $|a_1u_1^2 + a_2u_2^2|_p = 1$, thus $|P(v)|_p = p^{2m} = ||v||_p^2$. Finally, when $|a_1|_p = |a_2|_p = p^{-1}$, the quadratic form $p^{-1}P$ falls in the previous case. □

We are ready for the main proof.

Proof of Lemma 3.3.7. We write $R(x) = a_1x_1^2 + a_2x_2^2$, so $a_1, a_2 \in \mathbb{Z}_p^\times \cup p\mathbb{Z}_p^\times$. Let P be the standard quadratic form on $\mathbb{Q}_p^2$ that is $\mathbb{Q}_p$-equivalent to R.

Suppose first that R is isotropic, so $P(x) = x_1^2 - x_2^2$. Comparing the discriminants of R and P we see that $a_2 = -a_1\lambda^2$ for some $\lambda \in \mathbb{Q}_p^\times$. Moreover $|\lambda|_p = 1$ since $|a_i|_p \in \{1, p^{-1}\}$. By Lemma 3.3.8 there is $v = (t_1, t_2) \in \mathbb{Z}_p^2$ such that $P(v) = a_1$. Then

$$g = \begin{pmatrix} t_1 & \lambda t_2 \\ t_2 & \lambda t_1 \end{pmatrix} \in M_2(\mathbb{Z}_p)$$

takes P to R.

Suppose now that R is anisotropic and consider any $g \in GL(2, \mathbb{Q}_p)$ taking P to R. Let v_1 and v_2 be the columns of g. Since $|P(v_i)|_p = |a_i|_p \leq 1$, then $||v_i||_p \leq 1$ by Lemma 3.3.9. This shows that $||g||_p \leq 1$. □

Later we'll use the following observation.

Lemma 3.3.10. *Consider a prime $p > 2$. There is $k \in GL(2, \mathbb{Z}_p)$ taking x^2+y^2 to $-x^2-y^2$.*

Proof. It suffices to prove there is $(a, b) \in \mathbb{Q}_p^2$ such that $a^2 + b^2 = -1$ and $||(a, b)||_p = 1$, because then

$$k = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in GL(2, \mathbb{Z}_p)$$

works. If -1 is a square in $\mathbb{Q}_p$, we take $a = \sqrt{-1}$ and $b = 0$. If not, we choose $b \in \mathbb{Z} - p\mathbb{Z}$ such that $u = -1 - b^2$ is a square in $\mathbb{Z}_p^\times$ and we set $a = \sqrt{u}$.

□

3.3.3 Ternary quadratic forms

Lemma 3.3.11. *Let $p > 2$ be a prime number. We can write any almost standard quadratic form R on $\mathbb{Q}_p^3$ as $P \circ g$ for a standard quadratic form P and a non-singular $g \in M_3(\mathbb{Z}_p)$*

Proof. We write $R(x) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$, so $a_1, a_2, a_3 \in \mathbb{Z}_p^\times \cup p\mathbb{Z}_p^\times$. Let $\mathtt{C}$ be the natural map $\mathbb{Q}_p^\times \to \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$. We consider two cases.

Case I: $\mathtt{C}(a_ia_j) = \mathtt{C}(-1)$ for some $i \neq j$. Up to a permutation of variables we may suppose that $\mathtt{C}(a_1a_2) = \mathtt{C}(-1)$. Then $R_1(x) = a_1x_1^2+a_2x_2^2$ is $\mathbb{Q}_p$-equivalent to $P_1(x) = x_1^2-x_2^2$. We write $a_3 = c\lambda^2$ with $c \in \mathcal{C}_p$ and $\lambda \in \mathbb{Z}_p^\times$. By Lemma 3.3.7 there is a non-singular $g_1 \in M_2(\mathbb{Z}_p)$ that takes P_1 to R_1. Then $g = g_1 \oplus (\lambda)$ takes P to R.

Case II: $\mathtt{C}(a_ia_j) \neq \mathtt{C}(-1)$ for any $i \neq j$. Consider a diagonal matrix $k \in GL(3, \mathbb{Z}_p)$ such that

$$R'(x) = R \circ k(x) = b_1x_1^2 + b_2x_2^2 + b_3x_3^2$$

with $b_1, b_2, b_3 \in \mathcal{C}_p$. It suffices to prove the result for $R'(x)$. We consider two subcases.

- **Subcase II.1:** $|b_1|_p = |b_2|_p = |b_3|_p$. Then $\mathtt{C}(b_ib_j)$ is $\mathtt{C}(-1)$ or $\mathtt{C}(-\mathtt{n}_p)$ for any $i \neq j$. We assumed that the former case doesn't happen, so $\mathtt{C}(b_ib_j)$ is constant. This implies that $b_1 = b_2 = b_3 = -\mathtt{n}_p$ is a square. By Lemma 3.3.10 there is $k' \in GL(2, \mathbb{Z}_p)$ such that $k_1 = (1) \oplus k'$ takes $R''(x) = b_1(x_1^2 - x_2^2 - x_3^2)$ to R. We are done since R'' falls in Case I.

- **Subcase II.2:** The set $\{b_1, b_2, b_3\}$ meets $\mathbb{Z}_p^\times$ and $p\mathbb{Z}_p^\times$. Suppose first that $b_1, b_2 \in \mathbb{Z}_p^\times$ and $b_3 \in p\mathbb{Z}_p^\times$. Then $\mathtt{C}(b_1b_2) = \mathtt{C}(-\mathtt{n}_p)$. Comparing discriminants we see that $R_1(x) = b_1x_1^2 + b_2x_2^2$ is $\mathbb{Q}_p$-equivalent to $P_1(x) = x_1^2 - \mathtt{n}_px_2^2$ or $P_2(x) = px_1^2 - p\mathtt{n}_px_2^2$. But P_2 doesn't represent 1 nor $\mathtt{n}_p$, so R_1 is $\mathbb{Q}_p$-equivalent to P_1. Then R is $\mathbb{Q}_p$-equivalent to the standard form $P(x) = x_1^2 - \mathtt{n}_px_2^2 + b_3x_3^2$. By Lemma 3.3.7 there is $g_1 \in M_2(\mathbb{Z}_p)$ such that $g = g_1 \oplus (1)$ takes P to R'. When $b_1, b_2 \in p\mathbb{Z}_p^\times$ and $b_3 \in \mathbb{Z}_p^\times$, R_1 is $\mathbb{Q}_p$-equivalent to P_2 and we conclude as before.

□

3.3.4 Quadratic forms in 4 or more variables

Everything is in place to complete the proof of our main result.

Proof of Lemma 3.3.6. We write $R(x) = a_1x_1^2 + \cdots + a_dx_d^2$ with $a_1, \ldots, a_d \in \mathbb{Z}_p^\times \cup p\mathbb{Z}_p^\times$. We proceed by induction on d. The cases $d \leq 3$ are covered by lemmas 3.3.7 and 3.3.11, so suppose that $d \geq 4$. Two things can happen.

Case I: $\mathtt{C}(a_ia_j) = \mathtt{C}(-1)$ for some $i \neq j$. Let $R_1(x) = a_1x_1^2 + a_2x_2^2$ and $R_2(x) = a_3x_3^2 + \cdots + a_dx_d^2$. Up to a permutation of variables we may suppose that R_1 is $\mathbb{Q}_p$-equivalent to $P_1(x) = x_1^2 - x_2^2$. Let P_2 be the standard quadratic form $\mathbb{Q}_p$-equivalent to R_2. Then R is $\mathbb{Q}_p$-equivalent to $P(x) = P_1(x_1, x_2) + P_2(x_3, \ldots, x_d)$, which is standard. By the result for quadratic forms in 2 and $d-2$ variables, there are $g_1 \in M_2(\mathbb{Z}_p)$ and $g_2 \in M_{d-2}(\mathbb{Z}_p)$ such that $g = g_1 \oplus g_2$ takes P to R.

Case II: $\mathtt{C}(a_ia_j) \neq \mathtt{C}(-1)$ for any $i \neq j$. Consider a diagonal matrix $k \in GL(d, \mathbb{Z}_p)$ such that

$$R'(x) = R \circ k(x) = b_1x_1^2 + \cdots + b_dx_d^2$$

for some $b_1, \ldots, b_d \in \mathcal{C}_p$ with $\mathtt{C}(a_i) = \mathtt{C}(b_i)$. If there are three $b_i's$ in either $\mathbb{Z}_p^\times$ or $p\mathbb{Z}_p^\times$, in fact they are equal, so by the argument we used in subcase II.1 of Lemma 3.3.11 there is $k_1 \in GL(d, \mathbb{Z}_p)$ such that $R'' = R' \circ k_1$ falls in Case I (of this proof), and we are done. If this doesn't happen, then $d = 4$. Permuting the variables if necessary we have $b_1, b_2 \in \mathbb{Z}_p^\times$ and $b_3, b_4 \in p\mathbb{Z}_p^\times$. Arguing as in subcase II.2 of Lemma 3.3.11 we see that

$$b_1x_1^2 + b_2x_2^2 \underset{\mathbb{Q}_p}{\sim} x_1^2 - \mathtt{n}_px_2^2 \quad \text{and} \quad b_3x_3^2 + b_4x_4^2 \underset{\mathbb{Q}_p}{\sim} px_3^2 - p\mathtt{n}_px_4^2.$$

By Lemma 3.3.7 there are $g_1, g_2 \in M_2(\mathbb{Z}_p)$ such that $g = g_1 \oplus g_2$ takes the standard anisotropic quadradic form $P(x) = x_1^2 - \mathtt{n}_px_2^2 + px_3^2 - p\mathtt{n}_px_4^2$ to $R'(x)$. This concludes the proof. □

We close this section with a result about orthogonal groups of standard anisotropic quadratic forms.

Lemma 3.3.12. *Consider a prime $p > 2$. Let H_p be the orthogonal group of a standard anisotropic quadratic form on $\mathbb{Q}_p^d$. Then H_p is contained in $GL(d, \mathbb{Z}_p)$.*

Proof. It suffices to prove that $||h||_p \leq 1$ for any $h \in H_p$. Suppose that $H_p = O(P, \mathbb{Q}_p)$ with $P(x) = a_1x_1^2 + \cdots + a_dx_d^2$ standard anisotropic. Arguing as in the proof of Lemma 3.3.9 we see that $||v||_p \leq \sqrt{p}\,|P(v)|_p^{\frac{1}{2}}$ for any $v \in \mathbb{Q}_p^d$. If $v_1, \ldots, v_d$ are the columns of $h \in H_p$, then

$$||v_i||_p \leq \sqrt{p}\,|a_i|_p^{\frac{1}{2}} \leq \sqrt{p},$$

hence $||v_i||_p \leq 1$ and $||h||_p \leq 1$. □

3.4 The *Spin* group

Let ν be a prime and let $G, \widetilde{G}$ and H be groups of $\mathbb{Q}_\nu$-points of Zariski-connected semisimple $\mathbb{Q}_\nu$-groups. A covering—or isogeny—is morphism $H \to G$ with finite kernel and cokernel. We say that $\widetilde{G}$ is simply connected if for any H, any covering $H \to \widetilde{G}$ is an isomorphism. For any G there is a covering $\pi : \widetilde{G} \to G$ with $\widetilde{G}$ simply connected—see [PR94, Theorem 2.6, p. 62]. In this situation we say that $\widetilde{G}$ and $ker\pi$ are respectively the *universal covering* and the *fundamental group* of G. When G is defined over $\mathbb{Q}$, there is also a universal covering of G defined over $\mathbb{Q}$—see [PR94, Proposition 2.10, p. 76].

For example, $SL(d, \mathbb{Q}_\nu)$ is simply connected while $SO(P, \mathbb{Q}_\nu)$ isn't—see [PR94, Proposition 2.15, p. 86]—, where P is a non-degenerate quadratic form on $\mathbb{Q}_\nu^d$, $d \geq 3$. The universal covering of $SO(P, \mathbb{Q}_\nu)$ is the spin group of P, denoted by $Spin(P, \mathbb{Q}_\nu)$. It is constructed using the Clifford algebra of $(\mathbb{Q}_\nu^d, P)$—see [Sch85, Definition 3.4, p. 336]. If P is rational, $Spin(P, \mathbb{Q}_\nu)$ is the group of $\mathbb{Q}_\nu$-points of a $\mathbb{Q}$-group $\mathbf{Spin}(P)$[1], and the covering $\mathbf{Spin}(P) \to \mathbf{SO}(P)$ is defined over $\mathbb{Q}$. We'll denote by $SO(P, \mathbb{Q}_\nu)^\circ$ the image of $Spin(P, \mathbb{Q}_\nu)$ in $SO(P, \mathbb{Q}_\nu)$, which is a finite index subgroup. When $\nu = \infty$, $SO(P, \mathbb{R})^\circ$ is the neutral connected component of $SO(P, \mathbb{R})$.

Later we'll need a representative of small size of any $SO(P, \mathbb{Q}_\nu)^\circ$-coset in $O(P, \mathbb{Q}_\nu)$.

Lemma 3.4.1. *Consider a prime number $p > 2$ and an integer $d \geq 3$. Let H_p be the orthogonal group of a standard isotropic quadratic form on $\mathbb{Q}_p^d$. Any H_p°-coset in H_p has a representative η with $||\eta||_p \leq p$.*

Proof. Let $H_p = O(P, \mathbb{Q}_p)$ where $P(x)$ is an isotropic standard quadratic form on $\mathbb{Q}_p^d$. In particular $P(x)$ starts with $x_1^2 - x_2^2 + \ldots$. First we recall how we can identify in practice the H_p°-cosets of H_p[2]. For any $v \in \mathbb{Q}_p^d$ with $P(v) \neq 0$, let r_v be the reflection with respect to the P-orthogonal complement of v. Recall that these generate H_p. The *spinor norm* of H_p is the unique group morphism $\mathcal{S} : H_p \to \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ such that

$$\mathcal{S}(r_v) = P(v)(\mathbb{Q}_p^\times)^2$$

for every non-isotropic vector $v \in \mathbb{Q}_p^d$—see [Sch85, p. 336]. H_p° is the kernel of the restriction of $\mathcal{S}$ to $SO(P, \mathbb{Q}_p)$, hence two elements of H_p are in the same $H_p^\circ-$coset if and only if they have the same determinant and spinor norm, and in our situation the 8 possibilities occur. There

[1] We'll use boldface to denote abstract linear algebraic k-groups.

[2] The discussion that follows is valid for any non-degenerate quadratic form with coefficients in a field of characteristic $\neq 2$, but we'll stick with the case relevant to us.

is—for any non-degenerate finite dimensional quadratic space over a field of characteristic different from 2—an exact sequence

$$Spin(P,\mathbb{Q}_p) \longrightarrow SO(P,\mathbb{Q}_p) \xrightarrow{\mathcal{S}} \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2.$$

Since P is isotropic and non-degenerate, we even have

$$Spin(P,\mathbb{Q}_p) \longrightarrow SO(P,\mathbb{Q}_p) \xrightarrow{\mathcal{S}} \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \longrightarrow 1.$$

Indeed, consider $e_1 = (1,0,\ldots,0)$ and a non-isotropic vector $v \in \mathbb{Q}_p^d$. Then $r_{e_1}r_v$ is in $SO(P,\mathbb{Q}_p)$ and

$$\mathcal{S}(r_{e_1}r_v) = P(e_1)P(v)(\mathbb{Q}_p^\times)^2 = P(v)(\mathbb{Q}_p^\times)^2.$$

Thus $\mathcal{S}$ is surjective since P represents any element in $\mathbb{Q}_p$—it is isotropic and non-degenerate.

Consider the following system of representatives of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$:

$$\mathcal{C}_p = \{1, \mathtt{n}_p, p, \mathtt{n}_p p\},$$

where $\mathtt{n}_p$ is a non-square $\bmod p$ integer. By Lemma 3.3.8, any $m \in \mathcal{C}_p$ can be expressed as $P(u_m)$ for some $u_m = (\mathtt{a}_m, \mathtt{b}_m, 0, \ldots, 0)$ with $||u_m||_p \leq 1$. It's easy to see that in the four cases we can choose u_m with $||u_m||_p = 1$. The P-orthogonal complement of u_m is generated by

$$v_m = (\mathtt{b}_m, \mathtt{a}_m, 0, \ldots, 0), e_3, \ldots, e_d.$$

The inverse of

$$g_m = (u_m, v_m, e_3, \ldots, e_d) = \begin{pmatrix} \mathtt{a}_m & \mathtt{b}_m \\ \mathtt{b}_m & \mathtt{a}_m \end{pmatrix} \oplus I_{d-2}$$

is

$$g_m^{-1} = \begin{pmatrix} \mathtt{a}_m/m & -\mathtt{b}_m/m \\ -\mathtt{b}_m/m & \mathtt{a}_m/m \end{pmatrix} \oplus I_{d-2}.$$

Hence $||g_m||_p = 1$ and

$$||g_m^{-1}||_p = |m^{-1}|_p \leq p.$$

Let $h_0 = diag(-1,1,\ldots,1)$. The respective matrices of r_{e_1} and r_{u_m} in the standard basis of $\mathbb{Q}_p^d$ are h_0 and $h_m = g_m h_0 g_m^{-1}$. We have

$$||h_m||_p \leq ||g_m||_p ||g_m^{-1}||_p \leq p.$$

The matrices h_m and $h_0 h_m$ with $m \in \mathcal{C}_p$ form a system of representatives of H_p/H_p° verifying the desired condition. □

We'll need a statement like Lemma 3.4.1 also for $p = 2$. As we saw in the proof of that lemma, when the quadratic form P we consider is isotropic, there is a bound for a system of representatives of $O(P,\mathbb{Q}_p)/O(P,\mathbb{Q}_p)^\circ$ that depends only on the respective bound for $P(x) = x_1^2 - x_2^2$.

Lemma 3.4.2. *Let $P(x) = x_1^2 - x_2^2$ and $H_2 = O(P,\mathbb{Q}_2)$. Any H_2°-coset in H_2 has a representative η with $||\eta||_2 \leq 4$.*

Proof. For $v = (a, b) \in \mathbb{Q}_\nu^2$, let $v^\perp = (b, a)$. As in the proof of Lemma 3.4.1, it suffices to see that for any $m \in \mathcal{C}_2$, there is $u_m = (\mathtt{a}_m, \mathtt{b}_m) \in \mathbb{Q}_2^2$ such that $P(u_m) = m$, and such that the matrix h_m in the standard basis of $\mathbb{Q}_2^2$ of the linear map $u_m \mapsto -u_m, u_m^\perp \mapsto u_m^\perp$ verifies $||h_m||_2 \leq 4$. This matrix is

$$h_m = \frac{1}{m}\begin{pmatrix} -(\mathtt{a}_m^2 + \mathtt{b}_m^2) & 2\mathtt{a}_m\mathtt{b}_m \\ -2\mathtt{a}_m\mathtt{b}_m & \mathtt{a}_m^2 + \mathtt{b}_m^2 \end{pmatrix}.$$

One can take:

m	u_m
1	$(1, 0)$
3	$(2, 1)$
2	$(3/2, 1/2)$
6	$(5/2, 1/2)$

For $m \in \{-1, -3, -2, -6\}$ we take $u_m = u_{-m}^\perp$. □

Here the statement for certain diagonal isotropic quadratic forms.

Lemma 3.4.3. *Let $d \geq 2$ and let H_2 be the orthogonal group of a diagonal quadratic form $P(x) = x_1^2 - x_2^2 + a_3x_3^2 + \ldots + a_dx_d^2$ with $a_3, \ldots, a_d \in \mathbb{Q}_2^\times$. Any H_2°-coset in H_2 has a representative η with $||\eta||_2 \leq 4$.*

3.5 Isotropic ternary quadratic forms and SL(2)

Let ν be a prime. We'll explain the connection between $SL(2, \mathbb{Q}_\nu)$ and non-degenerate isotropic quadratic forms on $\mathbb{Q}_\nu^3$. Recall that the adjoint representation of $\mathbf{SL}(2)$ is the linear representation of $\mathbf{SL}(2)$ on its Lie algebra $\mathfrak{sl}(2)$ given by conjugation. It preserves the Killing form $\mathscr{K}$ of $\mathfrak{sl}(2)$, hence it is a morphism $\mathbf{SL}(2) \to \mathbf{SO}(\mathscr{K})$. Note that $\mathscr{K}(x) = 8(x_1x_2 + x_3^2)$ in the basis

$$\beta = \left(e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right)$$

of $mathfraksl(2, \mathbb{Q})$, so in particular $\mathscr{K}$ is $\mathbb{Q}$-isotropic. For any $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Q})$, the matrix of $Ad\, g$ with respect to β is

$$[Ad\, g]_\beta = \begin{pmatrix} a^2 & -b^2 & -2ab \\ -c^2 & d^2 & 2cd \\ -ac & bd & 2bc + 1 \end{pmatrix}. \tag{3.1}$$

The same formulas hold when we replace $\mathbb{Q}$ by $\mathbb{Q}_\nu$. $\mathscr{K}$ is similar to any non-degenerate isotropic quadratic form R on $\mathbb{Q}_\nu^3$, hence writing the adjoint representation of $SL(2, \mathbb{Q}_\nu)$ on an appropriate basis of $\mathfrak{sl}(2, \mathbb{Q}_\nu)$ yields a morphism $SL(2, \mathbb{Q}_\nu) \to SO(R, \mathbb{Q}_\nu)$. For later reference we gather some properties of this morphism when R is standard.

Let's work first with $SL(2, \mathbb{R})$. Consider

$$a_{\infty,t} = \begin{pmatrix} e^{t/2} & 0 \\ 0 & e^{-t/2} \end{pmatrix} \in SL(2, \mathbb{R}), \quad b_{\infty,t} = \begin{pmatrix} \cosh t & \sinh t & 0 \\ \sinh t & \cosh t & 0 \\ 0 & 0 & 1 \end{pmatrix} \in SO(2, 1)$$

Lemma 3.5.1. *There is a covering of Lie groups $\iota_\infty : SL(2,\mathbb{R}) \to SO(2,1)^\circ$ such that $\iota_\infty(a_{\infty,t}) = b_{\infty,t}$.*

Proof. Note that $\mathscr{K}(x) = 8(x_1^2 + x_2^2 - x_3^2)$ in the basis $\beta_1 = (h, e+f, e-f)$ of $\mathfrak{sl}(2,\mathbb{R})$, so the adjoint representation gives a morphism $\iota_\infty : SL(2,\mathbb{R}) \to SO(2,1)^\circ$. From (3.1) we deduce that

$$\iota_\infty(a_{\infty,t}) = \begin{pmatrix} 0 & 0 & 1 \\ 1/2 & 1/2 & 0 \\ 1/2 & -1/2 & 0 \end{pmatrix} \begin{pmatrix} e^t & 0 & 0 \\ 0 & e^{-t} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & -1 \\ 1 & 0 & 0 \end{pmatrix} = b_{\infty,t}.$$

□

Consider now

$$c_{\infty,t} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cosh t & \sinh t \\ 0 & \sinh t & \cosh t \end{pmatrix}.$$

Here is a slight variation of Lemma 3.5.1.

Lemma 3.5.2. *There is a covering of Lie groups $\iota'_\infty : SL(2,\mathbb{R}) \to SO(1,2)^\circ$ such that $\iota'_\infty(a_{\infty,t}) = c_{\infty,t}$.*

Now we'll discuss $SL(2,\mathbb{Q}_p)$. Consider

$$a_{p,m} = \begin{pmatrix} p^m & 0 \\ 0 & p^{-m} \end{pmatrix}$$

for any $m \in \mathbb{Z}$. We'll denote by K_p the group $SL(2,\mathbb{Z}_p)$ and $K_p(n) = ker(K_p \to SL(2,\mathbb{Z}/p^n\mathbb{Z}))$ for $n \geq 1$.

Recall that $SO(P,\mathbb{Q}_p)^\circ$ is the image of $Spin(P,\mathbb{Q}_p) \to SO(P,\mathbb{Q}_p)$—see 3.4.

Lemma 3.5.3. *Consider a prime $p > 2$ and a standard isotropic quadratic form P on $\mathbb{Q}_p^3$. There is a group morphism $\iota_p : SL(2,\mathbb{Q}_p) \to SO(P,\mathbb{Q}_p)^\circ$ with the following properties:*

(i) $||\iota_p(a_{p,m})||_p \leq p^{2m+1}$ *for any integer $m \geq 0$.*

(ii) For every $n \geq 1$, $\iota_p(K_p(n))$ is contained in the kernel of $SL(3,\mathbb{Z}_p) \to SL(3,\mathbb{Z}/p^{n-1}\mathbb{Z})$.

We'll use the next easy result to prove Lemma 3.5.3

Lemma 3.5.4. *Let $p > 2$ be a prime number. Consider $\mathscr{K}(x) = 8(xy + z^2)$ and an isotropic standard quadratic form P on $\mathbb{Q}_p^3$. There is $g \in GL(3,\mathbb{Q})$ such that $\mathscr{K} \circ g$ is a multiple of P, $||g||_p \leq p$ and $||g^{-1}||_p \leq 1$.*

Proof. Note that $P(x) = x_1^2 - x_2^2 + cx_3^2$ for some $c \in \mathcal{C}_p$ and that $|c^{-1}|_p \leq p$. The matrix

$$g = \begin{pmatrix} c^{-1} & -c^{-1} & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

takes $\mathscr{K}$ to $\frac{8}{c}P$. Its inverse is

$$g^{-1} = \begin{pmatrix} c/2 & 1/2 & 0 \\ -c/2 & 1/2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We readily see that $||g||_p \leq p$ and $||g^{-1}||_p \leq 1$. □

Proof of Lemma 3.5.3. Recall that $\mathscr{K}(x) = 8(xy + z^2)$ in the basis $\beta = (e, f, h)$ of $\mathfrak{sl}(2, \mathbb{Q}_p)$. By Lemma 3.5.4, there is $g_0 \in GL(3, \mathbb{Q})$ such that $\mathscr{K} \circ g_0$ is a multiple of P, $||g_0||_p \leq p$ and $||g_0^{-1}||_p \leq 1$. We define $\iota_p : SL(2, \mathbb{Q}_p) \to SO(P, \mathbb{Q}_p)$ as

$$\iota_p(g) = g_0^{-1}[Ad\, g]_\beta g_0.$$

Let's see that ι_p has the claimed properties.

Since g_0 is a rational matrix, ι defines a morphism of $\mathbb{Q}$-groups $\mathbf{SL}(2) \to \mathbf{SO}(P)$ with finite kernel. $\mathbf{SL}(2)$ is a simply connected $\mathbb{Q}$-group—see [PR94, p. 63]—, so by the uniqueness of the universal covering there is an isomorphism of $\mathbb{Q}$-groups $\psi : \mathbf{SL}(2) \to \mathbf{Spin}(P)$ such that the diagram

$$\begin{array}{ccc} \mathbf{SL}(2) & \xrightarrow{\quad\psi\quad} & \mathbf{Spin}(P) \\ & \searrow \quad \swarrow & \\ & \mathbf{SO}(P) & \end{array}$$

commutes—see [PR94, Proposition 2.10, p. 76]. Taking the $\mathbb{Q}_p$-points we see that the image of ι_p is indeed $SO(P, \mathbb{Q}_p)^\circ$.

From (3.1) we see that $[Ad\, a_{p,m}]_\beta = diag(p^{2m}, p^{-2m}, 1)$. Then

$$||\iota_p(a_{p,m})||_p \leq ||g_0^{-1}||_p \, ||[Ad\, a_{p,m}]_\beta||_p \, ||g_0||_p \leq p^{2m+1},$$

which proves (i).

Let's prove (ii). We have

$$[Ad\, g]_\beta - I_3 = \begin{pmatrix} (a-1)(a+1) & -b^2 & -2ab \\ -c^2 & (d-1)(d+1) & 2cd \\ -ac & bd & 2bc \end{pmatrix}.$$

If $g \in K_p(n)$, then $||[Ad\, g]_\beta - I_3||_p \leq p^{-n}$ since $a-1, b, c, d-1$ are in $p^n\mathbb{Z}_p$. Hence

$$||\iota_p(g) - I_3||_p \leq ||g_0^{-1}||_p \, ||[Ad\, g]_\beta - I_3||_p \, ||g_0||_p \leq p^{-(n-1)},$$

so we are done.

□

Corollary 3.5.5. *Consider a prime number $p > 2$ and an integer $d \geq 3$. Let H_p be the orthogonal group of a standard isotropic quadratic form on $\mathbb{Q}_p^d$. There is a morphism with finite kernel $\rho : SL(2, \mathbb{Q}_p) \to H_p^\circ$ with the following properties:*

(*i*) $||\rho(a_{p,m})||_p \leq p^{2m+1}$ *for any* $m \geq 0$,

(*ii*) $\rho(K_p(n))$ *is contained in* $ker(SL(d,\mathbb{Z}_p) \to SL(d,\mathbb{Z}/p^{n-1}\mathbb{Z}))$ *for every* $n \geq 1$.

Proof. Suppose that H_p is the orthogonal group of the standard isotropic form P on $\mathbb{Q}_p^d$. P is of the form

$$P(x) = x_1^2 - x_2^2 + a_3x_3^2 + \ldots + a_dx_d^2.$$

Note that $P_1(x) = x_1^2 - x_2^2 + a_3x_3^2$ is standard isotropic. We define ρ as the composition

$$SL(2,\mathbb{Q}_p) \xrightarrow{\iota_p} SO(P_1,\mathbb{Q}_p)^\circ \xrightarrow{\varphi} H_p^\circ,$$

with ι_p as in Lemma 3.5.3 and, for any $h \in SO(P_1,\mathbb{Q}_p)^\circ$, $\varphi(h)$ acts on $V = \mathbb{Q}_pe_1 \oplus \mathbb{Q}_pe_2 \oplus \mathbb{Q}_pe_3$ as h and as the identity on $\mathbb{Q}_pe_4 \oplus \cdots \oplus \mathbb{Q}_pe_d$. The claimed properties follow from Lemma 3.5.3. □

Chapter 4

Decay of coefficients of unitary representations

In this chapter we introduce the tools we'll need from the theory of unitary representations of semisimple groups. Our motivation is the unitary representation that arises from a measure-preserving dynamical system, that we discuss in Section 4.1. We'll explain how an estimate of the decay of the coefficients of this representation implies a mixing speed of the underlying dynamical system. In the three remaining sections we cite the results for $\mathbf{SL}(2)$ that we'll need.

4.1 Basic definitions and motivation

If $\mathcal{H}$ is a Hilbert space—always assumed to be complex—, we denote by $U(\mathcal{H})$ the group of unitary transformations of $\mathcal{H}$. A unitary representation of a locally compact group G on $\mathcal{H}$ is a group morphism $\pi : G \to U(\mathcal{H})$ such that $g \mapsto \pi(g)v$ is continuous for any $v \in \mathcal{H}$.

Let π be a unitary representation of G. We'll often denote by $\mathcal{H}_\pi$ the Hilbert space of π. For $v, w \in \mathcal{H}_\pi$, the map $g \mapsto \langle \pi(g)v, w\rangle$ is the *coefficient of v and w*. When $v = w$ we call it the *diagonal coefficient of v*. The unitary representations π_1 and π_2 of G are *unitary equivalent* if there is a G-equivariant bijective isometry $\mathcal{H}_{\pi_1} \to \mathcal{H}_{\pi_2}$.

We say that π is irreducible if 0 and $\mathcal{H}_\pi$ are the only G-invariant closed subspaces of $\mathcal{H}_\pi$. The set of equivalence classes of unitary representations of G, denoted by $\widehat{G}$, is known as the *unitary dual of G*. We denote by $[\pi]$ the unitary equivalence class π. A unitary representation σ of G is weakly contained in π if any diagonal coefficient of σ can be approximated uniformly on compact subsets by finite sums of diagonal coefficients of π. The support $supp\,\pi$ of π consists of the $[\sigma] \in \widehat{G}$ weakly contained in π.

Here is the important example of unitary representation that justifies the existence of this chapter: Let Y be a topological space endowed with a finite Borel measure μ. Suppose that α is a measure-preserving, continuous action of a locally compact group G on Y. The formula

$$\pi_\alpha(g)f(y) = f(\alpha(g^{-1})y)$$

defines a unitary representation π_α of G on $L^2(Y, \mu)$. Recall that α is mixing if for any

$\varphi, \psi \in L^2(Y)$,

$$\lim_{g\to\infty} \langle \pi_\alpha(g)\varphi, \psi\rangle = \frac{1}{\mu(Y)} \int_Y \varphi \mathrm{d}\mu \int_Y \overline{\psi}\mathrm{d}\mu.$$

The fact that α is mixing can be reformulated in terms of certain coefficients of π_α. Note that

$$L^2_0(Y) = \left\{ f \in L^2(Y) \mid \int_Y f \mathrm{d}\mu = 0 \right\}$$

is a G-invariant closed subspace of $L^2(Y)$. We denote π°_α the restriction of π_α to $L^2_0(Y)$. The orthogonal projection of $\varphi \in L^2(Y)$ to $L^2_0(Y)$ is $\varphi_0 = \varphi - \frac{1}{\mu(Y)} \int_Y \varphi \mathrm{d}\mu$ and

$$\langle \pi^\circ_\alpha(g)\varphi_0, \psi_0\rangle = \langle \pi_\alpha(g)\varphi, \psi\rangle - \frac{1}{\mu(Y)} \int_Y \varphi \mathrm{d}\mu \int_Y \overline{\psi}\mathrm{d}\mu.$$

This means that α is mixing if an only if any coefficient of π°_α vanishes at ∞. To obtain effective results about quadratic forms, we'll need to estimate the error term

$$\left| \langle \pi_\alpha(g)\varphi, \psi\rangle - \frac{1}{\mu(Y)} \int_Y \varphi \mathrm{d}\mu \int_Y \overline{\psi}\mathrm{d}\mu \right|$$

in terms of g. In other words, we want to know how fast the coefficients of π°_α decay.

4.2 Effective decay of coefficients

The result on the decay of coefficients we'll use applies to a family of unitary representations that verify an integrability condition that we explain now.

Let $k \in [2, \infty)$. A unitary representation π of G—again, a locally compact group—is almost L^k if there is a dense subset $\mathscr{D}$ of $\mathcal{H}_\pi$ such that the coefficient of any two vectors in $\mathscr{D}$ is an $L^{k+\varepsilon}$ function on G for any $\varepsilon > 0$—see the article [Sha00, p. 125] of Y. Shalom for a discussion of this concept.

The case $k = 2$ is particularly important. A unitary representation of G is *tempered* if and only if it is weakly contained in $L^2(G)$. There is a close connection between tempered and almost L^2 unitary representations: A result—[CHH88, Theorem 1]—of Cowling, Haagerup and Howe says that any almost L^2 unitary representation of a locally compact group G is tempered. Conversely, they show—[CHH88, Theorem 2]—that any tempered unitary representation is almost L^2 when G is the group of $\mathbb{Q}_\nu$-points of a semisimple linear $\mathbb{Q}_\nu$-group [1]. They achieve this by proving there is a dense subset $\mathscr{D}$ of $\mathcal{H}_\pi$ such that the coefficient of any $v, w \in \mathscr{D}$ decays at least as fast as the so-called *Harish-Chandra spherical function of* G, which is known to be in $L^{2+\varepsilon}(G)$ for any $\varepsilon > 0$. In the next section we'll define the Harish-Chandra function of $SL(2, \mathbb{Q}_\nu)$.

From now on we focus in the theory for $\mathbf{SL}(2)$, which is enough for our needs. We denote by $K_{2,p}$ the group $SL(2, \mathbb{Z}_p)$ and $K_{2,\infty} = SO(2, \mathbb{R})$. The Harish-Chandra function of $SL(2, \mathbb{Q}_\nu)$ is the map $\Xi_\nu : SL(2, \mathbb{Q}_\nu) \to [0, 1]$ given by

$$\Xi_\nu(g) = \int_{K_{2,\nu}} ||gke_1||^{-1} \mathrm{d}k,$$

[1] Since we work with othogonal groups of quadratic forms in at least 3 variables, for us *almost* L^2 and *tempered* are interchangeable terms.

where $||\cdot||$ is $||\cdot||_\nu$ when $\nu < \infty$, and the standard euclidean norm $||\cdot||_{euc}$ of $\mathbb{R}^2$ when $\nu = \infty$. We integrate with respect to the Haar probability measure on $K_{2,\nu}$. If π is a unitary representation of $SL(2,\mathbb{Q}_\nu)$ and $v \in \mathcal{H}_\pi$, we denote by $\delta_\nu(v)$ the square-root of the dimension of the $\mathbb{C}$-linear span of $\pi(K_{2,\nu})v$. We say that v is $K_{2,\nu}$-finite if and only if $\delta_\nu(v) < \infty$. The next result—which is a particular case of [CHH88, Theorem 2]—tells us that the coefficients of $K_{2,\nu}$-finite vectors decay at least as fast as Ξ_ν.

Theorem 4.2.1 (Cowling, Haagerup, Howe)**.** *Consider a prime ν. Let π be a tempered unitary representation of $SL(2,\mathbb{Q}_\nu)$. For any $v_1, v_2 \in \mathcal{H}_\pi$ we have*

$$|\langle \pi(g)v_1, v_2\rangle| \leq \Xi_\nu(g)||v_1||\,||v_2||\delta_\nu(v_1)\delta_\nu(v_2),$$

for any $g \in SL(2,\mathbb{Q}_\nu)$.

In Chapter 6 we'll need a decay speed for the larger family of $K_{2,\infty}$-smooth vectors of unitary representations of $SL(2,\mathbb{R})$. A vector $v \in \mathcal{H}_\pi$ is $K_{2,\infty}$-smooth if the map $K_{2,\infty} \to \mathcal{H}_\pi, k \mapsto \pi(k)v$ is smooth. Consider the matrix

$$\mathcal{Z} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

in the Lie algebra of $K_{2,\infty}$. If $v \in \mathcal{H}_\pi$ is $K_{2,\infty}$-smooth, we define its first Sobolev norm as $||v||_{\mathcal{Z}} = (||v||^2 + ||\pi(\mathcal{Z})v||^2)^{\frac{1}{2}}$, where

$$\pi(\mathcal{Z})v = \frac{\mathrm{d}}{\mathrm{d}t}\Big|_{t=0} \pi(e^{t\mathcal{Z}})v.$$

Lemma 4.2.2. *Let π be an almost L^{2k} unitary representation of $SL(2,\mathbb{R})$, where k is a positive integer. For any $K_{2,\infty}$-smooth vectors $v_1, v_2 \in \mathcal{H}_\pi$ and any $g \in SL(2,\mathbb{R})$ we have*

$$|\langle \pi(g)v_1, v_2\rangle| \leq 5\,\Xi_\infty^{\frac{1}{k}}(g)||v_1||_{\mathcal{Z}}||v_2||_{\mathcal{Z}}.$$

Proof. Note that $\pi^{\otimes k}$ is tempered because the coefficient of $v_1 \otimes \cdots \otimes v_k$ and $w_1 \otimes \cdots \otimes w_k$ is the product of k coefficients of π. Consider $v, w \in \mathcal{H}_\pi$. Applying Theorem 4.2.1 to $\pi^{\otimes k}$ we obtain

$$\begin{aligned} |\langle \pi(g)v, w\rangle|^k &= |\langle \pi^{\otimes k}(g)v^{\otimes k}, w^{\otimes k}\rangle| \\ &\leq \Xi_\infty(g)||v^{\otimes k}||\,||w^{\otimes k}||\delta_\infty(v^{\otimes k})\delta_\infty(w^{\otimes k}) \\ &\leq \Xi_\infty(g)(||v||\,||w||\delta_\infty(v)\delta_\infty(w))^k, \end{aligned}$$

so

$$|\langle \pi(g)v, w\rangle| \leq \Xi_\infty^{\frac{1}{k}}(g)||v||\,||w||\delta_\infty(v)\delta_\infty(w).$$

Let $r_\theta \in K_{2,\infty}$ be the rotation of angle θ. To obtain the inequality for $K_{2,\infty}$-smooth vectors we decompose $\mathcal{H}_\pi$ as Hilbert sum of $K_{2,\infty}$-invariant subspaces

$$\mathcal{H}_\pi = \widehat{\bigoplus_{m\in\mathbb{Z}}} \mathcal{H}_m,$$

where $K_{2,\infty}$ acts on $\mathcal{H}_m$ by $\pi(r_\theta)v_m = e^{im\theta}v_m$. Note that $e^{\theta\mathcal{Z}} = r_\theta$[2], so

$$\pi(\mathcal{Z})v_m = \frac{\mathrm{d}}{\mathrm{d}\theta}\Big|_{\theta=0} e^{im\theta}v_m = imv_m.$$

Consider a $K_{2,\infty}$-smooth $v = \sum_{m\in\mathbb{Z}} v_m$ with $v_m \in \mathcal{H}_m$. We have $\pi(\mathcal{Z})v = \sum_{m\in\mathbb{Z}} imv_m$, so

$$||\pi(\mathcal{Z})v||^2 = \sum_{m\in\mathbb{Z}} m^2||v_m||^2.$$

Consider a second $K_{2,\infty}$-smooth vector $w = \sum_{n\in\mathbb{Z}} w_n$. To obtain the bound for $\langle\pi(g)v, w\rangle$ we use the Cauchy-Schwarz inequality as follows:

$$\begin{aligned}
|\langle\pi(g)v, w\rangle| &\leq \sum_{m,n\in\mathbb{Z}} |\langle\pi(g)v_m, w_n\rangle| \\
&\leq \Xi_\infty^{\frac{1}{k}}(g) \left(\sum_{m\in\mathbb{Z}} ||v_m||\right)\left(\sum_{n\in\mathbb{Z}} ||w_n||\right) \\
&= \Xi_\infty^{\frac{1}{k}}(g) \left(||v_0|| + \sum_{m\in\mathbb{Z}-\{0\}} \frac{1}{m}||mv_m||\right)\left(||w_0|| + \sum_{n\in\mathbb{Z}-\{0\}} \frac{1}{n}||nw_n||\right) \\
&\leq (1+2\zeta(2))\,\Xi_\infty^{\frac{1}{k}}(g)\left(||v_0||^2 + ||\pi(\mathcal{Z})v||^2\right)^{\frac{1}{2}}\left(||w_0||^2 + ||\pi(\mathcal{Z})w||^2\right)^{\frac{1}{2}} \\
&\leq 5\,\Xi_\infty(g)^{\frac{1}{k}}||v||_{\mathcal{Z}}||w||_{\mathcal{Z}}.
\end{aligned}$$

□

For Chapter 7, we need a decay speed of coefficients of vectors fixed by small compact-open subgroups of $SL(2,\mathbb{Q}_p)$, that we achieve in Corollary 4.3.7. In the proof we'll use the next two lemmas. For any positive integer n we denote by $K_{2,p}(n)$ the kernel of the natural map $K_{2,p} \to SL(2,\mathbb{Z}/p^n\mathbb{Z})$. Let π be a unitary representation of $SL(2,\mathbb{Q}_p)$. A vector $v \in \mathcal{H}_\pi$ invariant under some $K_{2,p}(n)$ is $K_{2,p}$-finite, and the next result gives an upper bound of $\delta_p(v)$.

Lemma 4.2.3. *For any positive integer n we have*

$$\#SL(2,\mathbb{Z}/p^n\mathbb{Z}) = p^{3n} - p^{3n-2}.$$

Proof. Let A_n be a free $(\mathbb{Z}/p^n\mathbb{Z})$-module with basis (e_1, e_2). The $SL(2,\mathbb{Z}/p^n\mathbb{Z})$-orbit of e_1 has size $p^{2n} - p^{2n-2}$ because it consists of the elements $x_1e_1 + x_2e_2$ of A_n such that p does not divide x_1 and x_2 simultaneously. The stabilizer of e_1 in $SL(2,\mathbb{Z}/p^n\mathbb{Z})$ is

$$S_n := \begin{pmatrix} 1 & \mathbb{Z}/p^n\mathbb{Z} \\ 0 & 1 \end{pmatrix}.$$

Thus

$$\#SL(2,\mathbb{Z}/p^n\mathbb{Z}) = \#(SL(2,\mathbb{Z}/p^n\mathbb{Z})e_1)\,\#S_n = p^{3n} - p^{3n-2}, \tag{4.1}$$

as claimed. □

[2]An easy way to see this is with the standard identification of $\mathbb{C}$ with the matrices $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, a, b \in \mathbb{R}$. Note that i corresponds to $\mathcal{Z}$.

Here is a more explicit decay of coefficients of $K_{2,p}(n)$-fixed vectors.

Lemma 4.2.4. *Let π be a tempered unitary representation of $SL(2,\mathbb{Q}_p)$. If $v_1, v_2 \in \mathcal{H}_\pi$ are respectively $K_{2,p}(n_1)$ and $K_{2,p}(n_2)$-invariant, then*

$$|\langle \pi(g)v_1, v_2\rangle| \leq p^{\frac{3}{2}(n_1+n_2)}\Xi_p(g)||v_1||\,||v_2||$$

for any $g \in SL(2,\mathbb{Q}_p)$.

Proof. Note that $\pi(K_{2,p})v_i$ has at most $[K_{2,p} : K_{2,p}(n_i)] = \#SL(2,\mathbb{Z}/p^{n_i}\mathbb{Z})$ elements because v_i is $K_{2,p}(n_i)$-invariant. Then, by Lemma 4.2.3 we have

$$\delta_p(v_i) \leq (\#SL(2,\mathbb{Z}/p^{n_i}\mathbb{Z}))^{\frac{1}{2}} < p^{\frac{3}{2}n_i}.$$

From Theorem 4.2.1 we deduce that

$$\begin{aligned}|\langle \pi(g)v_1, v_2\rangle| &\leq \Xi_p(g)||v_1||\,||v_2||\delta_p(v_1)\delta_p(v_2)\\ &\leq p^{\frac{3}{2}(n_1+n_2)}\Xi_p(g)||v_1||\,||v_2||,\end{aligned}$$

for any $g \in SL(2,\mathbb{Q}_p)$. □

4.3 The Harish-Chandra function of $SL(2)$

The purpose of this section is to give estimates of the decay of Ξ_ν. Before that, we explain briefly how Ξ_ν arises as a coefficient of an important irreducible unitary representation of $SL(2,\mathbb{Q}_\nu)$. To lighten the notation, in this section we denote $G_\nu = SL(2,\mathbb{Q}_\nu)$ and $K_\nu = K_{2,\nu}$. Let B_ν be the subgroup of upper-triangular matrices of G_ν. We define $a_{p,m} = diag(p^m, p^{-m})$ and $a_{\infty,t} = diag(e^{\frac{t}{2}}, e^{-\frac{t}{2}})$ for $m \in \mathbb{Z}$ and $t \in \mathbb{R}$. Consider

$$A_p^+ = \{a_{p,m} \mid m \in \mathbb{N}\} \quad \text{and} \quad A_\infty^+ = \{a_{\infty,t} \mid t \geq 0\}.$$

For any irreducible unitary representation σ of G_ν, the subspace of K_ν-invariant vectors $\mathcal{H}_\sigma^{K_\nu}$ is either trivial or a line—see [Lub94, Proposition 5.1.4, p. 63]. In the latter case we say that σ is a *spherical* or *class-one irreducible unitary representation* of G_ν. Suppose that σ is spherical and let v be a unit vector of $\mathcal{H}_\sigma^{K_\nu}$. The diagonal coefficient $c_v : g \mapsto \langle \sigma(g)v, v\rangle$ of v is the a *spherical function* of σ[3]. The unitary representation σ_ν of G_ν induced by the trivial representation of B_ν is irreducible and class-one—see [Lub94, Theorem 5.1.7, p. 64]. Its spherical function is the Harish-Chandra function Ξ_ν of G_ν.

As Ξ_ν is K_ν bi-invariant, its decay speed depends only on the values it takes on A_ν^+, since $G_\nu = K_\nu A_\nu^+ K_\nu$ according to the *Cartan decomposition of* G_ν.

[3]Let $C_c(G_\nu//K_\nu)$ be the space of continuous K_ν bi-invariant functions $G_\nu \to \mathbb{C}$ with compact support. A function $F : G_\nu \to \mathbb{C}$ is spherical if it verifies the next three conditions:

(I) F is continuous and K_ν bi-invariant.

(II) $F(I_2) = 1$.

(III) For any $\varphi \in C_c(G_\nu//K_\nu)$, $F * \varphi = \eta_F(\varphi)F$ for some $\eta_F(\varphi) \in \mathbb{C}$.

The classification of class-one irreducible unitary representations of G_ν is equivalent to the classification of positive definite spherical functions of G_ν—see [Lan85, Theorem 9, p. 65].

4.3.1 Decay speed of Ξ_∞

Let $r_\theta \in K_\infty$ be the rotation of angle θ. The map $\theta \mapsto r_\theta$ is a parametrization $[0, 2\pi) \to K_\infty$, and λ_{K_∞} is simply $(2\pi)^{-1}\frac{\mathrm{d}}{\mathrm{d}\theta}$. Thus

$$\begin{aligned}\Xi_\infty(a_{\infty,t}) &= \frac{1}{2\pi}\int_0^{2\pi} ||a_{\infty,t} r_\theta e_1||_{euc}^{-1} \mathrm{d}\theta \\ &= \frac{1}{2\pi}\int_0^{2\pi} \left(e^t \cos^2\theta + e^{-t}\sin^2\theta\right)^{-\frac{1}{2}} d\theta.\end{aligned}$$

The next lemma describes the behavior of $\Xi_\infty(a_{\infty,t})$ for big t. See [HT92, p. 236] for a proof.

Lemma 4.3.1. *The functions $t \mapsto \Xi_\infty(a_{\infty,t})$ and $t \mapsto te^{-\frac{t}{2}}$ are equivalent as $t \to \infty$.*

For our purposes it will be convenient to dispose of an exponential upper bound of $\Xi_\infty(a_{\infty,t})$. The next corollary is immediate from Lemma 4.3.1.

Corollary 4.3.2. *There is a positive constant $\mathcal{D}_1$ such that $\Xi_\infty(a_{\infty,t}) \leq \mathcal{D}_1 e^{-\frac{t}{3}}$.*

Combining Corollary 4.3.2 and Lemma 4.2.2 we get a decay estimate along A_∞^+ for coefficients of K_∞-smooth vectors.

Corollary 4.3.3. *Let π be an almost L^{2m} unitary representation of $SL(2,\mathbb{R})$, with m a positive integer. For any $K_{2,\infty}$-smooth vectors $v_1, v_2 \in \mathcal{H}_\pi$ we have*

$$|\langle \pi(a_{\infty,t})v_1, v_2\rangle| \leq e^{-\frac{t}{3m}}(5\mathcal{D}_1^{\frac{1}{m}}||v_1||_{\mathcal{Z}}||v_2||_{\mathcal{Z}})$$

for $t \geq 0$.

4.3.2 Decay speed of Ξ_p

This time we'll obtain an explicit formula of $\Xi_p(a_{p,m})$, which easily implies an exponential decay of Ξ_p along A_p^+.

Lemma 4.3.4. *For any prime p and any integer $m \geq 0$ we have*

$$\Xi_p(a_{p,m}) = \frac{p^{-m}}{p+1}((2m+1)(p-1)+2).$$

To compute $\Xi_p(a_{p,m})$ we'll use a well-adapted measurable partition of K_p. For any integer $n \geq 0$ we define

$$F_n = \left\{(k_{ij}) \in K_p \mid |k_{11}|_p = p^{-n}, |k_{21}|_p = 1\right\}$$

and

$$F_{-n} = \left\{(k_{ij}) \in K_p \mid |k_{11}|_p = 1, |k_{21}|_p = p^{-n}\right\}.$$

As usual, we denote by λ_H a Haar measure of a locally compact group H. When H is compact we take the Haar probability measure.

Lemma 4.3.5. *The subset $\bigcup_{n\in\mathbb{Z}} F_n$ of K_p has full measure and*

$$\lambda_{K_p}(F_n) = \frac{p-1}{p+1}p^{-|n|} \tag{4.2}$$

for any $n \in \mathbb{Z}$.

Proof. Let (e_1, e_2) be the standard basis of $V = \mathbb{Q}_p^2$. We denote by Ψ be the map $k \mapsto ke_1$ from K_p to the unit sphere $\mathbb{S}_V$ of V. Note that $\mu = \Psi_*\lambda_{K_p}$ is the unique K_p-invariant probability measure on $\mathbb{S}_V$, thus

$$\mu(A) = \lambda_V(\mathbb{Z}_p A), \tag{4.3}$$

for any measurable subset A of $\mathbb{S}_V$. Consider $C_n = \Psi(F_n)$. Then

$$\lambda_{K_p}(F_n) = \mu(C_n),$$

since $F_n = \Psi^{-1}(C_n)$. Note that $\bigcup_{n\in\mathbb{Z}} C_n$ is conull in $\mathbb{S}_V$ because it consists of the points $(x_1, x_2) \in \mathbb{S}_V$ with $x_1 \neq 0 \neq x_2$. Since $C_n = diag(p^n, 1)C_0$ for any $n \geq 0$, from (4.3) we get

$$\mu(C_n) = \left|\det \begin{pmatrix} p^n & 0 \\ 0 & 1 \end{pmatrix}\right|_p \mu(C_0) = p^{-n}\mu(C_0).$$

In the same way one shows that $\mu(C_n) = p^{-|n|}\mu(C_0)$ for any $n \in \mathbb{Z}$. Thus

$$1 = \mu(\mathbb{S}_V) = \sum_{n\in\mathbb{Z}} \mu(C_n) = \frac{p+1}{p-1}\mu(C_0),$$

so

$$\lambda_{K_p}(F_n) = \mu(C_n) = \frac{p-1}{p+1}p^{-|n|}$$

for any $n \in \mathbb{Z}$. □

Let's prove the formula of $\Xi_p(a_{p,m})$.

Proof of Lemma 4.3.4. From the definition of F_n we easily see that

$$||a_{p,m}ke_1||_p^{-1} = \begin{cases} p^m & \text{if } n \leq -2m, \\ p^{-m-n} & \text{if } -2m < n < 0, \\ p^{-m} & \text{if } n \geq 0, \end{cases}$$

for $k \in F_n$ and $m \geq 0$. Then

$$\begin{aligned}
\Xi_p(a_{p,m}) &= \sum_{n\in\mathbb{Z}} \int_{F_n} ||a_{p,m}ke_1||_p^{-1} \mathrm{d}\lambda_{K_p}(k) \\
&= \left(\sum_{n\leq -2m} \lambda_{K_p}(F_n)\right) p^m + \sum_{-2m<n<0} \lambda_{K_p}(F_n) p^{-m-n} + \left(\sum_{n\geq 0} \lambda_{K_p}(F_n)\right) p^{-m} \\
&= \frac{p-1}{p+1}\left[\sum_{n\leq -2m} p^{m+n} + \sum_{-2m<n<0} p^{-m} + \sum_{n\geq 0} p^{-m-n}\right] \\
&= \frac{(p-1)p^{-m}}{p+1}\left[\sum_{\ell\leq 0} p^{\ell} + (2m-1) + \sum_{n\geq 0} p^{-n}\right] \\
&= \frac{(p-1)p^{-m}}{p+1}\left[\frac{2}{1-p^{-1}} + 2m - 1\right] \\
&= \frac{p^{-m}}{p+1}((2m+1)(p-1)+2),
\end{aligned}$$

as we wanted. □

Here is the exponential bound of Ξ_p we'll use in practice.

Corollary 4.3.6. *For any prime number p we have*

$$\Xi_p(a_{p,m}) < 10p^{-\frac{m}{2}}$$

for $m \geq 1$.

Proof. Note that

$$\begin{aligned}
\Xi_p(a_{p,m}) &= \frac{1}{p^m}\left((2m+1)\frac{p-1}{p+1} + \frac{2}{p+1}\right) \\
&\leq \frac{1}{p^m}\left(\left(2 - \frac{4}{p+1}\right)m + 1\right) \leq 3\frac{m}{p^m},
\end{aligned}$$

and $\frac{m}{p^m} < \frac{2}{\log 2} p^{-\frac{m}{2}}$ [4]. Thus

$$\Xi_p(a_{p,m}) < \frac{6}{\log 2} p^{-\frac{m}{2}} < 10p^{-\frac{m}{2}}.$$

□

Using Corollary 4.3.6 in Lemma 4.2.4 we obtain the next decay speed of coefficients.

Corollary 4.3.7. *Let π be a tempered unitary representation of $SL(2,\mathbb{Q}_p)$. Suppose that $v_1, v_2 \in \mathcal{H}_\pi$ are respectively $K_{2,p}(n_1)$ and $K_{2,p}(n_2)$-invariant. Then*

$$|\langle \pi(a_{p,m})v_1, v_2\rangle|_\infty \leq p^{-\frac{m}{2}}(10p^{\frac{3}{2}(n_1+n_2)}||v_1||\,||v_2||),$$

for any $m \geq 1$.

[4] Indeed:

$$\frac{p^{m/2}}{m} \geq \frac{2^{m/2}}{m} > \frac{1+\frac{\log 2}{2}m}{m} > \frac{\log 2}{2}.$$

Chapter 5

Effective criteria of $\mathbb{Z}_S$-equivalence

In this chapter we are interested in a slight generalization of the classical *problem of $\mathbb{Z}$-equivalence of integral quadratic forms*, which consists deciding if two given integral quadratic forms are $\mathbb{Z}$-equivalent. Gauss describes in [Gau65] an algorithm that solves the problem for binary quadratic forms. Unfortunately, it is hard to extend it to quadratic forms in 3 or more variables. An amazing contribution to the problem of $\mathbb{Z}$-equivalence is the following elegant result of Li and Margulis—see [LM16, Theorem 1]. The statement we present here is less sharp, but easier to read.

Theorem 5.0.1. *Let Q_1 and Q_2 be non-degenerate integral quadratic forms in $d \geq 3$ variables. If Q_1 and Q_2 are $\mathbb{Z}$-equivalent, there is $\gamma_0 \in GL(d,\mathbb{Z})$ with*

$$||\gamma_0||_\infty \leq A_d(||Q_1||_\infty ||Q_2||_\infty)^{\frac{13}{40}d^3} \tag{5.1}$$

such that $Q_1 \circ \gamma_0 = Q_2$.

Here A_d is a positive constant that depends only on d, and $||\gamma_0||_\infty, ||Q_i||_\infty$ are respectively the maximum of the absolute values of the entries of γ_0 and the coefficients of Q_i. Theorem 5.0.1 gives an effective criterion to decide if Q_1 and Q_2 as in the statement are $\mathbb{Z}$-equivalent: one checks if the equation $Q_1 \circ \gamma_0 = Q_2$ has a solution in the **finite** subset of $GL(d,\mathbb{Z})$ determined by (5.1). We'll sometimes refer to Theorem 5.0.1 as the *$\mathbb{Z}$-equivalence criterion of Li and Margulis*. The goal of this chapter is to obtain an effective criterion of $\mathbb{Z}[1/n]$-equivalence of quadratic forms.

Before going further we give an alternate description of the ring $\mathbb{Z}[1/n]$ and we introduce new notation. The ring $\mathbb{Z}[1/n]$ depends only on the prime divisors $p_1, \cdots, p_k$ of n because its consists of the rational numbers with denominator of the form $p_1^{a_1} \cdots p_k^{a_k}$ with $a_1, \ldots, a_k \in \mathbb{N}$. Thus it is natural to introduce, for any finite set $S_f = \{p_1, \ldots, p_k\}$ of primes, $S = \{\infty\} \cup S_f$—we'll explain in a moment why we add ∞—and the *ring of S-integers*

$$\mathbb{Z}_S = \left\{ \frac{m}{p_1^{a_1} \cdots p_k^{a_k}} \mid m \in \mathbb{Z}, a_1, \cdots, a_k \in \mathbb{N} \right\},$$

with the convention $\mathbb{Z}_{\{\infty\}} = \mathbb{Z}$. We denote by p_S the product of the primes in S_f, setting $p_{\{\infty\}} = 1$. The product ring $\prod_{\nu \in S} \mathbb{Q}_\nu$ will be denoted $\mathbb{Q}_S$ and we define the S-height of $t = (t_\nu)_{\nu \in S} \in \mathbb{Q}_S$ as

$$\mathscr{H}_S(t) = \prod_{\nu \in S} |t_\nu|_\nu.$$

The main reason for working with $S = S_f \cup \{\infty\}$ instead of S_f is that the diagonal embbeding of $\mathbb{Z}_S$ in $\mathbb{Q}_S$ is a lattice in $\mathbb{Q}_S$ (but is dense in $\mathbb{Q}_{S_f}$).

5.1 Effective criteria of $\mathbb{Z}_S$-equivalence

Thanks to the criterion of $\mathbb{Z}$-equivalence of Li and Margulis we can decide if Q_1 and Q_2 are $\mathbb{Z}$-equivalent by searching for a solution γ of $Q_1 \circ \gamma = Q_2$ in a finite subset of $GL(d,\mathbb{Z})$ since any entry of a $\gamma \in GL(d,\mathbb{Z})$ with $||\gamma||_\infty \leq M$ is an integer between $-M$ and M, hence there are finitely many choices. When $S_f \neq \emptyset$, $|x|_\infty \leq M$ has infinitely many solutions in $\mathbb{Z}_S$, so $||\gamma||_\infty \leq M$ doesn't determine a finite subset of $GL(d,\mathbb{Z}_S)$. To fix this, note that a system of inequalities

$$|x|_\nu \leq M_\nu, \quad \nu \in S,$$

defines a finite subset of $\mathbb{Z}_S$. In our criteria of $\mathbb{Z}_S$-equivalence we'll bound all the norms $||\gamma||_\nu, \nu \in S$, of a $\gamma \in GL(d,\mathbb{Z}_S)$ taking Q_1 to Q_2. When Q_1 and Q_2 are anisotropic over $\mathbb{Q}_S$[1] there is a uniform bound of

$$||\gamma||_S = \max_{\nu \in S} ||\gamma||_\nu$$

for any $\gamma \in GL(d,\mathbb{Z}_S)$ taking Q_1 to Q_2, thus the kind of criteria we aim at says nothing new in that case. Suppose then that Q_1 and Q_2 are $\mathbb{Q}_S$-isotropic[2]. We have two criteria of $\mathbb{Z}_S$-equivalence depending on whether Q_1 and Q_2 are $\mathbb{R}$-isotropic or not. The reader can find an explicit value of $\mathcal{C}_{i,d}$, as well as of any of the other constants in our statements that depend on d, in Appendix C.

Theorem 5.1.1. *Let S_f be a non-empty finite set of odd primes and let $S = \{\infty\} \cup S_f$. Consider non-degenerate, $\mathbb{R}$-isotropic integral quadratic forms Q_1 and Q_2 in $d \geq 3$ variables. If Q_1 and Q_2 are $\mathbb{Z}_S$-equivalent, there is $\gamma_0 \in GL(d,\mathbb{Z}_S)$ with*

$$||\gamma_0||_\infty < \mathcal{C}_{i,d} p_S^{19d^6} (||Q_1||_\infty ||Q_2||_\infty)^{2d^3},$$

and $||\gamma_0||_p \leq p|\delta_{Q_1}|_p^{-\frac{1}{2}}$ for $p \in S_f$, such that $Q_1 \circ \gamma_0 = Q_2$.

Theorem 5.1.2. *Let $S = \{\infty\} \cup S_f$ be a finite set of primes. Consider non-degenerate integral quadratic forms Q_1 and Q_2 in $d \geq 3$ variables that are $\mathbb{R}$-anisotropic and $\mathbb{Q}_{p_0}$-isotropic for some $p_0 > 2$ in S_f. If Q_1 and Q_2 are $\mathbb{Z}_S$-equivalent, there is $\gamma_0 \in GL(d,\mathbb{Z}_S)$ with*

$$\begin{aligned} ||\gamma_0||_{p_0} &< \mathcal{C}_{a,d} p_S^{13d^6} (||Q_1||_\infty ||Q_2||_\infty)^{\frac{1}{2}d^3+3d}, \\ ||\gamma_0||_p &\leq p|\delta_{Q_1}|_p^{-\frac{1}{2}} \qquad \text{for } p \in S_f - \{p_0\}, \\ ||\gamma_0||_\infty &\leq d^{d+1} \cdot d! ||Q_1||_\infty^{\frac{d-1}{2}} ||Q_2||_\infty^{\frac{1}{2}}, \end{aligned}$$

such that $Q_1 \circ \gamma_0 = Q_2$.

Remark 5.1.3. *The hypotheses $2 \notin S_f$ in Theorem 5.1.1 and $p_0 > 2$ in Theorem 5.1.2 can be removed by extending Proposition 5.3.1 (valid for all primes $\nu \neq 2$) to all ν. See Remark 3.3.5.*

[1] In other words, anisotropic over $\mathbb{Q}_\nu$ for every $\nu \in S$.

[2] That is, isotropic over $\mathbb{Q}_\nu$ for some $\nu \in S$.

Remark 5.1.4. *The last inequality in Theorem 5.1.2 is in fact verified by any matrix g_0 in $GL(d,\mathbb{R})$ taking Q_1 to Q_2. We included it in the statement for the sake of completeness.*

To prove our criteria of $\mathbb{Z}_S$-equivalence we need various tools that we'll introduce in subsequent chapters. In the rest of the present one we explain the dynamical interpretation of the arithmetic problem of $\mathbb{Z}_S$ equivalence of quadratic forms, we state three intermediate results and, taking them for granted, we prove Theorem 5.1.1 and Theorem 5.1.2.

5.2 Dynamical interpretation

Now we present a dynamical reformulation of the problem of $\mathbb{Z}_S$-equivalence. Suppose that Q_1 and Q_2 are $\mathbb{Z}_S$-equivalent, non-degenerate integral quadratic forms in $d \geq 3$ variables. We denote by $G_{d,S}$ the group $GL(d,\mathbb{Q}_S)$. There is a standard quadratic form P on $\mathbb{Q}_S^d$ such that

$$Q_1 = P \circ f \quad \text{and} \quad Q_2 = P \circ g,$$

for some $f, g \in G_{d,S}$. We want to bound all the ν-norms, $\nu \in S$, of some $\gamma_0 \in GL(d,\mathbb{Z}_S)$ that transforms Q_1 to Q_2. Let's consider first an easier question:

Q1. *Which matrices in $G_{d,S}$ take Q_1 to Q_2?*

It's easy to see that precisely those of the form $f^{-1}hg$ with $h \in O(P,\mathbb{Q}_S)$. We denote $O(P,\mathbb{Q}_S)$ by H_S and $\Gamma_{d,S}$ will be the diagonal copy of $GL(d,\mathbb{Z}_S)$ in $G_{d,S}$. Since we are looking for a matrix in $GL(d,\mathbb{Z}_S)$ taking Q_1 to Q_2, the next natural question is:

Q2. *For which $h \in H_S$ is $f^{-1}hg$ in $\Gamma_{d,S}$?*

To detect these elements of H_S we introduce the homogeneous space $X_{d,S} = G_{d,S}/\Gamma_{d,S}$[3]. Let $x_{d,S} = \Gamma_{d,S}/\Gamma_{d,S}$ be the base point of $X_{d,S}$ and consider the action of H_S on $X_{d,S}$ by left multiplication. Here is the link between the arithmetic problem of $\mathbb{Z}_S$-equivalence of quadratic forms and the dynamics of H_S on $X_{d,S}$: *$f^{-1}hg$ is in $\Gamma_{d,S}$ if and only if h moves $gx_{d,S}$ to $fx_{d,S}$.* Since Q_1 and Q_2 are $\mathbb{Z}_S$-equivalent, their corresponding points $fx_{d,S}$ and $gx_{d,S}$ in $X_{d,S}$ lie in the same H_S-orbit Y in $X_{d,S}$, which is closed since it comes from an integral quadratic form. Hence the problem of $\mathbb{Z}_S$-equivalence of integral quadratic forms is intimately related to the next dynamical problem.

Problem 5.2.1. *Given two points y_1 and y_2 in a closed H_S-orbit in $X_{d,S}$, bound the size of the smallest $h^* \in H_S$ moving y_2 to y_1.*

The answer is easy when H_S is compact—which happens iff Q_1 and Q_2 are anisotropic over $\mathbb{Q}_S$—because H_S itself is bounded. So let's consider the case where H_S is non-compact. With their [LM16, Theorem 5], Li and Margulis answer Problem 5.2.1 when $S = \{\infty\}$. We extend their result to any finite set $S = \{\infty\} \cup S_f$ of primes in Proposition 5.2.2 when H_∞ is non-compact, and in Proposition 5.2.3 when H_∞ is compact. A crucial fact to prove these results is that any closed H_S-orbit Y in $X_{d,S}$ admits a unique—up to multiplication by a

[3]The space $X_{d,S}$ has finite volume with respect to its $G_{d,S}$-invariant measure—unique up to multiplication by a positive constant.

positive real number—H_S-invariant measure μ_Y (see Lemma 6.1.3). For $g' \in G_{d,S}, \nu \in S$ and $S' \subseteq S$ we define

$$T_\nu(g') = \frac{||g'_\nu||_\nu^d}{|\det g'_\nu|_\nu} \quad \text{and} \quad T_{S'}(g') = \prod_{\nu \in S'} T_\nu(g').$$

Here are out two dynamical statements.

Proposition 5.2.2. *Let $S = \{\infty\} \cup S_f$ be a finite set of primes and let H_S be the orthogonal group of a standard quadratic form on $\mathbb{Q}_S^d$ with $d \geq 3$. Suppose that H_∞ is non-compact. Consider $f, g \in G_{d,S}$ such that $fx_{d,S}$ and $gx_{d,S}$ are in a closed H_S-orbit Y in $X_{d,S}$. Then there is $h^\star \in H_S$ with*

$$||h^\star_\infty||_\infty < C_d p_S^{9d^3} (T_\infty(f)T_\infty(g))^{\frac{3}{2}d(d-1)+6} (T_{S_f}(f)T_{S_f}(g))^{3d^2} \mu_Y(Y)^6,$$

$||h^\star_p||_p \leq p$ for odd $p \in S_f$ and $||h^\star_2||_2 \leq 4$ if $2 \in S_f$, such that $h^\star g x_{d,S} = f x_{d,S}$.

Proposition 5.2.3. *Let $S = \{\infty\} \cup S_f$ be a finite set of primes and let H_S be the orthogonal group of a standard quadratic form on $\mathbb{Q}_S^d$ with $d \geq 3$. Suppose that H_∞ is compact and that H_{p_0} is non-compact for some $p_0 > 2$ in S_f. Consider $f, g \in G_{d,S}$ such that $fx_{d,S}$ and $gx_{d,S}$ are in a compact H_S-orbit Y in $X_{d,S}$. Then there is $h^\star \in H_S$ with*

$$||h^\star_{p_0}||_{p_0} < F_d p_S^{13d^2} (T_{p_0}(f)T_{p_0}(g))^6 (T_S(f)T_S(g))^{d(d-1)} \mu_Y(Y)^4,$$

$||h^\star_p||_p \leq p$ for odd $p \in S_f - \{p_0\}$, and $||h^\star_2||_2 \leq 4$ if $2 \in S_f$, such that $h^\star g x_{d,S} = f x_{d,S}$.

Chapters 6 and 7 are devoted to prove propositions 5.2.2 and 5.2.3, respectively. We follow closely the original arguments of Li and Margulis, making an extra effort to give explicitly the constants C_d and F_d in the statements. Even if the strategy of the proof is the same in both cases, we keep them separate hoping that the ideas will be more transparent in this way.

5.3 The proof of the equivalence criteria

Taking the dynamical statements for granted, the thing missing to prove the criteria of $\mathbb{Z}_S$-equivalence is the relation of the terms $T_\nu(f), T_\nu(g)$ and $\mu_Y(Y)$ in propositions 5.2.2 and 5.2.3 to the quadratic forms Q_1 and Q_2. The next two results take care of this. The first one is a combination of Lemma 3.2.2 and Proposition 3.3.4, which are proved in Chapter 3.

Proposition 5.3.1. *Consider a prime $\nu \neq 2$ and an integer $d \geq 2$. Any non-degenerate integral quadratic form R on $\mathbb{Q}_\nu^d$ can be written as $P \circ g$, with P a standard quadratic form on $\mathbb{Q}_\nu^d$ and $g \in G_{d,\nu}$ such that*

$$||g||_\nu \leq \begin{cases} d||R||_\infty^{\frac{1}{2}} & \text{if } \nu = \infty, \\ (p||R||_p)^{\frac{1}{2}} & \text{if } \nu = p. \end{cases}$$

Now we handle the term $\mu_Y(Y)$. If Q is a non-degenerate integral quadratic form in d variables, we define

$$Y_{Q,S} = H_S g' x_{d,S},$$

where H_S is the orthogonal group of the standard quadratic form on $\mathbb{Q}_S^d$ that is $\mathbb{Q}_S$-equivalent to Q, and g' is any matrix in $G_{d,S}$ such that $O(Q, \mathbb{Q}_S) = (g')^{-1} H_S g'$. $Y_{Q,S}$ is closed in $X_{d,S}$—see Lemma 6.1.1—thus it admits a unique H_S-invariant finite measure $\mu_{Y_{Q,S}}$[4] up to multiplication by a positive constant—see Lemma 6.1.3. We denote by δ_Q the determinant of the matrix b_Q of Q in the standard basis of $\mathbb{Q}^d$. The next result, which extends [LM16, Theorem 6], gives an upper bound of the volume of $Y_{Q,S}$. Its proof is the goal of Chapter 8.

Proposition 5.3.2. *Consider a finite set $S = \{\infty\} \cup S_f$ of primes and $d \geq 3$. Let Q be a non-degenerate integral quadratic form in d variables isotropic over $\mathbb{Q}_S$. Then*

$$\mu_{Y_{Q,S}}(Y_{Q,S}) < \begin{cases} C_d^{(2)} p_S^{3d^6} \mathscr{H}_S(\delta_Q)^{\frac{d+1}{2}} & \text{if } S_f \neq \emptyset, \\ C_d^{(2)} 2^{2d^6} |\delta_Q|_\infty^{\frac{d+1}{2}} & \text{if } S = \{\infty\}. \end{cases}$$

To close this chapter let's prove our criteria of $\mathbb{Z}_S$-equivalence.

Proof of Theorem 5.1.1. Recall that the $\mathbb{R}$-isotropic, non-degenerate integral quadratic forms Q_1 and Q_2 in $d \geq 3$ variables are $\mathbb{Z}_S$-equivalent. Let P be the standard quadratic form on $\mathbb{Q}_S^d$ that is $\mathbb{Q}_S$-equivalent to $(Q_1)_S$ and $(Q_2)_S$[5] and let $H_S = O(P, \mathbb{Q}_S)$. Consider $f, g \in G_{d,S}$ taking respectively P to $(Q_1)_S$ and $(Q_2)_S$, with coordinates f_ν and g_ν verifying the inequalities of Proposition 5.3.1. Note that $f x_{d,S}$ and $g x_{d,S}$ are in the H_S-orbit $Y = Y_{Q_1,S}$ in $X_{d,S}$, which is closed by Lemma 6.1.1. According to Proposition 5.2.2 there is $h^\star \in H_S$ such that $h^\star g x_{d,S} = f x_{d,S}$,

$$||h_\infty^\star||_\infty < C_d p_S^{9d^3} (T_\infty(f) T_\infty(g))^{\frac{3}{2}d(d-1)+6} (T_{S_f}(f) T_{S_f}(g))^{3d^2} \mu_Y(Y)^6,$$

and $||h_p^\star||_p \leq p$ for $p \in S_f$—recall that $2 \notin S_f$. Since $f^{-1} h^\star g = (\gamma_0, \dots, \gamma_0) \in \Gamma_{d,S}$ takes $(Q_1)_S$ to $(Q_2)_S$, then $\gamma_0 \in GL(d, \mathbb{Z}_S)$ takes Q_1 to Q_2.

Now we relate $T_\nu(f)$ and $T_\nu(g)$ to Q_1 and Q_2. For $p \in S_f$, $||Q_1||_p \leq 1$ because Q_1 is integral, so $||f_p||_p \leq \sqrt{p}$. Since $||f_p||_p$ is an integral power of p, in fact $||f_p||_p \leq 1$, thus

$$T_p(f) = \frac{||f_p||_p^d}{|\det f_p|_p} \leq \left(\frac{|(\delta_P)_p|_p}{|\delta_{Q_1}|_p} \right)^{\frac{1}{2}} \leq |\delta_{Q_1}|_p^{-\frac{1}{2}}. \tag{5.2}$$

For T_∞ we have

$$T_\infty(f) = \frac{||f_\infty||_\infty^d}{|\det f_\infty|_\infty} \leq d^d \left(\frac{||Q_1||_\infty^d}{|\delta_{Q_1}|_\infty} \right)^{\frac{1}{2}}. \tag{5.3}$$

[4] Note that μ_Y is determined by a Haar measure on H_S, which we fix as follows: each factor H_ν is the orthogonal group of a diagonal quadratic form, and we endow it with the Haar measure determined by the basis in (A.1) of its Lie algebra. In the introduction of Appendix A we explain how a basis of the Lie algebra determines a Haar measure. We consider in H_S the product measure.

[5] To avoid confusions, we'll write Q_S when we think a rational quadratic form Q as quadratic form over $\mathbb{Q}_S$ via the diagonal embedding $\mathbb{Q} \to \mathbb{Q}_S$.

Similar bounds hold for $T_p(g)$ and $T_\infty(g)$. Recall also that

$$\mu_Y(Y) \leq C_d^{(2)} p_S^{3d^6} \mathscr{H}_S(\delta_{Q_1})^{\frac{d+1}{2}} = C_d^{(2)} p_S^{3d^6} \mathscr{H}_S(\delta_{Q_1}\delta_{Q_2})^{\frac{d+1}{4}},$$

by Proposition 5.3.2. Then

$$\begin{aligned}||h^\star_\infty||_\infty &< C_d p_S^{9d^3} \left(d^{2d} \frac{||Q_1||_\infty^{\frac{d}{2}} ||Q_2||_\infty^{\frac{d}{2}}}{\sqrt{|\delta_{Q_1}\delta_{Q_2}|_\infty}} \right)^{\frac{3}{2}d(d-1)+6} \mathscr{H}_{S_f}(\delta_{Q_1}\delta_{Q_2})^{-\frac{3}{2}d^2} (C_d^{(2)} p_S^{3d^6} \mathscr{H}_S(\delta_{Q_1}\delta_{Q_2})^{\frac{d+1}{4}})^6 \\ &\leq \mathcal{J}_d p_S^{18d^6+9d^3} (||Q_1||_\infty ||Q_2||_\infty)^{\frac{3}{4}d^2(d-1)+3d} \frac{\mathscr{H}_S(\delta_{Q_1}\delta_{Q_2})^{\frac{3}{2}(d+1)}}{|\delta_{Q_1}\delta_{Q_2}|_\infty^{\frac{3}{4}d(d-1)+3} \mathscr{H}_{S_f}(\delta_{Q_1}\delta_{Q_2})^{\frac{3}{2}d^2}},\end{aligned}$$

where $\mathcal{J}_d = d^{3d^2(d-1)+12d} C_d (C_d^{(2)})^6$. Since $\mathscr{H}_S(\delta_{Q_1}\delta_{Q_2})$ is a positive integer and $d \geq 3$,

$$\mathscr{H}_S(\delta_{Q_1}\delta_{Q_2})^{\frac{3}{2}(d+1)} \leq \mathscr{H}_S(\delta_{Q_1}\delta_{Q_2})^{\frac{3}{2}d^2} = |\delta_{Q_1}\delta_{Q_2}|_\infty^{\frac{3}{2}d^2} \mathscr{H}_{S_f}(\delta_{Q_1}\delta_{Q_2})^{\frac{3}{2}d^2},$$

so

$$\frac{\mathscr{H}_S(\delta_{Q_1}\delta_{Q_2})^{\frac{3}{2}(d+1)}}{|\delta_{Q_1}\delta_{Q_2}|_\infty^{\frac{3}{4}d(d-1)+3} \mathscr{H}_{S_f}(\delta_{Q_1}\delta_{Q_2})^{\frac{3}{2}d^2}} \leq \frac{|\delta_{Q_1}\delta_{Q_2}|_\infty^{\frac{3}{2}d^2}}{|\delta_{Q_1}\delta_{Q_2}|_\infty^{\frac{3}{4}d(d-1)+3}} \leq |\delta_{Q_1}\delta_{Q_2}|_\infty^{d^2}.$$

Thus we obtain

$$||h^\star_\infty||_\infty \leq \mathcal{J}_d p_S^{19d^6} (||Q_1||_\infty ||Q_2||_\infty)^{\frac{3}{4}d^2(d-1)+3d} |\delta_{Q_1}\delta_{Q_2}|_\infty^{d^2}.$$

We are ready to bound γ_0:

$$\begin{aligned}||\gamma_0||_\infty = ||f_\infty^{-1} h^\star_\infty g_\infty||_\infty &\leq d^2 ||f_\infty^{-1}||_\infty ||g_\infty||_\infty ||h^\star_\infty||_\infty \\ &\leq d \cdot d! \frac{||f_\infty||_\infty^{d-1}}{|\det f_\infty|_\infty} ||g_\infty||_\infty ||h^\star_\infty||_\infty \\ &\leq d^{d+1} \cdot d! ||Q_1||_\infty^{\frac{d-1}{2}} ||Q_2||_\infty^{\frac{1}{2}} ||h^\star_\infty||_\infty \\ &\leq (d^{d+1} \cdot d! \mathcal{J}_d) p_S^{19d^6} (||Q_1||_\infty ||Q_2||_\infty)^{(\frac{3}{4}d^2+\frac{1}{2})(d-1)+3d} |\delta_{Q_1}\delta_{Q_2}|_\infty^{d^2} \\ &\leq (d^{d+1} \cdot d! \mathcal{J}_d) p_S^{19d^6} (||Q_1||_\infty ||Q_2||_\infty)^{d^3} |\delta_{Q_1}\delta_{Q_2}|_\infty^{d^2} \\ &\leq \mathcal{C}_{i,d} p_S^{19d^6} (||Q_1||_\infty ||Q_2||_\infty)^{2d^3},\end{aligned}$$

where

$$\mathcal{C}_{i,d} = d^{d+1} \cdot d!^{2d^2+1} \mathcal{J}_d = d^{3d^2(d-1)+13d+1} \cdot d!^{2d^2+1} C_d (C_d^{(2)})^6.$$

Finally, for $p \in S_f$

$$||\gamma_0||_p \leq ||f_p^{-1}||_p ||g_p||_p ||h^\star_p||_p \leq p |\delta_{Q_1}|_p^{-\frac{1}{2}}.$$

□

Proof of Theorem 5.1.2. This time Q_1 and Q_2 are $\mathbb{R}$-anisotropic, $\mathbb{Q}_{p_0}$-isotropic for some odd p_0 in S_f, and $\mathbb{Z}_S$-equivalent. Consider $f, g \in G_{d,S}$ as in Proposition 5.3.1 such that

$$(Q_1)_S = P \circ f \quad \text{and} \quad (Q_2)_S = P \circ g,$$

where P is a standard quadratic form on $\mathbb{Q}_S^d$. Let H_S be the orthogonal group of P and let $Y = Y_{Q_1,S}$. The bounds 5.2 and 5.3 for $T_\nu(f)$ and $T_\nu(g)$ hold also in the current situation. Take $h^\star \in H_S$ moving $gx_{d,S}$ to $fx_{d,S}$ as in Proposition 5.2.3. Once more $f^{-1}h^\star g = (\gamma_0, \dots, \gamma_0)$ is in $\Gamma_{d,S}$, and $\gamma_0 \in GL(d, \mathbb{Z}_S)$ takes Q_1 to Q_2. We have

$$\begin{aligned}
||h^\star_{p_0}||_{p_0} &< F_d p_S^{13d^2} (T_{p_0}(f)T_{p_0}(g))^6 (T_S(f)T_S(g))^{d(d-1)} \mu_Y(Y)^4 \\
&\leq F_d p_S^{13d^2} |\delta_{Q_1}\delta_{Q_2}|_{p_0}^{-3} \left(d^{2d} \frac{||Q_1||_\infty^{\frac{d}{2}} ||Q_2||_\infty^{\frac{d}{2}}}{\sqrt{\mathscr{H}_S(\delta_{Q_1}\delta_{Q_2})}} \right)^{d(d-1)} (C_d^{(2)} p_S^{3d^6} \mathscr{H}_S(\delta_{Q_1})^{\frac{d+1}{2}})^4 \\
&\leq \mathcal{C}_{a,d} p_S^{13d^6} (||Q_1||_\infty ||Q_2||_\infty)^{\frac{1}{2}d^2(d-1)} |\delta_{Q_1}\delta_{Q_2}|_\infty^3,
\end{aligned}$$

where $\mathcal{C}'_{a,d} = d^{2d^2(d-1)} F_d (C_d^{(2)})^4$. Then

$$\begin{aligned}
||\gamma_0||_{p_0} = ||f_{p_0}^{-1} h^\star_{p_0} g_{p_0}||_{p_0} &\leq \frac{||f_{p_0}||_{p_0}^{d-1}}{|\det f_{p_0}|_{p_0}} ||g_{p_0}||_{p_0} ||h^\star_{p_0}||_{p_0} \\
&\leq |\delta_{Q_1}|_{p_0}^{-\frac{1}{2}} ||h^\star_{p_0}||_{p_0} \\
&< \mathcal{C}'_{a,d} p_S^{13d^6} (||Q_1||_\infty ||Q_2||_\infty)^{\frac{1}{2}d^2(d-1)} |\delta_{Q_1}\delta_{Q_2}|_\infty^{\frac{7}{2}} \\
&\leq \mathcal{C}_{a,d} p_S^{13d^6} (||Q_1||_\infty ||Q_2||_\infty)^{\frac{1}{2}d^2(d-1)+\frac{7}{2}d^2} \\
&= \mathcal{C}_{a,d} p_S^{13d^6} (||Q_1||_\infty ||Q_2||_\infty)^{\frac{1}{2}d^3+3d},
\end{aligned}$$

where

$$\mathcal{C}_{a,d} = (d!)^7 \mathcal{C}'_{a,d} = (d!)^7 d^{2d^2(d-1)} F_d (C_d^{(2)})^4,$$

For $p \in S_f$,

$$||\gamma_0||_p = ||f_p^{-1} h^\star_p g_p||_p \leq |\delta_{Q_1}|_p^{-\frac{1}{2}} ||h^\star_p||_p \leq p |\delta_{Q_1}|_p^{-\frac{1}{2}}.$$

To conclude we bound the ∞-norm of γ_0. Recall that $H_\infty = O(d, \mathbb{R})$, so $||h^\star_\infty||_\infty \leq 1$.

$$\begin{aligned}
||\gamma_0||_\infty &= ||f_\infty^{-1} h^\star_\infty g_\infty||_\infty \\
&\leq d \cdot d! \frac{||f_\infty||_\infty^{d-1}}{|\det f_\infty|_\infty} ||g_\infty||_\infty \\
&\leq d^{d+1} \cdot d! ||Q_1||_\infty^{\frac{d-1}{2}} ||Q_2||_\infty^{\frac{1}{2}}.
\end{aligned}$$

□

Chapter 6

Dynamical statement I: $\mathbb{R}$-isotropic case

The goal of this chapter is to establish Proposition 5.2.2, the dynamical result we used to obtain our $\mathbb{Z}_S$-equivalence criterion for $\mathbb{R}$-isotropic integral quadratic forms 5.1.1. We'll restate it below.

Recall that $\mathbf{G}_d$ stands for $\mathbf{GL}(d)$. If $S = \{\infty\} \cup S_f$ is a finite set of primes, $\Gamma_{d,S}$ is the diagonal copy of $GL(d, \mathbb{Z}_S)$ in $G_{d,S}$, $X_{d,S}$ is the homogeneous space $G_{d,S}/\Gamma_{d,S}$ and $x_{d,S}$ is the basepoint $\Gamma_{d,S}/\Gamma_{d,S}$. For $g \in G_{d,S}, \nu \in S$ and $S' \subseteq S$ we define

$$T_\nu(g) = \frac{||g_\nu||_\nu^d}{|\det g_\nu|_\nu} \quad \text{and} \quad T_{S'}(g) = \prod_{\nu \in S'} T_\nu(g).$$

Finally, remember that a quadratic form $P = (P_\nu)_{\nu \in S}$ on $\mathbb{Q}_S^d$ is standard if, for each $\nu \in S$, P_ν is a standard quadratic form on $\mathbb{Q}_\nu^d$—see Chapter 3 for this definition. Here is the main result of this chapter:

Proposition 6.0.1. *Consider a finite set of primes $S = \{\infty\} \cup S_f$ and $d \geq 3$. Let H_S be the orthogonal group of a standard quadratic form on $\mathbb{Q}_S^d$. Suppose that H_∞ is non-compact. Take $f, g \in G_{d,S}$ such that $fx_{d,S}$ and $gx_{d,S}$ are in a closed H_S-orbit Y in $X_{d,S}$. Then there is $h^\star \in H_S$ such that $h^\star g x_{d,S} = f x_{d,S}$,*

$$||h_\infty^\star||_\infty < C_d p_S^{9d^3} (T_\infty(f)T_\infty(g))^{\frac{3}{2}d(d-1)+6} (T_{S_f}(f)T_{S_f}(g))^{3d^2} \mu_Y(Y)^6,$$

$||h_p^\star||_p \leq p$ for any odd $p \in S_f$, and $||h_2^\star||_2 \leq 4$ if $2 \in S_f$.

Here is a cartoon of the strategy that Li and Margulis follow to prove [LM16, Theorem 5], the same that we adapt to obtain Proposition 6.0.1: Consider points $y_1 = fx_{d,S}$ and $y_2 = gx_{d,S}$ in a closed H_S-orbit Y in $X_{d,S}$. We want to estimate the size of an $h_0 \in H_S$ moving y_1 to y_2. Suppose that the action of H_S on Y is mixing, and moreover that we dispose of an estimate of the mixing speed of the form: There is a function $F : H_S \to [0, \infty)$ vanishing at ∞ such that, for any measurable subsets $\mathcal{U}_1, \mathcal{U}_2$ of Y and any $h \in H_S$,

$$\left| \mu_Y((h\mathcal{U}_1) \cap \mathcal{U}_2) - \frac{\mu_Y(\mathcal{U}_1)\mu_Y(\mathcal{U}_2)}{\mu_Y(Y)} \right| \leq C_{\mathcal{U}_1,\mathcal{U}_2} F(h), \tag{6.1}$$

where $C_{\mathcal{U}_1,\mathcal{U}_2} > 0$ depends only on $\mathcal{U}_1$ and $\mathcal{U}_2$. Suppose now that $\mathcal{U}_1$ and $\mathcal{U}_2$ are small neighborhoods of y_1 and y_2. If we choose $h' \in H_S$ such that

$$C_{\mathcal{U}_1,\mathcal{U}_2} F(h') < \frac{\mu_Y(\mathcal{U}_1)\mu_Y(\mathcal{U}_2)}{\mu_Y(Y)},$$

by (6.1) necessarily $\mu_Y((h'\mathcal{U}_1) \cap \mathcal{U}_2)$ is positive. In other words, h' moves a point near y_1 to a point near y_2. Thus, there is $h_0 \in H_S$ of about the same size as h' that moves y_1 to y_2.

The purpose of this chapter is to turn this cartoon—which although somewhat inaccurate, serves as guide—into a real proof. The chapter is organized as follows: In Section 6.1 we'll prove that the orbits $Y_{Q,S}$ are indeed closed, which justifies our interest in the dynamical situation of Proposition 6.0.1, as well as a partial converse in Lemma 6.1.2. In the sketch of proof above we assumed that $H_S \curvearrowright Y$ is mixing, and this is not always the case, but in Section 6.2 we'll show that this is *virtually* true: there is a finite partition $Y_1 \sqcup \cdots \sqcup Y_\ell$ of Y and a finite index subgroup H_S° of H_S whose action on each Y_i is mixing. To obtain an estimate like (6.1) for $H_S^\circ \curvearrowright Y_i$ we'll first show that $L^2_0(Y_i)$ is an almost L^4 unitary representation of H_∞° and then we'll apply the decay speed for coefficients of smooth vectors—Corollary 4.3.3. Since the indicator functions of $\mathcal{U}_1$ and $\mathcal{U}_2$ are not smooth, we need to replace them by smooth functions supported on these small open sets. In Section 6.3 we prepare for this. Finally, we complete the proof of Proposition 7.0.1 in Section 6.4.

6.1 Closed orbits and integral quadratic forms

Let H_S be the orthogonal group of a non-degenerate quadratic form on $\mathbb{Q}_S^d$. The goal of this section is to explain the nice relationship there is between closed H_S-orbits in $X_{d,S}$ and integral quadratic forms: if Q is integral and non-degenerate, $Y_{Q,S}$ is closed in $X_{d,S}$. Conversely, closed H_S orbits in $X_{d,S}$ are always of this form when $d \geq 3$ and H_S is non-compact. This will play an important role to reduce the proof of Proposition 6.2.1 to the case when H_S is the orthogonal group of a ternary quadratic form. We start with the easy implication.

Lemma 6.1.1. *Let Q be a non-degenerate integral quadratic form in $d \geq 2$ variables. Then $Y_{Q,S}$ is closed in $X_{d,S}$ for any finite set $S = \{\infty\} \cup S_f$ of primes.*

Proof. We write $Q_S = P \circ g$ with $g \in G_{d,S}$ and P a standard quadratic form on $\mathbb{Q}_S^d$. Let $H_S = O(P, \mathbb{Q}_S)$. Suppose that $h_n g x_{d,S} \underset{n\to\infty}{\longrightarrow} f x_{d,S}$ for some $h_n \in H_S$ and some $f \in G_{d,S}$. There are $\gamma_n \in \Gamma_{d,S}$ such that $h_n g \gamma_n \to f$, so

$$P \circ f = \lim_{n\to\infty} P \circ (h_n g \gamma_n) = \lim_{n\to\infty} Q_S \circ \gamma_n.$$

The diagonal copy $M_d(\mathbb{Z}_S)^\Delta$ in $M_d(\mathbb{Q}_S)$ of $M_d(\mathbb{Z}_S)$ is discrete and closed. Since each $b_{Q\circ\gamma_n}$ is in $M_d(\mathbb{Z}_S)^\Delta$, then the matrix of $P \circ f$ is as well and $P \circ f = Q_S \circ \gamma_n$ for $n \gg 1$. Since $Q_S = P \circ g$, we have $f = hg\gamma_n$ for some $h \in H_S$ and some big enough n. In other words, $f x_{d,S}$ is in $Y_{Q,S}$. □

Now we'll see that closed H_S-orbits in $X_{d,S}$ always come from integral quadratic forms. When H_S is compact, every H_S-orbit in $X_{d,S}$ is closed, but not all of them are of the form $Y_{Q,S}$. Leaving aside this case, when $d \geq 3$, closed H_S-orbits come always from integral quadratic forms. This fact will be important in the proofs of Proposition 6.2.1 and Proposition 7.1.1.

Lemma 6.1.2. *Consider a finite set $S = \{\infty\} \cup S_f$ of primes and let R be a non-degenerate quadratic form in $d \geq 3$ variables with coefficients in $\mathbb{Q}_S$. If R is $\mathbb{Q}_S$-isotropic and $SO(R, \mathbb{Q}_S)x_{d,S}$ is closed in $X_{d,S}$, then $SO(R, \mathbb{Q}_S) = SO(Q_S, \mathbb{Q}_S)$ for a non-degenerate integral quadratic form Q in d variables.*

To prove this we need a fact that we'll use over and over: closed H_S-orbits in $X_{d,S}$ admit *finite* H_S-invariant measures. This is a result of Dani and Margulis, and is valid more generally for any semisimple subgroup H'_S of $G_{d,S}$, which means that $H'_S = \prod_{\nu \in S} H'_\nu$ and all the H'_ν are semisimple, algebraic subgroups of $GL(d, \mathbb{Q}_\nu)$—see [Ben20, Proposition 3.1] for a proof for semisimple real Lie groups.

Lemma 6.1.3. *Consider a finite set $S = \{\infty\} \cup S_f$ of primes and let H_S be the orthogonal group of a non-degenerate quadratic form in $d \geq 3$ variables with coefficients in $\mathbb{Q}_S$. Any closed H_S-orbit Y in $X_{d,S}$ admits a finite H_S-invariant measure μ_Y. Moreover, μ_Y is unique up to multiplication by a positive scalar.*

Proof of Lemma 6.1.2. For $\nu \in S$, let R_ν be the component of R in $\mathbb{Q}_\nu$. Since R is $\mathbb{Q}_S$-isotropic, then R_{ν_0} is isotropic for some $\nu_0 \in S$. We'll prove first that R_{ν_0} has an integral multiple Q. Let $H_S = SO(R, \mathbb{Q}_S)$, which is semisimple since $d \geq 3$. Then $\Lambda_S = \Gamma_{d,S} \cap H_S$ is a lattice in H_S by Lemma 6.1.3. For $S_0 \subset S$, let Λ_{S_0} be the projection of Λ_S to $G_{S_0,d}$. If we show that Λ_{ν_0}—which is contained in $SO(R_{\nu_0}, \mathbb{Q})$—is Zariski-dense, so R_{ν_0} has a non-trivial integral multiple Q. Let T be the subset of $\nu \in S$ for which R_ν is isotropic. Note that Λ_T is still a lattice in H_T because H_{S-T} is compact. H_T is semisimple, Zariski-connected and has no compact factors, hence Λ_T is Zariski-dense in H_T by Borel's Density Theorem—see [Zim84, p. 41 and Remark in p. 42]. Λ_T projects to Λ_{ν_0}, so this last one is Zariski-dense in H_{ν_0}.

Let $S' = S - \{\nu_0\}$. To show that $H_S = SO(Q_S, \mathbb{Q}_S)$ it suffices to prove that $H_{S'}$ contains a neighborhood of the identity in $SO(Q, \mathbb{Q}_{S'})$. Let $\Delta_{S'}$ be the diagonal copy of $SO(Q, \mathbb{Z}_S)$ in $G_{d,S'}$. Since $SO(Q, \mathbb{Q}_{\nu_0})$ is non-compact, by the Strong Approximation Theorem [1]the closure—with respect to the analytic topology—of $\Delta_{S'}$ is a clopen subgroup $U_{S'}$ of $SO(Q, \mathbb{Q}_{S'})$. Write $G_{d,S} = G_{\nu_0} \times G_{d,S'}$. Note that

$$(1 \times \Delta_{S'})x_{d,S} = (SO(Q, \mathbb{Z}_S) \times 1)x_{d,S} \subset H_S x_{d,S},$$

hence $(1 \times U_{S'})x_{d,S}$ is also contained in $H_S x_{d,S}$, since this last is closed in $X_{d,S}$. This implies also that there is a neighborhood of the identity $W_S = \prod_{\nu \in S} W_\nu$ in $G_{d,S}$ such that $w \mapsto w x_{d,S}$ is an homeomorphism $W_S \to W_S x_{d,S}$ and $(W_S x_{d,S}) \cap (H_S x_{d,S}) = (W_S \cap H_S)x_{d,S}$. Then $H_{S'}$ contains $U_{S'} \cap W_{S'}$.

□

To close this section we rewrite Lemma 6.1.2 in terms of the orbits $Y_{Q,S}$.

[1]See [PR94, Theorem 7.12]

Corollary 6.1.4. *Consider a finite set of primes $S = \{\infty\} \cup S_f$ and $d \geq 3$. Let H_S be the orthogonal group of a $\mathbb{Q}_S$-isotropic standard quadratic form on $\mathbb{Q}_S^d$. Then any closed H_S-orbit in $X_{d,S}$ is of the form $Y_{Q,S}$ for some integral quadratic form Q.*

Proof. Let Y be a closed H_S-orbit in $X_{d,S}$ and take $gx_{d,S} \in Y$. Consider $R = P \circ g$. The set $g^{-1}Y = O(R, \mathbb{Q}_S)x_{d,S}$ is also closed in $X_{d,S}$. Since R is isotropic, Lemma 6.1.2 tells us that $O(R, \mathbb{Q}_S) = O(Q_S, \mathbb{Q}_S)$ for some integral quadratic form Q, so $Y = Y_{Q,S}$. □

6.2 Mixing speed for closed H_S°-orbits

Let H_S be the orthogonal group of a standard quadratic form on $\mathbb{Q}_S^d$. In the introduction we said that the action of H_S on any closed H_S-orbit Y in $X_{d,S}$ is virtually mixing. Let's precise what we meant by that. Let H_S° be the image in H_S of the corresponding *Spin* group[2]. Since H_S° has finite index in H_S, there are finitely many H_S°-orbits $Y_1, \ldots, Y_\ell$ in Y. When H_∞ is non-compact, the action of H_∞° on each Y_i is mixing. What is really surprising is that there is a mixing speed for $H_\infty^\circ \curvearrowright Y_i$, valid independently of Y_i and Y. This is a consequence of deep results in the theory of automorphic representations. A detailed discussion of them is out of the scope of this work, we'll just present the relevant statements for our applications in 6.2.1. Once more, following the original arguments of Li and Margulis, and to keep things as concrete as possible, we'll state the mixing speed for a particular copy of $SO(2,1)^\circ$ in H_∞°. To do so, we introduce first more notation.

Consider a non-degenerate quadratic form R on $\mathbb{R}^d$ and a linear subspace V of $\mathbb{R}^d$. If $R\big|_V$ is non-degenerate, then $\mathbb{R}^d = V \oplus V^\perp$, where $V^\perp$ is the R-orthogonal complement of V. We denote by $O(R, \mathbb{R})^V$ the subgroup of $h \in O(R, \mathbb{R})$ such that $h(V) = V$ and h acts as the identity on $V^\perp$. Suppose that H_∞ is orthogonal group of a standard isotropic quadratic form P on $\mathbb{R}^d$. By definition of standard, $P(x) = x_1^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_d^2$ for some $1 \leq r < d$. Suppose that $r \geq 2$ and let $V = \mathbb{R}e_1 \oplus \mathbb{R}e_2 \oplus \mathbb{R}e_{r+1}$. We'll denote ρ_{H_∞} the morphism $SL(2, \mathbb{R}) \to H_\infty$ obtained composing $\iota_\infty : SL(2, \mathbb{R}) \to SO(2,1)^\circ$ as in Lemma 3.5.1 with the natural isomorphism $O(2,1) \to H_\infty^V$. If $r = 1$, set $V = \mathbb{R}e_1 \oplus \mathbb{R}e_{r+1} \oplus \mathbb{R}e_{r+2}$ and define ρ_{H_∞} as the composition

$$SL(2, \mathbb{R}) \xrightarrow{\iota'_\infty} SO(1,2)^\circ \longrightarrow H_\infty^V,$$

with ι'_∞ as in Lemma 3.5.2. Note that the image of ρ_{H_∞} is $H_\infty^{V\circ}$, the neutral connected component of H_∞^V. We'll denote by $\mathcal{X}_{H_\infty} \in \mathfrak{h}_\infty$ the image of

$$\mathcal{Z} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathfrak{sl}(2, \mathbb{R})$$

under (the derivative at I_2 of) ρ_{H_∞}.

Let π be a unitary representation of H_∞. Recall that if $v \in \mathcal{H}_\pi$ is H_∞-smooth, for $\mathcal{X} \in \mathfrak{h}_\infty$ we define

$$||v||_{\mathcal{X}} = (||v||^2 + ||\pi(\mathcal{X})v||^2)^{\frac{1}{2}}.$$

Finally, we set $\mathcal{D} = 5\sqrt{\mathcal{D}_1}$, with $\mathcal{D}_1$ is as in Corollary 4.3.2.

[2]For the definition of *Spin* see Section 3.4 of Chapter 3.

Proposition 6.2.1. *Consider a finite set $S = \{\infty\} \cup S_f$ of primes and $d \geq 3$. Let H_S be the orthogonal group of a standard quadratic form on $\mathbb{Q}_S^d$ with H_∞ non-compact and let $\rho = \rho_{H_\infty}$. Suppose that Y' is a closed H_S°-orbit in $X_{d,S}$. For any H_∞°-smooth functions $\varphi_1, \varphi_2 \in L^2(Y')$ we have*

$$\left| \int_{Y'} (\varphi_1 \circ \rho(a_{\infty,-t}))\overline{\varphi_2} d\mu_{Y'} - \frac{1}{\mu_{Y'}(Y')} \int_{Y'} \varphi_1 d\mu_{Y'} \int_{Y'} \overline{\varphi_2} d\mu_{Y'} \right| \leq \mathcal{D} e^{-t/6} ||\varphi_1||_{\mathcal{X}_{H_\infty}} ||\varphi_2||_{\mathcal{X}_{H_\infty}} \tag{6.2}$$

for $t \geq 0$.

Like we said in Chapter 4, a mixing speed of $H_S \curvearrowright Y'$ can be interpreted as a speed of decay of coefficients of $L_0^2(Y)$. We'll obtain Proposition 6.2.1 from the next lemma and the decay speed of coefficients of Corollary 4.3.3.

Lemma 6.2.2. *Consider a finite set $S = \{\infty\} \cup S_f$ of primes and $d \geq 3$. Let H_S be the orthogonal group of a standard quadratic form P on $\mathbb{Q}_S^d$ with H_∞ non-compact. Let V be a 3-dimensional subspace of $\mathbb{R}^d$ where P_∞ is non-degenerate and isotropic. For any closed H_S°-orbit Y' in $X_{d,S}$, the unitary representation of $H_\infty^{V\circ}$ on $L_0^2(Y')$ is almost L^4.*

Taking Lemma 6.2.2 for granted for the moment, let's deduce Proposition 6.2.1.

Proof of Proposition 6.2.1. Let Y' be a closed H_S°-orbit in $X_{d,S}$ and let π be the unitary representation of H_∞° on $L^2(Y')$. Consider $\varphi_1, \varphi_2 \in L^2(Y')$ and define

$$\psi_i = \varphi_i - \frac{1}{\mu_{Y'}(Y')} \int_{Y'} \varphi_i \mathrm{d}\mu_{Y'},$$

which is simply the orthogonal projection of φ_i to $L_0^2(Y')$. Note that the left-hand side of inequality (6.2)—the one we want to prove—is equal to $|\langle \pi(\rho(a_{\infty,t}))\psi_1, \psi_2 \rangle|_\infty$.

By definition of $\rho : SL(2,\mathbb{R}) \to H_\infty$, its image is of the form $H_\infty^{V\circ}$, where

$$V = \mathbb{R}e_1 \oplus \mathbb{R}e_i \oplus \mathbb{R}e_j$$

for some $1 < i < j$. By Lemma 6.2.2, the unitary representation of $H_\infty^{V\circ}$ on $L_0^2(Y')$ is almost L^4. Since $\rho : SL(2,\mathbb{R}) \to H_\infty^{V\circ}$ is a finite covering of Lie groups, the unitary representation of $SL(2,\mathbb{R})$ on $L_0^2(Y')$ is also almost L^4. The decay speed of coefficients of smooth vectors—Corollary 4.3.3—give the result:

$$|\langle \pi \circ \rho(a_{\infty,t})\psi_1, \psi_2 \rangle|_\infty \leq e^{-\frac{t}{6}} (5\sqrt{\mathcal{D}_1} ||\varphi_1||_{\mathcal{X}_{H_\infty}} ||\varphi_2||_{\mathcal{X}_{H_\infty}}).$$

□

The technical results we use to prove Lemma 6.2.3—Proposition 6.2.5 and Theorem 6.2.6—work only when the subspace V of $\mathbb{R}^d$ is defined over $\mathbb{Q}$. The next lemma is essentially a restatement of Lemma 6.2.2 with this extra hypothesis. After stating it we'll see that we can eliminate the rationality assumption.

Lemma 6.2.3. *Let Q be an $\mathbb{R}$-isotropic non-degenerate integral quadratic form in $d \geq 3$ variables. Consider a 3-dimensional subspace W of $\mathbb{Q}^d$ such that Q is non-degenerate and isotropic on $V' = W_\mathbb{R}$. For any finite set $S = \{\infty\} \cup S_f$ of primes, the unitary representation of $SO(Q,\mathbb{R})^{V'\circ}$ on $L_0^2(SO(Q_S,\mathbb{Q}_S)^\circ x_{d,S})$ is almost L^4.*

Proof of Lemma 6.2.2. Suppose that $Y' = H_S^\circ g x_{d,S}$ is closed in $X_{d,S}$. Then so is $g^{-1}Y' = (g^{-1}H_S^\circ g)x_{d,S}$. By Lemma 6.1.2, $g^{-1}H_S^\circ g = O(Q, \mathbb{Q}_S)$ for some non-degenerate integral quadratic form Q in d variables. Consider a 3-dimensional linear subspace V of $\mathbb{R}^d$ where P_∞ is isotropic and non-degenerate, and let $V'' = g_\infty^{-1}V$. The unitary representations of $H_\infty^{V\circ}$ and $g_\infty^{-1}H_\infty^{V\circ}g_\infty = SO(Q,\mathbb{R})^{V''\circ}$ on $L^2(Y')$ and $L^2(SO(Q,\mathbb{Q}_S)x_{d,S})$ are unitary equivalent. We'll show that the latter one is almost L^4.

Choose a linear subspace $W \subseteq \mathbb{Q}^d$ of dimension 3 such that the restrictions of Q to V'' and $V' = W_\mathbb{R}$ have the same signature. By Witt's Theorem—see [Ser95, p. 58]—there is $h_0 \in SO(Q,\mathbb{R})^\circ$ such that $SO(Q,\mathbb{R})^{V''\circ} = h_0 SO(Q,\mathbb{R})^{V'\circ}h_0^{-1}$. The left multiplication by h_0 is a measure-preserving homeomorphism $SO(Q,\mathbb{Q}_S)^\circ x_{d,S} \to SO(Q,\mathbb{Q}_S)^\circ x_{d,S}$, equivariant with respect to $SO(Q,\mathbb{R})^{V'\circ} \to SO(Q,\mathbb{R})^{V''\circ}$ (the conjugation by h_0). Hence the unitary representations of these groups on $L_0^2(SO(Q,\mathbb{Q}_S)^\circ x_{d,S})$ are unitary equivalent. The one of $SO(Q,\mathbb{R})^{V'\circ}$ is almost L^4 by Lemma 6.2.3, so we are done. □

The remaining of this section is devoted to the proof of Lemma 6.2.3.

6.2.1 Automorphic representations at ∞

We introduce here the technical statements we use to prove Lemma 6.2.3.

Let $\mathbf{J}$ be a semisimple $\mathbb{Q}$-subgroup of $\mathbf{GL}(d)$. The group $\Lambda_\infty = J_\infty \cap GL(d,\mathbb{Z})$ is a lattice in J_∞ by Borel, Harish-Chandra's Theorem. For any positive integer N, the N-th principal congruence subgroup of Λ_∞ is defined as

$$\Lambda_\infty(N) = ker(\Lambda_\infty \to GL(d,\mathbb{Z}/N\mathbb{Z})).$$

More generally, if $S = \{\infty\} \cup S_f$ is a finite set of primes, then $\Lambda_S = G_{d,S} \cap \Gamma_{d,S}$ is a lattice in $G_{d,S}$. If N is a natural number not divisible by any $p \in S_f$, the N-th principal congruence subgroup $\Lambda_S(N)$ of Λ_S is the kernel of $\Lambda_S \to GL(d,\mathbb{Z}/N\mathbb{Z})$. A congruence subgroup of Λ_S is a subgroup that contains a principal congruence subgroup.

Recall that the unitary dual of J_∞, denoted by $\widehat{J_\infty}$, is the set of equivalence classes of irreducible unitary representations. We endow it with the Fell topology—see [BdlHV08, p. 427]. If π is a unitary representation of J_∞, its support $\operatorname{supp}\pi$ is the set of elements of $\widehat{J_\infty}$ weakly contained in π. The automorphic spectrum $\widehat{J_\infty}^{Aut}$ of $\mathbf{J}$ is the closure in $\widehat{J_\infty}$ of

$$\bigcup_{N\geq 1} \operatorname{supp}(L^2(J_\infty/\Lambda_\infty(N)).$$

This notion is independent of the $\mathbb{Q}$-embedding $\mathbf{J} \hookrightarrow \mathbf{GL}(d)$ since the commensurability class of congruence subgroups is independent of the the $\mathbb{Q}$-embedding—see [Ben09, Corollary 2.8]. For us, an *automorphic representation* of J_∞ is a unitary representation whose support is contained in $\widehat{J_\infty}^{Aut}$. The next lemma provides various examples of automorphic representations.

Lemma 6.2.4. *Consider a simple, simply-connected $\mathbb{Q}$-subgroup $\boldsymbol{J}$ of $\boldsymbol{GL}(d)$ and a finite set $S = \{\infty\} \cup S_f$ of primes. Let Λ be a congruence subgroup of Λ_S. Suppose that J_∞ is non-compact. The natural unitary representation of J_∞ on $L^2(J_S/\Lambda)$ is automorphic.*

Proof. First, let's see that it is enough to treat the case where Λ is a principal congruence subgroup of Λ_S. If Λ' is a finite-index subgroup of Λ, the natural map $F : J_S/\Lambda' \to J_S/\Lambda$ is a J_S-equivariant finite covering, thus we can identify $L^2(J_S/\Lambda)$ with the subspace of functions in $L^2(J_S/\Lambda')$ constant on almost every fiber of F. So let's assume that $\Lambda = \Lambda_S(N)$ with N relatively prime to p_S.

We'll show that, as unitary representations of J_∞,

$$\operatorname{supp} L^2(J_S/\Lambda_S(N)) = \overline{\bigcup_{n\geq 1} \operatorname{supp} L^2(J_\infty/\Lambda_\infty(Np_S^n))}.$$

It suffices to see that there is, for $n \geq 1$, a J_∞-invariant subspace $\mathcal{H}_n$ of $\mathcal{H} = L^2(J_S/\Lambda_S(N))$ such that $\cup_{n\geq 1}\mathcal{H}_n$ is dense in $\mathcal{H}$, and the unitary representations of J_∞ on $L^2(J_\infty/\Lambda_S(Np_S^n))$ and $\mathcal{H}_n$ are isomorphic.

For p prime and $n \geq 1$ consider $K_p = GL(d, \mathbb{Z}_p), K_p^n = ker(K_p \to GL(d, \mathbb{Z}/p^n\mathbb{Z}))$ and $U_p^n = J_p \cap K_p^n$. Suppose that $S_f = \{p_1, \ldots, p_\ell\}$. We'll denote by $U_{S_f}^n$ the group $U_{p_1}^n \times \cdots \times U_{p_\ell}^n$. For every $n \geq 1$, $J_\infty \times U_{S_f}^n$ is an open subgroup of J_S, and we'll see that it acts transitively on J_S/Λ. By the Strong Approximation Theorem [PR94, Theorem 7.2], $J_\infty\Lambda$ is dense in J_S, hence $J_S = (J_\infty \times U_{S_f}^n)\Lambda$. Note that $(J_\infty \times U_{S_f}^n) \cap \Lambda_S(N) = \Lambda_\infty(Np_S^n)$, so there is an identification

$$J_S/\Lambda_S(N) \simeq (J_\infty \times U_{S_f}^n)/\Lambda_\infty(Np_S^n).$$

We then have an isomorphism of J_∞-spaces

$$J_\infty/\Lambda_\infty(Np_S^n) \simeq U_{S_f}^n \backslash (J_\infty \times U_{S_f}^n)/\Lambda_\infty(Np_S^n),$$

which identifies $L^2(J_\infty/\Lambda_\infty(Np_S^n))$ with the subspace $\mathcal{H}_n$ of $U_{S_f}^n$-invariant vectors of $\mathcal{H}$. Since the $(U_{S_f}^n)_{n\geq 1}$ are arbitrarily small, $\cup_{n\geq 1}\mathcal{H}_n$ is dense in $\mathcal{H}$[3].

□

Lemma 6.2.4 says that we can define also the automorphic spectrum of J_∞ as the closure in $\widehat{J_\infty}$ of the union of the supports, as unitary representation of J_∞, of $L^2(J_S/\Lambda)$, where S runs though all the finite sets $\{\infty\} \cup S_f$ of primes and Λ is any congruence subgroup of Λ_S. In the next chapter we'll introduce the ring $\mathbb{A}$ of adèles of $\mathbb{Q}$, thanks to which we construct a natural unitary representation of J_∞ that contains all the $L^2(J_S/\Lambda)$. The automorphic spectrum of J_∞ can be also defined more succinctly as the support of this representation.

Following Li and Margulis, here is the first technical tool—see [LM16, Lemma 5]—we'll use to prove Lemma 6.2.3. As they remark in their article, it is a consequence of two deep results from the theory of automorphic representations: the Kim-Sarnak bound for the Ramanujan Conjecture for $\mathbf{SL}(2)$ over $\mathbb{Q}$—see [Kim03, Appendix 2]—and the Jacquet-Langlands Correspondence—see [Lub94, Theorem 3.4, p. 163].

Proposition 6.2.5. *Let R be a non-degenerate integral quadratic form in 3 variables. Any $\sigma \in \widehat{Spin(R)}^{Aut}$ is either trivial or almost L^4.*

[3] A continuous function $F : J_S/\Lambda \to \mathbb{C}$ with compact support is the uniform limit as $n \to \infty$ of $F_n : x \mapsto \int_{U_{S_f}^n} F(ux)\mathrm{d}u$ and $C_c(J_S/\Lambda)$ is dense in $\mathcal{H}$.

In the proof of Lemma 6.2.3 we'll show that the unitary representation of $SO(Q,\mathbb{R})^{V'\circ}$ on $L^2_0(SO(Q_S,\mathbb{Q}_S)^\circ x_{d,S})$ is automorphic using the so-called Burger-Sarnak's Restriction Principle—see [BS91, Theorem 1.1]:

Theorem 6.2.6. *Let $\boldsymbol{J}$ be a connected semisimple linear $\mathbb{Q}$-group and let $\boldsymbol{J'}$ be a semisimple $\mathbb{Q}$-subgroup of $\boldsymbol{J}$. If π is an automorphic representation of J_∞, then $\pi\big|_{J'_\infty}$ is an automorphic representation of J'_∞.*

6.2.2 The proof of Lemma 6.2.3

Having now the adequate tools at our disposal, let's complete the proof of Lemma 6.2.3.

Proof of Lemma 6.2.3. Let R be the restriction of Q to W. We'll denote by $\mathbf{H}^R$ and $\mathbf{H}^Q$ the semisimple $\mathbb{Q}$-groups $\mathbf{SO}(R)$ and $\mathbf{SO}(Q)$. Let $\iota:\mathbf{H}^R\to\mathbf{H}^Q$ be the natural morphism of $\mathbb{Q}$-groups such that $\iota(H^R_k)=SO(Q,k)^{W_k}$ for any field extension k of $\mathbb{Q}$. Let $\mathbf{J}^R$ be the $\mathbb{Q}$-group $\mathbf{Spin}(R)$ and let $\mathcal{R}$ be the covering $\mathbf{J}^R\to\mathbf{H}^R$. We define $\mathcal{Q}:\mathbf{J}^Q\to\mathbf{H}^Q$ in the same fashion. To become familiar with the new notation, remark that $SO(Q,\mathbb{Q}_S)^\circ=\mathcal{Q}_S(J^Q_S)$. The composition $\iota\circ\mathcal{R}$ lifts to $\widetilde{\iota}:\mathbf{J}^R\to\mathbf{J}^Q$, so we have the commutative diagram

$$\begin{array}{ccc}\mathbf{J}^R & \xrightarrow{\ \widetilde{\iota}\ } & \mathbf{J}^Q\\ \Big\downarrow{\scriptstyle\mathcal{R}} & & \Big\downarrow{\scriptstyle\mathcal{Q}}\\ \mathbf{H}^R & \xrightarrow[\ \iota\ ]{} & \mathbf{H}^Q\end{array}$$

We denote $\Lambda=\mathcal{Q}_S^{-1}(H^Q_S\cap\Gamma_{d,S})$, which is a congruence subgroup of J^Q_S. To see that the unitary representation of $SO(Q,\mathbb{R})^{V'\circ}$ on $L^2_0(\mathcal{Q}_S(J^Q_S)x_{d,S})$ is almost L^4, it suffices to show that one of J^R_∞ on $L^2_0(J^Q_S/\Lambda)$ is almost L^4, because $\mathcal{R}_\infty$ has finite kernel and by the commutativity of the diagram. We see $\mathbf{J}^R$ as a $\mathbb{Q}$-subgroup of $\mathbf{J}^Q$ using $\widetilde{\iota}$. The unitary representation π of J^Q_∞ on $L^2_0(J^Q_S/\Lambda)$ is automorphic by Lemma 6.2.4, hence $\sigma=\pi\big|_{J^R_\infty}$ is automorphic by Theorem 6.2.6. Proposition 6.2.5 says that an irreducible automorphic representation of J^R_∞ is either trivial or almost L^4, hence we have to show that the trivial representation of J^R_∞ is not weakly contained in σ. If this happens, then σ would have a non-zero J^R_∞-invariant vector[4], which is impossible. Indeed, if $\varphi\in L^2_0(J^Q_S/\Lambda)$ is J^R_∞-invariant, then φ is J^Q_∞-invariant by the Howe-Moore phenomenon—see Lemma 8.3.8. Since J^Q_∞ is normal in J^Q_S, then φ—as function on J^Q_S—is J^Q_∞-invariant on the right. The group J^Q_∞ is non-compact, so $J^Q_\infty\Lambda$ is dense in J^Q_S by the Strong Approximation Theorem—see [PR94, Theorem 7.12]. This shows that φ is almost surely constant. Recall that $\int_{Y'}\varphi=0$, so the only possibility is $\varphi=0$. □

6.3 Preparing to apply the mixing speed

Suppose that $y_1=fx_{d,S}$ and $y_2=gx_{d,S}$ are in a closed H°_S-orbit Y' in $X_{d,S}$. To prove Proposition 6.0.1, we'll apply Proposition 6.2.1 to smooth functions φ_1,φ_2 supported on

[4]Because the trivial representation is an isolated point in $\widehat{J^R}^{Aut}$ by Proposition 6.2.5.

small neighborhoods $\mathcal{U}_1, \mathcal{U}_2$ of y_1 and y_2. We have to estimate the L^2-norms of φ_i and of some derivative of it, so it will be convenient to choose $\mathcal{U}_i$ that identifies with a neighborhood of the identity in H_S, in that way we can do the computations *on* H_S. We take care of this in 6.3.1, and in 6.3.2 we construct the bump function on H_S that we'll use to define the $\varphi_i's$.

6.3.1 Injectivity radius in $X_{d,S}$

For any $r > 0$ we define

$$G_{\infty,d}(r) = \{g_\infty \in G_{\infty,d}(r) \mid ||g_\infty - I_d||_\infty < r \text{ and } ||g_\infty^{-1} - I_d||_\infty < r\},$$

and

$$G_{d,p}(r) = \{g_p \in G_{d,p} \mid ||g_p - I_d||_p \leq r \text{ and } ||g_p^{-1} - I_d||_p \leq r\}.$$

For $g \in G_{d,S}$ and $\nu \in S$ we denote

$$r_\nu(g) = T_\nu^{-1}(g) = \frac{|\det g_\nu|_\nu}{||g_\nu||_\nu^d},$$

and

$$\mathscr{B}_S^g = G_{\infty,d}\left(\frac{r_\infty(g)}{3d^2 \cdot d!}\right) \times \prod_{p \in S_f} G_{d,p}(r_p(g)).$$

Lemma 6.3.1. *The map $\mathscr{B}_S^g \to X_{d,S}$, $f \mapsto fgx_{d,S}$ is injective for any $g \in G_{d,S}$.*

We'll use the following observation in the proof of Lemma 6.3.1.

Lemma 6.3.2. *The ball $G_{d,p}(r)$ is a compact-open subgroup of $G_{d,p}$ for any $0 < r \leq 1$.*

Proof. Consider $g_p \in G_{d,p}$. If $||g_p - I_d||_p \leq 1$, then g_p has coefficients in $\mathbb{Z}_p$ because

$$||g_p||_p \leq \max\{||g_p - I_d||_p, ||I_d||_p\} = 1.$$

This implies that $G_{d,p}(1) = GL(d, \mathbb{Z}_p)$ of $G_{d,p}$. More generally we have

$$G_{d,p}(p^{-n}) = \ker(GL(d, \mathbb{Z}_p) \to GL(d, \mathbb{Z}/p^n\mathbb{Z}))$$

for any positive integer n. □

Proof of Lemma 6.3.1. The statement is equivalent to

$$(g^{-1}(\mathscr{B}_S^g)^{-1}\mathscr{B}_S^g g) \cap \Gamma_{d,S} = \{I_d\}$$

for any $g \in G_{d,S}$. Suppose that $f, h \in \mathscr{B}_S^g$ and $\gamma = (\gamma_0, \ldots, \gamma_0) \in \Gamma_{d,S}$ verify $\gamma = g^{-1}f^{-1}hg$. We'll prove that $\gamma_0 - I_d$ has integral coefficients and $||\gamma_0 - I_d||_\infty < 1$. Note that $f_p^{-1}h_p$ is in $G_{d,p}$ for $p \in S_f$ since $r_p(g) \leq 1$. Hence:

$$\begin{aligned} ||\gamma_0 - I_d||_p &= ||g_p^{-1}(f_p^{-1}h_p - I_d)g_p||_p \\ &\leq ||g_p^{-1}||_p||g_p||_p||f_p^{-1}h_p - I_d||_p \\ &\leq \frac{||g_p||_p^d}{|\det g_p|_p} \cdot r_p(g) = 1, \end{aligned}$$

so $\gamma - I_d$ has integral coefficients. The computation in the real coordinate is similar:

$$\begin{aligned}
||\gamma_0 - I_d||_\infty &= ||g_\infty^{-1}(f_\infty^{-1}h_\infty - I_d)g_\infty||_\infty \\
&\leq d^2||g_\infty^{-1}||_\infty||g||_\infty||f_\infty^{-1}h_\infty - I_d||_\infty \\
&\leq \frac{d\cdot d!}{r_\infty(g)}(||f_\infty^{-1}h_\infty - f_\infty^{-1}||_\infty + ||f_\infty^{-1} - I_d||_\infty) \\
&< \frac{d^2\cdot d!}{r_\infty(g)}(||f_\infty^{-1}||_\infty||h_\infty - I_d||_\infty + ||f_\infty^{-1} - I_d||_\infty) \\
&< \frac{d^2\cdot d!}{r_\infty(g)}\cdot\frac{r_\infty(g)}{3d^2\cdot d!}\left(\frac{r_\infty(g)}{3d^2\cdot d!} + 2\right) \\
&\leq \frac{1}{3}\left(\frac{1}{3d^2} + 2\right) < 1.
\end{aligned}$$

The only integral matrix with ∞-norm strictly less than 1 is the zero matrix, so $\gamma_0 = I_d$. $\square$

6.3.2 Bump functions on closed H_S°-orbits

Let H_S be the orthogonal group of a standard quadratic form $P = (P_\nu)_{\nu\in S}$ on $\mathbb{Q}_S^d$ and suppose that $Y' = H_S^\circ g x_{d,S}$ is closed in $X_{d,S}$. We define $\mathcal{U}^g = (\mathscr{B}_S^g \cap H_S)gx_{d,S}, r_g = \frac{r_\infty(g)}{3d^2\cdot d!}$ and $\varphi_g : Y' \to [0,\infty)$ as

$$\varphi_g(y) = \begin{cases} \psi_{r_g}(b_\infty) & \text{if } y = bgx_{d,S} \text{ with } b \in H_S \cap \mathscr{B}_S^g, \\ 0 & \text{if } y \in Y' - \mathcal{U}^g. \end{cases}$$

Here ψ_{r_g} is as in Lemma A.2.18. The function φ_g is well-defined—recall that $\mathscr{B}_S^g \to X_{d,S}, b \mapsto bgx_{d,S}$ is injective by Lemma 6.3.1—, H_∞°-smooth and has support in $\mathcal{U}^g$. Here we prove some properties of φ_g that we'll use in the proof of Proposition 6.0.1. We'll use freely the properties of ψ_{r_g} proved in Lemma A.2.18. Before doing computations, we remind the reader that if $P_\nu(x) = a_1x_1^2 + \cdots + a_dx_d^2$, we endow H_ν with the Haar measure induced by the basis

$$E_{ij} - a_ia_j^{-1}E_{ji}, \quad 1 \leq i < j \leq d$$

of the Lie algebra of H_ν—see the introduction of Appendix A. We have

$$\begin{aligned}
\int_{Y'}\varphi_g \mathrm{d}\mu_{Y'} &= \int_{H_S\cap\mathscr{B}_S^g}\psi_{r_g}(b_\infty)\mathrm{d}\lambda_{H_S}(b) \\
&= \lambda_{H_{S_f}}(H_{S_f}\cap\mathscr{B}_{S_f}^g)\int_{H_\infty(r_g)}\psi_{r_g}(b_\infty)\mathrm{d}\lambda_{H_\infty}(b_\infty) \\
&= (p_S^{-3}r_{S_f}(g))^{\frac{1}{2}d(d-1)} < 1,
\end{aligned}$$

where $r_{S_f}(g) = \prod_{p\in S_f} r_p(g)$. To get the last line we used the volume formula of Corollary A.2.12. Note that $r_p(g) \leq 1$ for $p \in S_f$, hence $p_S^{-3} r_{S_f}(g) < 1$. Similarly we have

$$\begin{aligned} ||\varphi_g||_{L^2(Y')} &= \left(\int_{H_S \cap \mathscr{B}_S^g} \psi_{r_g}^2(b_\infty) \mathrm{d}\lambda_{H_S}(b) \right)^{\frac{1}{2}} \\ &= \lambda_{H_{S_f}}(H_{S_f} \cap \mathscr{B}_{S_f}^g)^{\frac{1}{2}} ||\psi_{r_g}||_{L^2(H_\infty)} \\ &< \mathcal{M}_d r_g^{-(\frac{1}{4}d(d-1)+1)} \\ &= (3d^2 \cdot d!)^{\frac{1}{4}d(d-1)+1} \mathcal{M}_d r_\infty(g)^{-(\frac{1}{4}d(d-1)+1)}, \end{aligned} \tag{6.3}$$

where $\mathcal{M}_d$ is as in Lemma A.2.18, and[5]

$$\begin{aligned} ||\mathcal{X}_{H_\infty}(\varphi_g)||_{L^2(Y')} &\leq ||\mathcal{X}_{H_\infty}(\psi_{r_g})||_{L^2(H_\infty)} \\ &\leq (3d^2 \cdot d!)^{\frac{1}{4}d(d-1)+1} \mathcal{M}_d ||\mathcal{X}_{H_\infty}||_\infty r_\infty(g)^{-(\frac{1}{4}d(d-1)+1)} \\ &= 2(3d^2 \cdot d!)^{\frac{1}{4}d(d-1)+1} \mathcal{M}_d r_\infty(g)^{-(\frac{1}{4}d(d-1)+1)}. \end{aligned} \tag{6.4}$$

Recall that $||\varphi_g||_{\mathcal{X}_{H_\infty}} = (||\varphi_g||^2_{L^2(Y')} + ||\mathcal{X}_{H_\infty}(\varphi_g)||^2_{L^2(Y')})^{\frac{1}{2}}$. Combining (6.3) and (6.4) we obtain

$$||\varphi_g||_{\mathcal{X}_{H_\infty}} \leq \mathcal{N}_d r_\infty(g)^{-(\frac{1}{4}d(d-1)+1)},$$

where $\mathcal{N}_d = 3(3d^2 \cdot d!)^{\frac{1}{4}d(d-1)+1} \mathcal{M}_d$. We gather these properties of φ_g in the next lemma.

Lemma 6.3.3. *Consider a finite set of primes $S = \{\infty\} \cup S_f$ and $d \geq 3$. Let H_S be the orthogonal group of a standard quadratic form on $\mathbb{Q}_S^d$. Suppose that H_∞ is non-compact. Take $g \in G_{d,S}$ such that $Y' = H_S^\circ g x_{d,S}$ is closed. The function $\varphi_g : Y' \to [0,\infty)$ has support in $\mathcal{U}^g$, is H_∞°-smooth,*

$$||\varphi_g||_{L^1(Y')} = (p_S^{-3} r_{S_f}(g))^{\frac{1}{2}d(d-1)} < 1,$$

and

$$||\varphi_g||_{\mathcal{X}_{H_\infty}} \leq \mathcal{N}_d r_\infty(g)^{-(\frac{1}{4}d(d-1)+1)}.$$

6.4 The proof of the dynamical statement

We are finally ready to prove the main result of this chapter.

Proof of Proposition 6.0.1. Let's choose $\eta \in H_S$ such that $\eta g x_{d,S}$ and $f x_{d,S}$ are in the closed H_S°-orbit $Y' \subseteq Y$ in $X_{d,S}$, η_∞ is a diagonal matrix with ± 1 in the main diagonal, $||\eta_p||_p \leq p$ for odd $p \in S_f$ and $||\eta_2||_2 \leq 4$ if $2 \in S_f$[6].

Consider the H_∞°-smooth functions $\varphi_1 := \varphi_{\eta g}, \varphi_2 = \varphi_f : Y' \to [0,\infty)$ of Lemma 6.3.3, supported respectively in the open subsets $\mathcal{U}^{\eta g}$ and $\mathcal{U}^f$ of Y'. By Proposition 6.2.1 and

[5] Here $\mathcal{X}_{H_\infty} \in \mathfrak{h}_\infty$ is as in Proposition 6.2.1.

[6] This is possible thanks to lemmas 3.4.1 and 3.4.3 when H_p is non-compact and Lemma 3.3.12 when H_p is compact.

Lemma 6.3.3 we have

$$\left|\int_{Y'}(\varphi_1\circ\rho(a_{\infty,-t}))\overline{\varphi_2}\mathrm{d}\mu_Y-\frac{(p_S^{-6}r_{S_f}(f)r_{S_f}(\eta g))^{\frac{1}{2}d(d-1)}}{\mu_Y(Y')}\right|_\infty \leq \mathcal{D}e^{-\frac{t}{6}}||\varphi_1||_{\mathcal{X}_{H_\infty}}||\varphi_2||_{\mathcal{X}_{H_\infty}}$$
$$\leq \mathcal{D}\mathcal{N}_d^2e^{-\frac{t}{6}}(r_\infty(f)r_\infty(g))^{-(\frac{1}{4}d(d-1)+1)}. \tag{6.5}$$

Recall that $\rho=\rho_{H_\infty}$ is the morphism $SL(2,\mathbb{R})\to H_\infty$ of Proposition 6.2.1. Let's assume that $(\rho(a_{\infty,t})\mathcal{U}^{\eta g})\cap\mathcal{U}^f=\emptyset$ for any $t\in[0,1]$[7]. Then, for any such t, $\int_{Y'}(\varphi_1\circ\rho(a_{\infty,t}))\overline{\varphi_2}\mathrm{d}\mu_{Y'}=0$, so (6.5) yields

$$\frac{(p_S^{-6}r_{S_f}(f)r_{S_f}(\eta g))^{\frac{1}{2}d(d-1)}}{\mu_Y(Y')}\leq\mathcal{D}\mathcal{N}_d^2e^{-\frac{t}{6}}(r_\infty(f)r_\infty(g))^{-(\frac{1}{4}d(d-1)+1)}. \tag{6.6}$$

Let t_0-1 be positive number for which we have equality in (6.6) for $t=t_0-1$. Then

$$\mathcal{D}\mathcal{N}_d^2e^{-\frac{t_0}{6}}(r_\infty(f)r_\infty(g))^{-(\frac{1}{4}d(d-1)+1)}<\frac{(p_S^{-6}r_{S_f}(f)r_{S_f}(\eta g))^{\frac{1}{2}d(d-1)}}{\mu_Y(Y')}.$$

Let $h'_\infty=\rho(b_{\infty,t_0})$. From (6.5) we deduce that

$$\int_{Y'}(\varphi_1\circ(h'_\infty)^{-1})\overline{\varphi_2}\mathrm{d}\mu_Y(Y')\neq 0,$$

so $h'_\infty\mathcal{U}^{\eta g}$ meets $\mathcal{U}^f$. Thus there are

$$s\in\mathscr{B}_S^{\eta g}\cap H_S^\circ\quad\text{and}\quad t\in\mathscr{B}_S^f\cap H_S^\circ$$

such that $(t^{-1}h'_\infty s)\eta g x_{d,S}=fx_{d,S}$. We set $h^\star=t^{-1}h'_\infty s\eta$. For $p\in S_f$ we have

$$||h_p^\star||_p=||t_p^{-1}s_p\eta_p||_p\leq||\eta_p||_p\leq\begin{cases}p & \text{if } p>2,\\ 4 & \text{if } p=2.\end{cases}$$

It remains only to prove the bound for $||h_\infty^\star||_\infty$. Before doing so, note that by the choice of t_0 we have

$$(p_S^{-6}r_{S_f}(f)r_{S_f}(\eta g))^{\frac{1}{2}d(d-1)}=\mathcal{D}\mathcal{N}_d^2e^{\frac{1}{6}}e^{-\frac{t_0}{6}}(r_\infty(f)r_\infty(g))^{-(\frac{1}{4}d(d-1)+1)}\mu_Y(Y'),$$

so

$$\begin{aligned}e^{t_0}&<3\mathcal{D}^6\mathcal{N}_d^{12}p_S^{18d(d-1)}(r_{S_f}(f)r_{S_f}(\eta g))^{-3d(d-1)}(r_\infty(f)r_\infty(g))^{-(\frac{3}{2}d(d-1)+6)}\mu_Y(Y)^6\\&<3\cdot2^{3d^2(d-1)}\mathcal{D}^6\mathcal{N}_d^{12}p_S^{9d^3}(r_{S_f}(f)r_{S_f}(g))^{-3d(d-1)}(r_\infty(f)r_\infty(g))^{-(\frac{3}{2}d(d-1)+6)}\mu_Y(Y)^6.\end{aligned}$$

[7] If this is not the case there is $h^\star\in H_S$ such that $h^\star g x_{d,S}=fx_{d,S}$, $||h_p^\star||_p\leq p$ for odd $p\in S_f$, $||h_2^\star||_2\leq 4$ if $2\in S_f$ and $||h_\infty^\star||_\infty<12d^2$.

To obtain the last line we use that $r_{S_f}(\eta g)^{-1} \leq 2^d p_S^d r_{S_f}(g)^{-1}$ by the choice of η[8]. Recall that $T_\nu(g) = r_\nu(g)^{-1}$ by definition. Now

$$\begin{aligned}
||h^\star_\infty||_\infty &= ||t_\infty^{-1} h'_\infty s_\infty \eta_\infty||_\infty \\
&\leq d^2 ||t_\infty^{-1}||_\infty ||s_\infty||_\infty ||h'_\infty||_\infty \\
&\leq 4d^2 ||h'_\infty||_\infty \\
&< 12 \cdot 2^{3d^2(d-1)} \mathcal{D}^6 \mathcal{N}_d^{12} d^2 p_S^{9d^3} (r_{S_f}(g) r_{S_f}(g))^{-3d(d-1)} (r_\infty(f) r_\infty(g))^{-(\frac{3}{2}d(d-1)+6)} \mu_Y(Y)^6 \\
&= C_d p_S^{9d^3} (T_{S_f}(g) T_{S_f}(g))^{3d(d-1)} (T_\infty(f) T_\infty(g))^{\frac{3}{2}d(d-1)+6} \mu_Y(Y)^6,
\end{aligned}$$

which completes the proof. □

[8] In fact $r_{S_f}(\eta g)^{-1} \leq p_S^d r_{S_f}(g)^{-1}$ if $2 \notin S_f$.

Chapter 7

Dynamical statement II: $\mathbb{R}$-anisotropic case

The purpose of this chapter is to establish Proposition 5.2.3, which is the main ingredient of the proof of the criterion of $\mathbb{Z}_S$-equivalence of $\mathbb{R}$-anisotropic integral quadratic forms—Theorem 5.1.2. We'll use the same notation as in Chapter 6.

Consider a finite set $S = \{\infty\} \cup S_f$ of primes and $d \geq 3$. We look at the action of H_S—the orthogonal group of a standard quadratic form on $\mathbb{Q}_S^d$—on the space $X_{d,S}$ of lattices of $\mathbb{Q}_S^d$, but now H_∞ is compact. An important difference with respect to the dynamical setting in the previous chapter is that closed H_S-orbits in $X_{d,S}$ are compact[1]. Here is the main result we'll prove.

Proposition 7.0.1. *Consider a finite set of primes $S = \{\infty\} \cup S_f$ and $d \geq 3$. Let H_S be the orthogonal group of a standard quadratic form on $\mathbb{Q}_S^d$. Suppose that H_∞ is compact and H_{p_0} is non-compact for some $p_0 > 2$ in S_f. Take $f, g \in G_{d,S}$ such that $fx_{d,S}$ and $gx_{d,S}$ are in a compact H_S-orbit Y in $X_{d,S}$. Then there is $h^\star \in H_S$ such that $h^\star g x_{d,S} = f x_{d,S}$,*

$$||h_{p_0}^\star||_{p_0} \leq F_d p_S^{13d^2} (T_{p_0}(f)T_{p_0}(g))^6 (T_S(f)T_S(g))^{d(d-1)} \mu_Y(Y)^4,$$

$||h_p^\star||_p \leq p$ for odd $p \in S_f - \{p_0\}$ and $||h_2^\star||_2 \leq 4$ is $2 \in S_f$.

Remark 7.0.2. *The assumption $p_0 > 2$ can be removed easily, we just need to extend Lemma 3.5.3 to $p = 2$.*

The main idea behind the proof of Proposition 7.0.1 is now an effective uniform mixing speed—Proposition 7.1.1—for the action of $H_{p_0}^\circ$ on compact H_S°-orbits in $X_{d,S}$, which is the topic of Section 7.1. Having this, we prove Proposition 7.0.1 in Section 7.2. Many arguments will be identical to those in Chapter 6, so we'll take the liberty of skipping some details.

7.1 Mixing speed for compact H_S°-orbits

Once more we'll state the mixing speed for compact H_S°-orbits just for a copy in H_{p_0} of an orthogonal group of a ternary quadratic form.

[1]Indeed, if $H_S g x_{d,S}$ is closed, $g^{-1} H_S g = O(Q, \mathbb{Q}_S)$ for a non-degenerate integral quadratic form Q, and $g^{-1} H_S g x_{d,S}$ is homeomorphic to $O(Q, \mathbb{Q}_S)/O(Q, \mathbb{Z}_S)$, which is compact since $O(Q, \mathbb{R})/O(Q, \mathbb{Z})$ is compact—see [Ben09, Theorem 5.8, p.48].

Consider $p > 2$. Suppose that H_p is the orthogonal group of a standard isotropic quadratic form P on $\mathbb{Q}_p^d$. Then

$$P(x) = x_1^2 - x_2^2 + a_3x_3^2 + \cdots$$

and $R(x) = x_1^2 - x_2^2 + a_3x_3^2$ is a standard isotropic quadratic form on $V = \mathbb{Q}_pe_1 \oplus \mathbb{Q}_pe_2 \oplus \mathbb{Q}_pe_3$. We define the morphism $\rho_{H_p} : SL(2, \mathbb{Q}_p) \to H_p^\circ$ as the composition

$$SL(2, \mathbb{Q}_p) \xrightarrow{\iota_p} SO(R, \mathbb{Q}_p)^\circ \longrightarrow H_p^{V\circ} \hookrightarrow H_p^\circ,$$

with ι_p as in Lemma 3.5.3[2]. For any positive integer m we denote

$$a_{p,m} = \begin{pmatrix} p^m & 0 \\ 0 & p^{-m} \end{pmatrix} \in SL(2, \mathbb{Q}_p). \tag{7.1}$$

Let $K_{d,p} = GL(d, \mathbb{Z}_p)$ and $K_{d,p}(n) = ker(K_{d,p} \to GL(d, \mathbb{Z}/p^n\mathbb{Z}))$. Here is the uniform mixing speed.

Proposition 7.1.1. *Consider a finite set $S = \{\infty\} \cup S_f$ of primes and $d \geq 3$. Let H_S be the orthogonal group of a standard quadratic form on $\mathbb{Q}_S^d$. Suppose that H_∞ is compact and H_{p_0} is non-compact for some $p_0 > 2$. Let $\rho = \rho_{H_{p_0}} : SL(2, \mathbb{Q}_{p_0}) \to H_{p_0}^\circ$ as defined above. Consider a compact H_S°-orbit Y' in $X_{d,S}$ and L^2-functions φ_1 and φ_2 on Y' that are respectively $H_{p_0}^\circ \cap (K_{d,p_0}(n_1))$ and $H_{p_0}^\circ \cap (K_{d,p_0}(n_2))$-invariant. Then*

$$\left| \int_{Y'} (\varphi_1 \circ \rho(a_{p_0,-m}))\overline{\varphi_2} d\mu_{Y'} - \frac{\int_{Y'} \varphi_1 d\mu_{Y'} \int_{Y'} \overline{\varphi_2} d\mu_{Y'}}{\mu_{Y'}(Y')} \right| \leq p_0^{-\frac{m}{2}} \left(10 p_0^{\frac{3}{2}(n_1+n_2+2)} ||\varphi_1||_{L^2} ||\varphi_2||_{L^2} \right).$$

Lemma 7.1.2 shows that the unitary representation of $H_{p_0}^{V\circ}$ on $L_0^2(Y')$ is tempered. Let's see first how to deduce Proposition 7.1.1 form Lemma 7.1.2: the unitary representation $SL(2, \mathbb{Q}_{p_0}) \curvearrowright L_0^2(Y')$ (through ρ) is also tempered since ι_{p_0} is a finite covering. Using Lemma 3.5.3 we see that

$$\rho(K_{2,p_0}(n+1) \cap SL(2, \mathbb{Q}_p)) \subset K_{d,p_0}(n),$$

thus φ_i is invariant with respect to $K_{2,p_0}(n_i + 1) \cap SL(2, \mathbb{Q}_p)$. Then the inequality of Proposition 7.1.1 is obtained by applying Corollary 4.3.7 to ψ_1 and ψ_2, the orthogonal projections of φ_1, φ_2 to $L_0^2(Y')$, and using that $||\psi_i||_{L^2} \leq ||\varphi_i||_{L^2}$.

The fact that $H_{p_0}^{V\circ} \curvearrowright L_0^2(Y')$ is tempered follows from the next result in the same way that Lemma 6.2.3 implies Lemma 6.2.2.

Lemma 7.1.2. *Let $S = \{\infty\} \cup S_f$ be a finite set of primes and let Q be an $\mathbb{R}$-anisotropic integral quadratic form in $d \geq 3$ variables. Consider a 3-dimensional linear subspace W of $\mathbb{Q}^d$, $p_0 \in S_f$ and $V' = W_{\mathbb{Q}_{p_0}}$. Suppose that $Q\big|_{V'}$ is isotropic and non-degenerate. Then the unitary representation of $SO(Q, \mathbb{Q}_{p_0})^{V'\circ}$ on $L_0^2(SO(Q, \mathbb{Q}_S)^\circ x_{d,S})$ is tempered.*

In 7.1.1 and 7.1.3 we introduce the tools we'll use in the proof of Lemma 7.1.2, which we give in 7.1.4.

[2]As in the real case, if W is a linear subspace of $\mathbb{Q}_p$ on which P is non-degenerate, H_p^W consists of the $h \in H_p$ such that $h(W) = W$ and h acts as the identity on the P-orthogonal complement of W.

7.1.1 Automorphic representations at finite primes

Let $\mathbf{J}$ be a connected semisimple $\mathbb{Q}$-subgroup of $\mathbf{GL}(d)$. In Chapter 6 we defined the automorphic spectrum of J_∞, and now we extend this notion to J_p. For a finite set of primes $S = \{\infty\} \cup S_f$, let Λ_S be the diagonal copy of $J_{\mathbb{Z}_S}$ in J_S and let $\Lambda_S(N)$ be the corresponding principal congruence subgroup for any natural number N relatively prime to p_S. If π is a unitary representation of J_S and $S' \subseteq S$, we'll denote by $\mathrm{supp}_{S'}\pi$ the support of the restriction of π to $J_{S'}$. We endow $\widehat{J_S}$ with its Fell topology. The automorphic spectrum of J_p is the subset of $\widehat{J}_p$ given by

$$\widehat{J}_p^{\,Aut} = \overline{\bigcup_{p \nmid N} \mathrm{supp}_p L^2(J_{S_p}/\Lambda_{S_p}(N))}.$$

The proof of the next lemma goes along the same lines as the proof of Lemma 6.2.4[3].

Lemma 7.1.3. *Let $\boldsymbol{J}$ be a simple connected $\mathbb{Q}$-group and let $S = \{\infty\} \cup S_f$ be a finite set of primes. Suppose that J_p is non-compact for some $p \in S_f$. Then the unitary representation of J_p on $L^2(J_S/\Lambda)$ is automorphic, for any congruence subgroup Λ of Λ_S.*

We'll need an extension of the Restriction Principle of Burger and Sarnak—Theorem 6.2.6—to finite primes.

Theorem 7.1.4. *Let $\boldsymbol{J}' \subseteq \boldsymbol{J}$ be connected semisimple $\mathbb{Q}$-groups and let ν be a prime number. The restriction to J'_ν of an automorphic representation of J_ν is automorphic.*

This result is proved by Clozel and Ullmo [CU04, Théorème 5.1][4].

7.1.2 Unitary representations of adelic groups

We make a small technical detour to explain the form of irreducible unitary representations of adelic groups.

The *ring of adèles* $\mathbb{A}$ of $\mathbb{Q}$ is the restricted product of all the $\mathbb{Q}_\nu$ with respect to $(\mathbb{Z}_p)_p$. In concrete terms, $\mathbb{A}$ consists of the $a \in \prod_\nu \mathbb{Q}_\nu$ such that a_p is in $\mathbb{Z}_p$ for almost every p[5], endowed with the topology having as basis all the subsets of the form $\prod_\nu \mathcal{U}_\nu$, where $\mathcal{U}_\nu$ is an open subset of $\mathbb{Q}_\nu$ and $\mathcal{U}_p = \mathbb{Z}_p$ for almost every p. The sum and multiplication on $\mathbb{A}$ are defined component-wise. $\mathbb{A}$ is a locally compact topological ring. We work with the Haar measure $\lambda_{\mathbb{A}}$ of $\mathbb{A}$ determined by

$$\lambda_{\mathbb{A}}(\mathcal{U}) = \prod_\nu \lambda_{\mathbb{Q}_\nu}(\mathcal{U}_\nu),$$

for any basic open subset $\mathcal{U} = \prod_\nu \mathcal{U}_\nu$. If $r \in \mathbb{Q}$, then r is a p-adic integer for almost any p, hence there is a diagonal embedding $\mathbb{Q} \hookrightarrow \mathbb{A}$, whose image we identify with $\mathbb{Q}$. Consider the subset

$$\mathcal{W} = (-1, 1) \times \prod_p \mathbb{Z}_p$$

[3] Minor modifications are required. For example, when applying the Strong Approximation Theorem: since we are not assuming that $\mathbf{J}$ is simply connected, $J_p\Lambda$ might not be dense in J_S, but its closure is a finite index subgroup of J_S.

[4] See also [CU04, Section 5.4, p. 227], where it's shown that it's not necessary to ask for $\mathbf{J}$ simply connected.

[5] This means for all except finitely many p.

of $\mathbb{A}$. Note that $\mathbb{Q}$ is a lattice in $\mathbb{A}$ since $\mathbb{Q} \cap \mathcal{W} = \{0\}$ and $\mathbb{A} = \mathbb{Q} + \mathcal{W}$.

Consider now a $\mathbb{Q}$-subgroup $\mathbf{H}$ of $\mathbf{GL}(d)$. The adelic group $H_{\mathbb{A}}$ is the restricted product of the H_ν with respect to $(U_p)_p$, where $U_p = H_p \cap GL(d, \mathbb{Z}_p)$. It is a locally compact group, and one can describe its unitary dual in terms of the $\widehat{H_\nu}$ when $\mathbf{H}$ satisfies a technical condition: we say that $\mathbf{H}$ is *nice* if H_ν is a group of type I—for this definition, see [GGPS69, p. 222]—for every ν and, for almost any p, the subspace $\mathcal{H}_{\sigma_p}^{U_p}$ of U_p-invariant vectors of $\mathcal{H}_{\sigma_p}$ is of dimension at most one for any $\sigma_p \in \widehat{H_p}$. The unitary representation σ_p is *spherical* if $\dim \mathcal{H}_{\sigma_p}^{U_p} = 1$.

Assume that $\mathbf{H}$ is nice. Here is the construction of irreducible representations of $H_{\mathbb{A}}$: Consider an irreducible unitary representation σ_ν of H_ν for each prime ν. Suppose that σ_p is spherical for almost any p and, for such p, choose an U_p-invariant unit vector $w_p \in \mathcal{H}_{\sigma_p}$. The restricted tensor product $\sigma = \otimes_\nu \sigma_\nu$ is defined as follows: Let $\mathcal{H}'_\sigma$ be the linear span of the vectors $\otimes_\nu v_\nu$ with $v_\nu \in \mathcal{H}_{\sigma_\nu}$ each ν and $v_p = w_p$ for almost every p. We consider the inner product

$$\langle \otimes_\nu v_\nu, \otimes_\nu v'_\nu \rangle = \prod_\nu \langle v_\nu, v'_\nu \rangle.$$

Let $(\mathcal{H}_\sigma, \langle \cdot, \cdot \rangle)$ be the Hilbert space obtained by completing $(\mathcal{H}'_\sigma, \langle \cdot, \cdot \rangle)$. The action of $H_{\mathbb{A}}$ on $\mathcal{H}_\sigma$ given by

$$\sigma(h)(\otimes_\nu v_\nu) = \otimes_\nu \sigma_\nu(h_\nu) v_\nu,$$

is a unitary representation σ. It doesn't depend on the choice of the U_p-invariant vectors w_p. The following description of $\widehat{H_{\mathbb{A}}}$ is taken from [GGPS69, p. 273, 274].

Theorem 7.1.5. *Let $\boldsymbol{H}$ be a nice $\mathbb{Q}$-subgroup of $\boldsymbol{GL}(d)$. Any irreducible unitary representation of $H_{\mathbb{A}}$ is of the form $\otimes_\nu \sigma_\nu$, where $\sigma_\nu \in \widehat{H_\nu}$ and σ_p spherical for almost any p[6]. Conversely, any unitary representation of $H_{\mathbb{A}}$ of this form is irreducible.*

We close this parenthesis with the lemma that allows to apply the previous theorem to orthogonal groups.

Lemma 7.1.6. *The special orthogonal group $\boldsymbol{SO}(Q)$ of a non-degenerate rational quadratic form Q in $d \geq 3$ variables is nice.*

7.1.3 Automorphic representations of quaternion algebras

Here we cite two important technical results we'll use to prove Lemma 7.1.2: the Jacquet-Langlands Correspondence and a representation-theoretic formulation of a famous theorem of Deligne about holomorphic modular forms. The role of these is similar to that of Proposition 6.2.5 in the previous chapter. Both are stated in terms of quaternion algebras. We start by fixing some notation.

Let D be a $\mathbb{Q}$-quaternion algebra. We'll denote by $\mathbf{G}^D$ the $\mathbb{Q}$-group of automorphisms of D. In concrete terms, for any prime ν, $G_\nu^D \simeq \mathbb{Q}_\nu^\times \backslash D_\nu^\times$ since all the automorphisms of D_ν are interior by the Skolem-Noether Theorem. Recall that we say that D is ramified at ν if D_ν is a division algebra. When this doesn't happen, $D_\nu \simeq M_2(\mathbb{Q}_\nu)$ and we say that D is split at ν. Alternatively, D ramifies or splits at ν if G_ν^D is respectively compact and non-compact. In

[6] The σ_ν are unique up to unitary equivalence.

the latter case $G_\nu^D \simeq PGL(2,\mathbb{Q}_\nu)$. Let's fix a $\mathbb{Q}$-embedding $\mathbf{G}^D \hookrightarrow \mathbf{GL}(3)$[7]. For any finite set $S = \{\infty\} \cup S_f$ of primes, let Λ_S^D be the diagonal copy of $G_{\mathbb{Z}_S}^D$ in G_S^D. We denote Λ^D the diagonal embedding of $G_{\mathbb{Q}}^D$ in $G_{\mathbb{A}}^D$.

In this chapter, the next result replaces Proposition 6.2.5.

Lemma 7.1.7. *Let D be a $\mathbb{Q}$-quaternion algebra ramified at ∞ and split at p_0. Any $\rho \in \widehat{G_{p_0}^D}^{Aut}$ is either one-dimensional or tempered.*

We'll deduce Lemma 7.1.7 from the two technical results mentioned before. Suppose that $D_{\mathbb{Q}}$ is a division algebra. The first black box is the Jacquet-Langlands Correspondence, a link between irreducible automorphic representations of $G_{\mathbb{A}}^D$ and *cuspidal representations of* $PGL(2,\mathbb{A})$. We won't cite the most general formulation, which is given in terms of the multiplicative group of D, rather than $\mathbf{G}^D$—see [Gel75, Theorems 10.1 and 10.2]. For our purposes, the following statement taken from [Lub94, Theorem 6.2.1, p. 80] is enough.

Theorem 7.1.8. *Consider $\mathbb{Q}$-quaternion algebra D and let S be the set of primes on which D ramifies. Let $\sigma' = \otimes\sigma'_\nu$ be an irreducible unitary representation of $G_{\mathbb{A}}^D$ contained in $L^2(G_{\mathbb{A}}^D/G_{\mathbb{Q}}^D)$. If σ' is not one-dimensional, there is an irreducible unitary representation $\sigma = \otimes\sigma_\nu$ of $PGL(2,\mathbb{A})$ contained in $L^2(PGL(2,\mathbb{A})/PGL(2,\mathbb{Q}))$ such that:*

a) σ_ν is in the discrete series of $PGL(2,\mathbb{Q}_\nu)$ if $\nu \in S$.

b) σ_ν and σ'_ν are unitary equivalent if $\nu \notin S$.

Our second black box is a theorem of Deligne, originally formulated in the language of modular forms. Again, the statement here—taken form [Lub94, Theorem 6.1.2, p. 79]—is weaker than the original one, but it spares us the work of defining cuspidal representation.

Theorem 7.1.9. *Let $\sigma = \otimes_\nu \sigma_\nu$ be an irreducible unitary representation of $PGL(2,\mathbb{A})$ contained in $L^2(PGL(2,\mathbb{A})/PGL(2,\mathbb{Q}))$. If σ_∞ is in the discrete series of $PGL(2,\mathbb{R})$, then σ_p is tempered for any $p < \infty$.*

We are ready to prove the lemma about irreducible automorphic representations of $G_{p_0}^D$

Proof of Lemma 7.1.7. To start, note that $G_{\mathbb{A}}^D/G_{\mathbb{Q}}^D$ and G_S^Q/Λ are compact since G_∞^D is compact[8], where $S = \{\infty\} \cup S_f$ is a finite set of primes and Λ is any congruence subgroup of Λ_S^D—see [Ben09, Theorem 5.8, p. 48]. Thus $L^2(G_{\mathbb{A}}^D/\Lambda^D)$ and $L^2(G_S^D/\Lambda)$ decompose as a Hilbert sum of countably many irreducible unitary representations—of $G_{\mathbb{A}}^D$ and G_S^D, respectively—, each with finite multiplicity [GGPS69, Theorem, p. 23].

Let A_{p_0} be the subset of $\widehat{G_{p_0}^D}$ consisting of the equivalence classes of one-dimensional or tempered irreducible unitary representations. Since A_{p_0} is closed[9] in $\widehat{G_{p_0}^D}$, it suffices to prove

[7] Every automorphism of D_ν is an orientation-preserving isometry of $(Im(D_\nu), N_{D_\nu})$, hence the $\mathbb{Q}$-embedding can be defined writing any automorphism in terms of a basis of D.

[8] More generally, this holds whenever D is not isomorphic to $M_2(\mathbb{Q})$. Equivalently, when D ramifies at some ν.

[9] Tempered irreducible unitary representations form a closed subset since they are the support of $L^2(G_{p_0}^D)$. Also, there are finitely many one-dimensional representations, each corresponding to a closed singleton in $\widehat{G_{p_0}^D}$—see [BdlHV08, Corollary F.2.9, p. 432].

that $\mathrm{supp}_{p_0} L^2(G^D_{S_p}/\Lambda)$ is contained in A_{p_0} for any congruence subgroup Λ of $\Lambda^D_{S_{p_0}}$. Take $\rho \in \widehat{G^D_{p_0}}$ contained in $L^2(G^D_{S_{p_0}}/\Lambda)$. As we did in the proof of Lemma 6.2.4, one can show that $L^2(G^D_{\mathbb{A}}/\Lambda^D)$ contains a subrepresentation of $G^D_{S_{p_0}}$ unitary equivalent to $L^2(G^D_{S_{p_0}}/\Lambda)$—see also [Lub94, Proposition 6.3.1, p. 82]—, hence there is an irreducible representation $\sigma' = \otimes_\nu \sigma'_\nu$ of $G^D_{\mathbb{A}}$ contained in $L^2(G^D_{\mathbb{A}}/\Lambda^D)$ such that σ'_{p_0} is unitary equivalent to ρ. Since ρ is not one-dimensional, neither is σ', so it corresponds to an irreducible unitary representation $\sigma = \otimes_\nu \sigma_\nu$ of $PGL(2,\mathbb{A})$ contained in $L^2(PGL(2,\mathbb{A})/PGL(2,\mathbb{Q}))$ by Theorem 7.1.8. Since D ramifies at ∞, σ_∞ is in the discrete series of $PGL(2,\mathbb{R})$, so σ_{p_0} is tempered by Theorem 7.1.9. As D splits at p_0, $\sigma_{p_0} \simeq \sigma'_{p_0} \simeq \rho$, so we are done. □

Now we reformulate Lemma 7.1.7 in terms of quadratic forms.

Corollary 7.1.10. *Consider a non-degenerate integral quadratic form R in 3 variables. Suppose that R is $\mathbb{R}$-anisotropic and $\mathbb{Q}_{p_0}$-isotropic. An automorphic representation of $H^R_{p_0}$ that doesn't contain one-dimensional unitary representations is tempered.*

Proof. Let D be the $\mathbb{Q}$-quaternion algebra such that $\mathbf{SO}(R)$ and $\mathbf{G}^D$ are $\mathbb{Q}$-isomorphic. Then D ramifies at ∞ and splits at p_0. Consider $A_{p_0} \subseteq \widehat{G^D_{p_0}}$ an in the proof of Lemma 7.1.7. If an automorphic representation π of $H^R_{p_0}$ contains weakly a one-dimensional representation ρ, in fact π must contain ρ since the points in A_{p_0} corresponding to one-dimensional representations are isolated in A_{p_0}. □

7.1.4 The proof of the mixing speed

We are ready to prove the representation-theoretic result that gives the effective mixing speed.

Proof of Lemma 7.1.2. Let R be the restriction of Q to W. $\mathbf{H}^Q$ and $\mathbf{H}^R$ denote the groups $\mathbf{SO}(Q)$ and $\mathbf{SO}(R)$. We extend any $h \in H^R_{\mathbb{Q}}$ to $\mathbb{Q}^d$ by the identity of the Q-orthogonal complement of W. This defines a $\mathbb{Q}$-morphism $\mathbf{H}^R \hookrightarrow \mathbf{H}^Q$, which we use to see $\mathbf{H}^R$ as $\mathbb{Q}$-subgroup of $\mathbf{H}^Q$.

The space $Y = H^Q_S x_{d,S}$ has finitely many $H^{Q\circ}_S$-orbits, say $Y'_1 = H^{Q\circ}_S x_{d,S}, \dots, Y'_\ell$. Consider the closed subspace $L^2_{00}(Y)$ of the $\varphi \in L^2(Y)$ with $\int_{Y'_i} \varphi = 0$ for $1 \leq i \leq \ell$, and the natural $H^{Q\circ}_S$-equivariant inclusion

$$L^2_0(Y'_1) \hookrightarrow L^2_{00}(Y). \tag{7.2}$$

We'll show that the unitary representation of $H^R_{p_0}$ on $L^2_{00}(Y)$ is tempered. This implies the result we seek by (7.2) and since $H^{R\circ}_{p_0}$ is an open, finite-index subgroup of $H^R_{p_0}$.

Let π be the unitary representation of H^Q_S on $L^2_{00}(Y)$. $\pi\big|_{H^Q_{p_0}}$ is automorphic by Lemma 7.1.3, so $\pi\big|_{H^R_{p_0}}$ is also automorphic thanks to Theorem 7.1.4. So, according to Corollary 7.1.10, it suffices to check that $L^2_{00}(Y)$ doesn't contain one-dimensional representations of $H^R_{p_0}$. Take $\varphi \in L^2_{00}(Y)$ such that

$$\pi(h)\varphi = \chi(h)\varphi$$

for every $h \in H^R_{p_0}$, where χ is a (unitary) character of $H^R_{p_0}$. Since χ is trivial on $H^{R\circ}_{p_0}$, φ is $H^{R\circ}_{p_0}$-invariant. As $H^{R\circ}_{p_0}$ has non-trivial unipotents, φ is $H^{Q\circ}_{p_0}$-invariant by Lemma 8.3.8.

As function on H_S^Q, φ is $H_{p_0}^{Q\circ}$-invariant on the left and Γ_S^Q-invariant on the right, where $\Gamma_S^Q = (SO(Q,\mathbb{Z}_S) \hookrightarrow H_S^Q)$. But $H_{p_0}^{Q\circ}$ is a normal subgroup of H_S^Q, thus φ is also $H_{p_0}^{Q\circ}$-invariant on the right. By the Strong Approximation Theorem, $H_S^{Q\circ}$ is contained in the analytic closure of $H_{p_0}^{Q\circ}\Gamma_S^Q$, hence φ is $H_S^{Q\circ}$-invariant on the left—thus also on the right since $H_S^{Q\circ} \trianglelefteq H_S^Q$. This shows that φ is almost surely constant on each Y_i, but recall that $\int_{Y_i'} \varphi = 0$, so necessarily $\varphi = 0$. □

7.2 The proof of the dynamical statement

Having the uniform mixing speed of Proposition 7.1.1 at our disposal, we establish now the dynamical result behind our criterion of $\mathbb{Z}_S$-equivalence for $\mathbb{R}$-anisotropic integral quadratic forms.

Proof of Proposition 7.0.1. We choose $\eta \in H_S$ such that $\eta g x_{d,S}$ and $f x_{d,S}$ are in the same compact H_S°-orbit $Y' \subseteq Y$, $||\eta_p||_p \leq p$ for odd $p \in S_f$, $||\eta_2||_2 \leq 4$ if $2 \in S_f$ and $\eta_\infty = diag(\pm 1, 1, \dots, 1)$[10].

For $g' \in G_{d,S}$, recall that we introduced in 6.3.1 the small balls

$$\mathscr{B}_S^{g'} = G_{d,\infty}\left(\frac{r_\infty(g')}{3d^2 \cdot d!}\right) \times \prod_{p\in S_f} G_{d,p}(p^{-3} r_p(g')),$$

where $r_\nu(g') = \frac{|\det g'_\nu|_\nu}{||g'_\nu||_\nu^d}$ and $r_{S'}(g') = \prod_{\nu\in S'} r_\nu(g')$ if $S' \subseteq S$. Consider the neighborhoods of $f x_{d,S}$ and $\eta g x_{d,S}$ in Y'

$$\mathcal{U} = (\mathscr{B}_S^f \cap H_S^\circ) f x_{d,S}, \quad \mathcal{V} = (\mathscr{B}_S^{\eta g} \cap H_S^\circ)\eta g x_{d,S}.$$

Let $n_2 = -\log_{p_0}(r_{p_0}(f)) + 4$. Consider $\rho : SL(2,\mathbb{Q}_{p_0}) \to H_{p_0}$ as in Proposition 7.1.1. Note that $\mathcal{U}$ is invariant under

$$H_{p_0}^\circ \cap G_{d,p_0}(p_0^{-3} r_p(f)) = H_{p_0}^\circ \cap K_{d,p_0}(p^{-(n_2-1)}).$$

In other words, $\varphi_2 = \mathbb{1}_{\mathcal{U}}$ is a $H_{p_0}^\circ \cap K_{d,p_0}(p^{-(n_2-1)})$-invariant vector of $L^2(Y')$. By the same token, if $n_1 = -\log_{p_0}(r_{p_0}(\eta g))+4$, then $\varphi_1 = \mathbb{1}_{\mathcal{V}}$ is $H_{p_0}^\circ \cap K_{d,p_0}(p^{-(n_1-1)})$-invariant. Proposition 7.1.1 applied to φ_1 and φ_2 yields

$$\begin{aligned}\left|\mu_Y((\rho(a_{p_0,m})\mathcal{V}) \cap \mathcal{U}) - \frac{\mu_Y(\mathcal{U})\mu_Y(\mathcal{V})}{\mu_Y(Y')}\right|_\infty &\leq p_0^{-\frac{1}{2}m}(10 p_0^{\frac{3}{2}(n_1+n_2)} ||\mathbb{1}_{\mathcal{U}}||_{L^2}||\mathbb{1}_{\mathcal{V}}||_{L^2}) \\ &= p_0^{-\frac{1}{2}m}(10 p_0^{12}(r_{p_0}(f) r_{p_0}(\eta g))^{-\frac{3}{2}}(\mu_Y(\mathcal{U})\mu_Y(\mathcal{V}))^{\frac{1}{2}}),\end{aligned} \tag{7.3}$$

for any $m \geq 1$. Suppose that $\rho(a_{p_0,1})\mathcal{V}$ and $\mathcal{U}$ are disjoint[11]. Let m_0 be the smallest positive integer such that the right-hand side of (7.3) is strictly smaller than $\frac{\mu_Y(\mathcal{U})\mu_Y(\mathcal{V})}{\mu_Y(Y')}$ and set

[10] As before, this is possible thanks to lemmas 3.4.1 and 3.3.12.

[11] Otherwise there is $h^\star \in H_S$ such that $h^\star g x_{d,S} = f x_{d,S}, ||h^\star_{p_0}||_{p_0} \leq p_0^4$, $||h^\star_p||_p \leq p$ for odd $p \in S_f - \{p_0\}$ and $||h^\star_2||_2 \leq 4$ if $2 \in S_f$.

$h'_{p_0} = \rho(a_{p_0,m_0})$. From (7.3) we deduce that that $h'_{p_0}\mathcal{V}$ meets $\mathcal{U}$, hence there are

$$s \in \mathscr{B}_S^f \cap H_S^\circ \quad \text{and} \quad t \in \mathscr{B}_S^{\eta g} \cap H_S^\circ$$

such that $(t^{-1}h'_{p_0}s)\eta g x_{d,S} = f x_{d,S}$. We set $h^\star = t^{-1}h'_{p_0}s\eta$, which is in H_S. For $p \in S_f - \{p_0\}$ we have

$$||h_p^\star||_p = ||t_p^{-1}s_p\eta_p||_p \leq ||\eta_p||_p \leq \begin{cases} p & \text{if } p > 2, \\ 4 & \text{if } p = 2. \end{cases}$$

Before bounding $h^\star_{p_0}$ note that by the choice of m_0

$$\frac{\mu_Y(\mathcal{U})\mu_Y(\mathcal{V})}{\mu_Y(Y')} \leq p_0^{-\frac{1}{2}m}(10p_0^{\frac{25}{2}}(r_{p_0}(f)r_{p_0}(\eta g))^{-\frac{3}{2}}(\mu_Y(\mathcal{U})\mu_Y(\mathcal{V}))^{\frac{1}{2}}),$$

thus

$$p_0^{m_0} \leq 10^2 p_0^{25}(r_{p_0}(f)r_{p_0}(\eta g))^{-3}(\mu_Y(\mathcal{U})\mu_Y(\mathcal{V}))^{-1}\mu_Y(Y)^2. \tag{7.4}$$

Since $\mathcal{U}$ and $\mathscr{B}_S^f$ have the same volume by Lemma 6.3.1, using the volume estimate of Lemma A.2.1 and Corollary A.2.12 we get

$$\mu_Y(\mathcal{U})^{-1} = \lambda_{H_S}(\mathscr{B}_S^f)^{-1} \leq \mathcal{F}_d p_S^{\frac{3}{2}d(d-1)} r_S(f)^{-\frac{1}{2}d(d-1)},$$

where $\mathcal{F}_d = \mathtt{R}_d^{-1}(3d^2 \cdot d!)^{\frac{1}{2}d(d-1)}$ with $\mathtt{R}_d$ as in Lemma A.2.1. Similarly

$$\mu_Y(\mathcal{V})^{-1} \leq \mathcal{F}_d p_S^{\frac{3}{2}d(d-1)} r_S(\eta g)^{-\frac{1}{2}d(d-1)}.$$

Now we go back to (7.4):

$$p_0^{m_0} \leq (10\mathcal{F}_d)^2 p_0^{25} p_S^{3d(d-1)}(r_{p_0}(f)r_{p_0}(\eta g))^{-3}(r_S(f)r_S(\eta g))^{-\frac{1}{2}d(d-1)}\mu_Y(Y)^2.$$

Since $||\eta_p||_p \leq p$ for odd $p \in S_f$, then $r_p(\eta g)^{-1} \leq p^d r_p(g)^{-1}$. If $2 \in S_f$, $||\eta_2||_2 \leq 4$, so $r_2(\eta g)^{-1} \leq 4^d r_2(g)^{-1}$. Thus

$$\begin{aligned} p_0^{m_0} &\leq (10\mathcal{F}_d)^2 \cdot 2^{\frac{1}{2}d^2(d-1)} p_0^{3d+25} p_S^{\frac{7}{2}d(d-1)}(r_{p_0}(f)r_{p_0}(g))^{-3}(r_S(f)r_S(g))^{-\frac{1}{2}d(d-1)}\mu_Y(Y)^2 \\ &\leq (10\mathcal{F}_d)^2 \cdot 2^{\frac{1}{2}d^2(d-1)} p_S^{\frac{1}{2}(7d^2-d+50)}(r_{p_0}(f)r_{p_0}(g))^{-3}(r_S(f)r_S(g))^{-\frac{1}{2}d(d-1)}\mu_Y(Y)^2. \end{aligned}$$

Recall that $||h'_{p_0}||_{p_0} = ||\rho(a_{p_0,m_0})||_{p_0} \leq p_0^{2m_0+1}$ by Lemma 3.5.5 and, by definition, $T_{S'}(g) = T_{S'}(g)^{-1}$ it $S' \subseteq S$. We are ready to bound $h^\star_{p_0}$:

$$\begin{aligned} ||h^\star_{p_0}||_{p_0} &= ||t_{p_0}^{-1}h'_{p_0}s_{p_0}\eta_{p_0}||_{p_0} \\ &\leq p_0^{2m_0+2} \\ &\leq (10\mathcal{F}_d)^4 \cdot 2^{d^2(d-1)} p_S^{7d^2-d+52}(r_{p_0}(f)r_{p_0}(g))^{-6}(r_S(f)r_S(g))^{-d(d-1)}\mu_Y(Y)^4 \\ &< (10\mathcal{F}_d)^4 \cdot 2^{d^2(d-1)} p_S^{13d^2}(T_{p_0}(f)T_{p_0}(g))^6(T_S(f)T_S(g))^{d(d-1)}\mu_Y(Y)^4. \end{aligned}$$

□

Chapter 8

Volume of closed H_S-orbits

The objective of this chapter is to prove Proposition 5.3.2, which gives an upper bound of the volume of the closed orbit $Y_{Q,S} \subset X_{d,S}$ associated to a non-degenerate integral quadratic form Q in $d \geq 3$. We'll recall the notation and restate the result.

Let $S = \{\infty\} \cup S_f$ be a finite set of primes. Consider the groups $G_{d,S} = GL(d, \mathbb{Q}_S)$, $\Gamma_{d,S} = (GL(d, \mathbb{Z}_S) \hookrightarrow G_{d,S})$ and the space of lattices $X_{d,S} = G_{d,S}/\Gamma_{d,S}$ of $\mathbb{Q}_S^d$ and its base point $x_{d,S} = \Gamma_{d,S}/\Gamma_{d,S}$. Let Q be a non-degenerate integral quadratic form in d variables and let P be the standard quadratic form on $\mathbb{Q}_S^d$ that is $\mathbb{Q}_S$-equivalent to Q_S[1]. We define

$$Y_{Q,S} = H_S g x_{d,S},$$

where H_S is the orthogonal group of P—we'll say that H_S is the standard conjugate of $O(Q, \mathbb{Q}_S)$—and $g \in G_{d,S}$ takes P to Q_S. The orbit $Y_{Q,S}$ is closed in $X_{d,S}$ by Lemma 6.1.1, hence it admits an H_S-invariant measure $\mu_{Y_{Q,S}}$[2] by Lemma 6.1.3. Remember that δ_Q is the determinant of the matrix of Q in the standard basis of $\mathbb{Q}^d$ and p_S is the product of the primes in S_f if $S_f \neq \emptyset$. Here is the main result of this chapter, a generalization of [LM16, Theorem 6, p. 891]. We remind the reader that an explicit value of the constant $C_d^{(2)}$, as well as all the constants that depend on d in our statements can be found in Appendix C.

Proposition 8.0.1. *Consider a finite set $S = \{\infty\} \cup S_f$ of primes and $d \geq 3$. Let Q be a non-degenerate integral quadratic form in d variables such that Q_S is isotropic. Then*

$$\mu_{Y_{Q,S}}(Y_{Q,S}) < \begin{cases} C_d^{(2)} p_S^{3d^6} \mathscr{H}_S(\delta_Q)^{\frac{d+1}{2}} & \text{if } S_f \neq \emptyset, \\ C_d^{(2)} 2^{2d^6} |\delta_Q|_\infty^{\frac{d+1}{2}} & \text{if } S = \{\infty\}. \end{cases}$$

8.1 Intermediate statements and main proof

Our proof of Proposition 8.0.1 relies on three intermediate statements. To formulate them, it is convenient to replace $X_{d,S}$ by the space $X_{d,S}^1$ of covolume 1 lattices of $\mathbb{Q}_S^d$ because the latter has finite volume. We identify $X_{d,S}^1$ with $G_{d,S}^1/\Gamma_{d,S}$, where

$$G_{d,S}^1 := \{g \in G_{d,S} \mid \mathscr{H}_S(\det g) = 1\}.$$

[1] Recall that Q_S is the quadratic form on $\mathbb{Q}_S^d$ determined by Q via the diagonal embedding $\mathbb{Q} \to \mathbb{Q}_S$.

[2] In 8.4.1 of Section 8.4 we'll fix a Haar measure on H_S, which determines the normalization of $\mu_{Y_{Q,S}}$.

Let $x^1_{d,S} = \Gamma_{d,S}/\Gamma_{d,S} \in X^1_{d,S}$, and let $\beta_{d,S}$ be the $G^1_{d,S}$-invariant measure on $X^1_{d,S}$ determined by our choice of Haar measure on $G^1_{d,S}$—see section 8.4. Consider Q, P and H_S as before. Instead of $Y_{Q,S}$, we'll work with the following subset of $X^1_{d,S}$: Write $Q = P \circ f'$ with $f' \in G_{d,S}$. Let

$$M_S(Q) = \left(\frac{\mathscr{H}_S(\delta_Q)}{\mathscr{H}_S(\delta_P)}\right)^{\frac{1}{2}}. \tag{8.1}$$

We define $N = N_S(Q) \in \mathbb{Q}_S$ as $N_\infty = M_S(Q)^{-\frac{1}{d}}$ and $N_p = 1$ for $p \in S_f$. It's easy to see that $f = N_S(Q)f'$ is in $G^1_{d,S}$, so we set

$$Y^1_{Q,S} = H_S f x^1_{d,S}.$$

Notice that $Y_{Q,S} \subseteq X_S$ and $Y^1_{Q,S} \subseteq X^1_{d,S}$ have the same volume. Indeed, both are identified with $H_S/(H_S \cap (f^{-1}\Gamma_{d,S}f))$ since conjugation by f and f' is the same. For $g \in M_d(\mathbb{Q}_S)$ we define its *S-height* as

$$\mathscr{H}_S(g) = \prod_{\nu \in S} ||g_\nu||_\nu.$$

We pass to the intermediate statements. The first one—proved in Section 8.2—says that if we move a point in $Y^1_{Q,S}$ in a transversal direction, the time it takes to get back to $Y^1_{Q,S}$ can't be arbitrarily small. In other words, the orbits $Y^1_{Q,S}$ are isolated in directions transversal to H_S. This corresponds to [LM16, Lemma 16, p. 893] in the article of Li and Margulis.

Lemma 8.1.1. *Let $S = \{\infty\} \cup S_f$ be a finite set of primes. Consider a non-degenerate integral quadratic form Q in $d \geq 3$ variables and the standard conjugate H_S of $O(Q_S, \mathbb{Q}_S)$. Take $g \in G^1_{d,S}$ and $u \in G^1_{d,S} - H_S$ with $||u_p||_p \leq 1$ for $p \in S_f$. If $gx^1_{d,S}$ and $ugx^1_{d,S}$ are in $Y^1_{Q,S}$, then*

$$||u_\infty - I_d||_\infty \geq \frac{1}{2d^3} p_S^{-1} \mathscr{H}_S(g)^{-2} \mathscr{H}_S(\delta_Q)^{-\frac{1}{d}}.$$

Consider a non-compact orthogonal group H_S of a non-degenerate quadratic form on $\mathbb{Q}^d_S$, $d \geq 3$. The second intermediate result—proved in Section 8.3—says there is a compact subset of $X^1_{d,S}$ that meets at least half of any closed H_S-orbit in $X^1_{d,S}$. This generalizes [LM16, Lemma 13, p. 892]. We need some notation for the precise statement. For any $M > 0$ we define

$$\widetilde{\Omega}_{d,S}(M) = \left\{ g \in SL^{\pm}(d, \mathbb{R}) \times \prod_{p \in S_f} GL(d, \mathbb{Z}_p) : ||g_\infty||_\infty \leq M \right\},$$

and $\Omega_{d,S}(M) = \widetilde{\Omega}_{d,S}(M)x^1_{d,S}$. Consider $\mathcal{E}_d = 2^{d^3} \cdot 3^{2d^4} d^{3d^3}$. We introduce the following compact subset of $X^1_{d,S}$

$$\Omega_{d,S} = \begin{cases} \Omega_{d,S}(\mathcal{E}_d p_S^{2d^4}) & \text{if } S_f \neq \emptyset, \\ \Omega_{\infty,d}(\mathcal{E}_d 2^{d^4}) & \text{if } S = \{\infty\}. \end{cases}$$

Lemma 8.1.2. *Consider $d \geq 3$ and a finite set $S = \{\infty\} \cup S_f$ of primes. The compact subset $\Omega_{d,S}$ of $X^1_{d,S}$ has the following property: Let H_S be the orthogonal group of an isotropic, non-degenerate quadratic form on $\mathbb{Q}^d_S$. For any closed H_S-orbit Y in $X^1_{d,S}$ we have*

$$\mu_Y(Y \cap \Omega_{d,S}) \geq \frac{1}{2}\mu_Y(Y).$$

The last intermediate result—proved in Section 8.4—shows a recurrence of closed H_S-orbits in directions transversal to H_S. It is the counterpart of Lemma 8.1.1. For the case $S = \{\infty\}$, see [LM16, Lemma 15, p. 892].

Lemma 8.1.3. *Consider a finite set $S = \{\infty\} \cup S_f$ of primes and $d \geq 3$. Let H_S be the orthogonal group of a non-degenerate diagonal quadratic form on $\mathbb{Q}_S^d$. Suppose that H_S is non-compact. For any closed H_S-orbit Y in $X_{d,S}^1$ with $\mu_Y(Y) > A_d p_S^{4c_d}$, there is $u \in G_{d,S}^1 - H_S$ such that $u(Y \cap \Omega_{d,S})$ meets Y, $||u_p||_p \leq 1$ for any $p \in S_f$, and*

$$||u_\infty - I_d||_\infty \leq C_d^{(4)} p_S^4 \mu_Y(Y)^{-\frac{1}{c_d}}.$$

Let's deduce the main result of the chapter from the intermediate results.

Proof of Proposition 8.0.1. Let Q be a non-degenerate integral quadratic form in $d \geq 3$ variables. Suppose that Q_S is isotropic. Let P be the standard quadratic form on $\mathbb{Q}_S^d$ that is $\mathbb{Q}_S$-equivalent to Q_S and set $H_S = O(P, \mathbb{Q}_S)$. As we explained right before Lemma 8.1.2, the H_S-orbits $Y_{Q,S}$ and $Y := Y_{Q,S}^1$—respectively in $X_{d,S}$ and $X_{d,S}^1$—have the same volume

$$\mu_{Y_{Q,S}}(Y_{Q,S}) = \mu_Y(Y).$$

Let A_d be as in Lemma 8.1.3. We consider two cases:

- $\boxed{\mu_Y(Y) > A_d p_S^{4c_d}}$ By Lemma 8.1.3 there is g respectively in $\widetilde{\Omega}_{d,S}(\mathcal{E}_d p_S^{2d^4})$ and $\widetilde{\Omega}_{d,S}(\mathcal{E}_d 2^{d^4})$ if $S_f \neq \emptyset$ and $S = \{\infty\}$, as well as $u \in G_{d,S}^1 - H_S$ with $||u_p||_p \leq 1$ for $p \in S_f$ and

  $$||u_\infty - I_d||_\infty \leq C_d^{(4)} p_S^4 \mu_Y(Y)^{-\frac{1}{c_d}},$$

  such that $g x_{d,S}^1$ and $u g x_{d,S}^1$ are in Y. We also know that

  $$||u_\infty - I_d||_\infty \geq \frac{1}{2d^3} p_S^{-1} \mathscr{H}_S(g)^{-2} \mathscr{H}_S(\delta_Q)^{-\frac{1}{d}},$$

  by Lemma 8.1.1. Let's consider the case $S_f \neq \emptyset$. It follows that

  $$\begin{aligned} \mu_Y(Y) &< \left(\frac{2^4 d^2}{d-1} \mathscr{H}_S(g)^2 p_S^5 \mathcal{V}_d^{\frac{1}{c_d}} \mathscr{H}_S(\delta_Q)^{\frac{1}{d}} \right)^{c_d} \\ &< (2^5 d (\mathcal{E}_d p_S^{2d^4})^2 p_S^5)^{c_d} \mathcal{V}_d \mathscr{H}_S(\delta_Q)^{\frac{c_d}{d}} \\ &< \mathcal{F}_d \mathcal{V}_d p_S^{3d^6} \mathscr{H}_S(\delta_Q)^{\frac{d+1}{2}}, \end{aligned}$$

  where $\mathcal{F}_d = (2^{2d^3+5} \cdot 3^{4d^4} d^{6d^3+1})^{c_d}$. When $S = \{\infty\}$, a similar computation yields

  $$\mu_Y(Y) < \mathcal{F}_d \mathcal{V}_d 2^{2d^6} |\delta_Q|_\infty^{\frac{d+1}{2}}.$$

- $\boxed{\mu_Y(Y) \leq A_d p_S^{4c_d}}$ Since $\mathscr{H}_S(\delta_Q)$ is a positive integer, we have

  $$\mu_Y(Y) \leq A_d p_S^{4c_d} \leq A_d p_S^{4c_d} \mathscr{H}_S(\delta_Q)^{\frac{d+1}{2}}.$$

Since $A_d p_S^{4c_d}$ is smaller than $\mathcal{F}_d \mathcal{V}_d p_S^{3d^6}$ and $\mathcal{F}_d \mathcal{V}_d 2^{2d^6}$, in both cases we get the inequality of the statement. □

8.2 Transversal isolation of compact H_S-orbits

In this section we prove Lemma 8.1.1. The proof is short and elementary. It is based on the next four lemmas. For the definition of $M_S(Q)$ see (8.1).

Lemma 8.2.1. *Let Q be a non-degenerate integral quadratic form in $d \geq 2$ variables. Then*

$$1 \leq M_S(Q) \leq p_S \mathscr{H}_S(\delta_Q)^{\frac{1}{2}}$$

for any finite set $S = \{\infty\} \cup S_f$ of primes.

Proof. Let P be the standard quadratic form on $\mathbb{Q}_S^d$ that is $\mathbb{Q}_S$-equivalent to Q_S. We have

$$(\delta_P)_\infty = \pm 1 \quad \text{and} \quad p^{-2} \leq |(\delta_P)_p|_p \leq 1$$

for $p \in S_f$, thus

$$p_S^{-2} \leq \mathscr{H}_S(\delta_P) \leq 1.$$

Since $M_S(Q) = \left(\frac{\mathscr{H}_S(\delta_Q)}{\mathscr{H}_S(\delta_P)}\right)^{\frac{1}{2}}$ and $\mathscr{H}_S(\delta_Q)$ is a positive integer, the inequality we want follows. □

Lemma 8.2.2. *For any $g_\infty \in GL(d, \mathbb{R})$ we have*

$$||g_\infty||_\infty \geq \frac{|\det g_\infty|_\infty^{\frac{1}{d}}}{\sqrt{d}}.$$

Proof. Consider $f = |\det g_\infty|_\infty^{-\frac{1}{d}} g$. Notice that f is in $SL^{\pm}(d, \mathbb{R})$. Thanks to the Iwasawa decomposition of this group we can write $f = kan$, for some $k \in O(d, \mathbb{R})$,

$$a = diag(a_1, \ldots, a_d)$$

and n unipotent and upper-triangular. Since $|a_1 \cdots a_d|_\infty = 1$, then $||an||_\infty \geq 1$. Thus

$$\begin{aligned} 1 \leq ||an||_\infty = ||k^{-1} f||_\infty &= |\det g_\infty|_\infty^{-\frac{1}{d}} ||k^{-1} g_\infty||_\infty \\ &\leq \sqrt{d} \cdot |\det g_\infty|_\infty^{-\frac{1}{d}} ||g_\infty||_\infty, \end{aligned}$$

which is equivalent to what we wanted. □

Lemma 8.2.3. *For any $g_p \in GL(d, \mathbb{Q}_p)$ we have*

$$||g_p||_p \geq |\det g_p|_p^{\frac{1}{d}}.$$

Proof. We write $g = kan$ with $k \in GL(d, \mathbb{Z}_p)$,

$$a = diag(p^{n_1}, \ldots, p^{n_d}),$$

and n unipotent, upper-triangular. Then

$$||g_p||_p = ||an||_p \geq \max_i |p^{n_i}|_p.$$

The product of the positive real numbers $|p^{n_i}|_p |\det g_p|_p^{-\frac{1}{d}}$ for $1 \leq i \leq d$ is 1, so at least one is ≥ 1. Thus

$$||g_p||_p \geq |\det g_p|_p^{\frac{1}{d}}.$$

□

Lemma 8.2.4. *If t is a real number in the interval $[0, \frac{1}{2}]$, then*

$$\sqrt{t+1} - 1 \geq \frac{2}{5}t.$$

Proof. Since $F(t) = \sqrt{t+1} - 1$ is concave, it suffices to verify the inequality for $t \in \{0, 1/2\}$. When $t = \frac{1}{2}$,

$$2\left(\sqrt{\frac{3}{2}} - 1\right) = 0.44\ldots > \frac{2}{5}.$$

□

We are ready to prove the transversal isolation of the orbits $Y_{Q,S}$.

Proof of Lemma 8.1.1. Let Q be a non-degenerate integral quadratic form in $d \geq 3$ variables. The strategy we'll follow is: points in $Y^1_{Q_S}$ correspond to quadratic forms $\mathbb{Z}_S$-equivalent to Q. The ones associated to $gx^1_{d,S}$ and $ugx_{d,S}$ are different because $u \notin H_S$, so the S-height of the difference of their matrices is at least 1. From this we'll deduce the bound for u_∞.

First we recover the matrices with coefficients in $\mathbb{Z}_S$ corresponding to points in $Y^1_{Q,S}$. We'll recall briefly the definition of $Y^1_{Q,S}$. Let P be the standard quadratic form $\mathbb{Q}_S$-equivalent to Q_S, $H_S = O(P, \mathbb{Q}_S)$ and consider $f' \in G_{d,S}$ such that $Q = P \circ f'$. Let $f = N_S(Q)f'$, where $N_S(Q) \in \mathbb{Q}_S$ is defined as:

$$N_S(Q)_\infty = M_S(Q)^{-\frac{1}{3}},$$

and $N_S(Q)_p = 1$ for $p \in S_f$. See (8.1) for the definition of $M_S(Q)$. Then f is in $G^1_{d,S}$ and

$$Y^1_{Q,S} = H_S f x^1_{d,S}.$$

Let $b \in GL(d, \mathbb{Q}_S)$ be the matrix of P in the standard basis of $\mathbb{Q}^d_S$. If g' is in $H_S f' \Gamma_{d,S}$, then

$${}^t g' b g' = {}^t\gamma\, {}^t f' b f' \gamma = {}^t\gamma b_{Q_S} \gamma$$

for some $\gamma \in \Gamma_{d,S}$. It follows that the matrix ${}^t g' b g' \in M_d(\mathbb{Q}_S)$ is the diagonal image of a matrix in $M_d(\mathbb{Z}_S)$. This implies that if $g_1 x^1_{d,S}$ is in $Y^1_{Q,S}$—for $g_1 \in G^1_{d,S}$—then $N_S(Q)^{-2}\, {}^t g_1 b g_1 \in M_d(\mathbb{Q}_S)$ is the diagonal image of a matrix with coefficients in $\mathbb{Z}_S$.

Now we compare the matrices $B, C \in M_d(\mathbb{Q}_S)$ associated to the two points of the statement. We'll renormalize them to make the estimates in $M_d(\mathbb{R})$. Let $g, u \in G^1_{d,S}$ as in the statement. Then $gx^1_{d,S}$ and $ugx^1_{d,S}$ are in $Y_{Q,S}$. We consider

$$B = N_S(Q)^{-2}({}^t g b g), \quad C = N_S(Q)^{-2}({}^t g\, {}^t u b u g).$$

For any $p \in S_f$ we have

$$\begin{aligned} ||C_p||_p &= ||\, {}^t g_p\, {}^t u_p b_p u_p g_p||_p \\ &\leq ||\, {}^t g_p||_p ||\, {}^t u_p||_p ||P_p||_p ||u_p||_p ||g_p||_p \\ &\leq ||g_p||_p^2, \end{aligned}$$

and similarly $||B_p||_p \leq ||g_p||_p^2$. It follows that $\mathscr{H}_{S_f}(g)^2 B_\infty$ and $\mathscr{H}_{S_f}(g)^2 C_\infty$ have integral coefficients, where

$$\mathscr{H}_{S_f}(g) = \prod_{p \in S_f} ||g_p||_p.$$

These two matrices are different because ${}^t ubu \neq b$, hence the ∞-norm of their difference is at least 1:

$$\begin{aligned} 1 &\leq ||\mathscr{H}_{S_f}(g)^2 C_\infty - \mathscr{H}_{S_f}(g)^2 B_\infty||_\infty \\ &= \mathscr{H}_{S_f}(g)^2 M_S(Q)^{\frac{2}{d}} || {}^t g_\infty ({}^t u_\infty b_\infty u_\infty - b_\infty) g_\infty||_\infty. \end{aligned}$$

We rearrange this inequality and we work with the right-hand side:

$$\begin{aligned} \mathscr{H}_{S_f}(g)^{-2} M_S(Q)^{-\frac{2}{d}} &\leq || {}^t g_\infty ({}^t u_\infty b_\infty u_\infty - b_\infty) g_\infty||_\infty \\ &\leq d^2 || {}^t g_\infty||_\infty \cdot || {}^t u_\infty b_\infty u_\infty - b_\infty||_\infty \cdot ||g_\infty||_\infty \\ &= d^2 ||g_\infty||_\infty^2 \cdot || {}^t (u_\infty - I_d) b_\infty (u_\infty - I_d) + {}^t (u_\infty - I_d) b_\infty + b_\infty (u_\infty - I_d)||_\infty \\ &\leq d^2 ||g_\infty||_\infty^2 (d||u_\infty - I_d||_\infty \cdot ||b_\infty (u_\infty - I_d)||_\infty + 2||u_\infty - I_d||_\infty) \\ &\leq d^3 ||g_\infty||_\infty^2 (||u_\infty - I_d||_\infty^2 + ||u_\infty - I_d||_\infty). \end{aligned}$$

Hence

$$||u_\infty - I_d||_\infty^2 + ||u_\infty - I_d||_\infty \geq C_g,$$

where $C_g = d^{-3} \mathscr{H}_S(g)^{-2} M_S(Q)^{-\frac{2}{d}}$. We obtain that $||u_\infty - I_d||_\infty$ is greater or equal than the positive root of $t^2 + t - C_g$, that is

$$||u_\infty - I_d||_\infty \geq \frac{1}{2}(\sqrt{4C_g + 1} - 1).$$

Using (8.2.1) and lemmas 8.2.2, 8.2.3 we deduce that

$$\begin{aligned} 4C_g = 4 \cdot d^{-3} \mathscr{H}_S(g)^{-2} M_S(Q)^{-\frac{2}{d}} &\leq 4 \cdot d^{-3} (d \mathscr{H}_S(\det g)^{-\frac{2}{d}}) \\ &= 4 \cdot d^{-2} < \frac{1}{2}. \end{aligned}$$

We use now Lemma 8.2.4 and the lower bound of (8.2.1):

$$\begin{aligned} ||u_\infty - I_d||_\infty &\geq \frac{1}{5} \cdot 4C_g \\ &= \frac{4}{5d^3} \mathscr{H}_S(g)^{-2} M_S(Q)^{-\frac{2}{d}} \\ &\geq \frac{4}{5d^3} p_S^{-\frac{2}{d}} \mathscr{H}_S(g)^{-2} \mathscr{H}_S(\delta_Q)^{-\frac{1}{d}} \\ &\geq \frac{1}{2d^3} p_S^{-1} \mathscr{H}_S(g)^{-2} \mathscr{H}_S(\delta_Q)^{-\frac{1}{d}}, \end{aligned}$$

which is what we wanted. □

8.3 Uniform recurrence of closed H_S-orbits

The goal of this section is to prove the existence of the compact subset $\Omega_{d,S}$ of $X^1_{d,S}$ of Lemma 8.1.2 that intersects at least a half of any closed H_S-orbit in $X^1_{d,S}$. In other words, closed H_S-orbits are uniformly recurrent. This is a refinement of Dani-Margulis' Recurrence of Unipotent Flows, and in fact the heart of the proof is an effective version of it.

The section is divided into four parts: Suppose that Ω is a subset of $X^1_{d,S}$ and that the *systole* of any $\Delta \in \Omega$ is at least t, for some $t > 0$. In 8.3.1 we give—in terms of t—a compact subset of $GL(d, \mathbb{Q}_S)$ that covers Ω. We describe in 8.3.2 a compact subset $\mathfrak{O}_{d,S}$ of $X^1_{d,S}$ having the properties of $\Omega_{d,S}$, using the systole map $\alpha_1 : X^1_{d,S} \to \mathbb{R}$. To achieve this, we'll use an effective result of recurrence of unipotent flows on $X^1_{d,S}$, whose proof is postponed to 8.3.4. The main proof is given in 8.3.3.

8.3.1 Effective S-adic Mahler's Criterion

The classical version of Mahler's Criterion gives a necessary and sufficient condition for a subset of lattices of $\mathbb{R}^d$ of covolume 1 to be relatively compact in terms of the systole[3] map. We'll prove here an effective version for lattices of $\mathbb{Q}^d_S$. The statement is specially tailored for our needs: it gives an explicit lift to $GL(d, \mathbb{Q}_S)$ of a compact subset in $X^1_{d,S}$ described in terms of the systole map. We'll prove the result first for $S = \{\infty\}$ and then for general S.

Recall that any lattice of $\mathbb{R}^d$ is of the form $g\mathbb{Z}^d$ with $g \in GL(d, \mathbb{R})$. Thus we can identify respectively the space of lattices and lattices of covolume 1 of $\mathbb{R}^d$ with $X_{d,\infty} = GL(d, \mathbb{R})/GL(d, \mathbb{Z})$ and $X^1_{d,\infty} = SL^{\pm}(d, \mathbb{R})/GL(d, \mathbb{Z})$. We parametrize these spaces with the *Siegel sets* of $GL(d, \mathbb{R})$. Let's recall the definition.

Consider the following subgroups of $G_{d,\infty} = GL(d, \mathbb{R})$:

$$\begin{aligned} K &= O(d, \mathbb{R}) \\ A &= \{diag(a_1, \cdots, a_d) \in G_{d,\infty} \mid a_i > 0 \text{ for every } 1 \leq i \leq d\}, \\ N &= \{\text{unipotent, upper-triangular matrices in } G_{d,\infty}\}. \end{aligned}$$

For $\alpha, \beta > 0$ we denote

$$\begin{aligned} A_\alpha &= \{diag(a_1, \cdots, a_d) \in A \mid a_i \leq \alpha a_{i+1} \text{ for } 1 \leq i \leq d-1\}, \\ N_\beta &= \{n \in N \mid ||n - I_d||_\infty \leq \beta\}. \end{aligned}$$

The (α, β)-Siegel set of $G_{d,\infty}$ is defined as

$$\mathscr{S}^{\alpha,\beta}_{d,\infty} = KA_\alpha N_\beta.$$

The next lemma bounds the ∞-norm of $g \in \mathscr{S}^{\alpha,\beta}_{d,\infty} \cap SL^{\pm}(d, \mathbb{R})$ in terms of α, β and the length of a vector in $\Delta = g\mathbb{Z}^d$. It can be thought as an effective version Mahler's Criterion since

$$X_{d,\infty} = (\mathscr{S}^{\alpha,\beta}_{d,\infty} \cap SL^{\pm}(d, \mathbb{R}))x_{d,\infty}$$

for α and β big enough—see Proposition 9.3.1. We denote by $||\cdot||_{euc}$ the standard euclidean norm on $\mathbb{R}^d$.

[3] The systole of a lattice Δ of $\mathbb{R}^d$ is the length of the shortest non-zero vector in Δ.

Lemma 8.3.1. *Let $\mathscr{S}_{d,\infty}^{\alpha,\beta}$ be a Siegel set of $GL(d,\mathbb{R})$ with $\beta \leq 1 \leq \alpha$. Any $g \in \mathscr{S}_{d,\infty}^{\alpha,\beta} \cap SL^{\pm}(d,\mathbb{R})$ verifies*

$$||g||_\infty \leq \sqrt{d} \cdot \alpha^{\frac{(d-1)^2}{2}} \max\{1, ||ge_1||_{euc}^{-(d-1)}\}.$$

Proof. We write $g = kan$ with $k \in O(d,\mathbb{R}), a = diag(a_d, \dots, a_d) \in A_\alpha$, and $n \in N_\beta$. Notice that $||ge_1||_{euc} = a_1$, and

$$||an||_\infty = ||(a_1, \dots, a_d)||_\infty$$

because an is upper-triangular and

$$|(an)_{ij}|_\infty = |a_i n_{ij}|_\infty \leq \beta |a_i|_\infty \leq |a_i|_\infty$$

if $i < j$. We'll bound from above a_k in terms of a_1 and α. By the definition of A_α we have $a_i \leq \alpha^{j-i} a_j$ and $a_j^{-1} \leq \alpha^{j-i} a_i^{-1}$ if $i < j$. Then

$$\begin{aligned} 1 = [a_1 \cdots a_{k-1}] a_k [a_{k+1} \cdots a_d] &\geq [a_1(\alpha^{-1}a_1) \cdots (\alpha^{-(k-2)}a_1)] a_k [(\alpha^{-1}a_k) \cdots (\alpha^{-(d-k)}a_k)] \\ &= \alpha^{-\frac{(k-2)(k-1)}{2}} a_1^{k-1} \alpha^{-\frac{(d-k)(d-k+1)}{2}} a_k^{d-k+1}, \end{aligned}$$

hence

$$\begin{aligned} a_k &\leq \alpha^{\frac{(k-2)(k-1)}{2(d-k+1)}} \alpha^{\frac{d-k}{2}} a_1^{-\frac{k-1}{d-k+1}} \\ &\leq \alpha^{\frac{(d-2)(d-1)}{2}} \alpha^{\frac{d-1}{2}} \max\{1, a_1^{-(d-1)}\} \\ &= \alpha^{\frac{(d-1)^2}{2}} \max\{1, a_1^{-(d-1)}\}. \end{aligned}$$

This gives and upper bound for $||an||_\infty$. To finish we have

$$\begin{aligned} ||g||_\infty = ||kan||_\infty &\leq \sqrt{d} \cdot ||an||_\infty \\ &\leq \sqrt{d} \cdot \alpha^{\frac{(d-1)^2}{2}} \max\{1, a_1^{-(d-1)}\}. \end{aligned}$$

□

We pass to the S-adic case. Let $S = \{\infty\} \cup S_f$ be a finite set of primes. We define the height of $v \in \mathbb{Q}_S^d$ as

$$\mathscr{H}_S(v) = ||v_\infty||_{euc} \prod_{p \in S_f} ||v_p||_p.$$

Notice that in the real factor we are using the euclidean norm of $\mathbb{R}^d$ instead of $||\cdot||_\infty$. First we characterize the lattices—that is discrete and co-compact subgroups—of $\mathbb{Q}_S^d$ in an analogous way to the case $S = \{\infty\}$.

Lemma 8.3.2. *Consider a finite set $S = \{\infty\} \cup S_f$ of primes and let $d \geq 1$. Any lattice of $\mathbb{Q}_S^d$ is of the form $g\mathbb{Z}_S^d$ with $g \in GL(d, \mathbb{Q}_S)$.*

Proof. Consider a lattice Δ of $\mathbb{Q}_S^d$. We start with two general observations. We'll take $\mathbb{Z}_S$ embedded diagonally in $\mathbb{Q}_S^d$.

First we'll see that Δ is indeed a $\mathbb{Z}_S$-module. Take $p \in S_f$. Then $p\Delta$ is also a lattice of $\mathbb{Q}_S^d$. We have $p\Delta \subseteq \Delta$, so

$$[\Delta : p\Delta]\text{cov } \Delta = \text{cov } (p\Delta). \tag{8.2}$$

Since $\mathscr{H}_S(p) = 1$, the multiplication by p is a volume-preserving linear automorphism of $\mathbb{Q}_S^d$, hence Δ and $p\Delta$ have the same covolume. Thus $\Delta = p\Delta$ by (8.2). More generally, $\Delta = u\Delta$ for any $u \in \mathbb{Z}_S^\times$ since $\mathbb{Z}_S^\times$ is generated by $S_f \cup \{-1\}$. This shows that Δ is a $\mathbb{Z}_S$-module.

Now we'll show that if $v \in \Delta$ has a zero coordinate, then $v = 0$. Recall that p_S is the product of the primes in S_f if this set is non-empty and $p_S = 1$ for $S = \{\infty\}$. If $v_\infty = 0$, then $p_S^n v \to 0$ as $n \to \infty$. Since $p_S^n v \in \Delta$ and Δ is discrete, $p_S^n v = 0$ for $n \gg 1$, so $v = 0$. Suppose now that $v_{p_0} = 0$ for some $p_0 \in S_f$ and let $T = S - \{p_0\}$. Choose $k_0 > 1$ such that $p_0^{k_0} > p_T$ Then

$$\lim_{n\to\infty} \left(\frac{p_T}{p_0^{k_0}}\right)^n v = 0.$$

These vectors are in Δ, so we conclude as before that $v = 0$.

Now we prove the result by induction on d.

Take first $d = 1$. Let

$$\alpha_1(\Delta) = \inf\{\mathscr{H}_S(v) \mid v \in \Delta - \{0\}\}.$$

We claim that $\alpha_1(\Delta)$ is attained by some $v_0 \in \Delta - \{0\}$. Consider a sequence $v_n \in \Delta - \{0\}$ with $\mathscr{H}_S(v_n) \to \alpha_1(\Delta)$. We may suppose that $(v_n)_p$ is in $\mathbb{Z}_p^\times$ for every n and any $p \in S_f$[4]. Then (v_n) is trapped in a compact of the form $C_N = [-N, N] \times \prod_{p\in S_f} \mathbb{Z}_p^\times$. The set $\Delta \cap C_N$ is finite, hence some vector in it attains $\alpha_1(\Delta)$. Let's see that $\Delta = \mathbb{Z}_S v_0$. Since v_0 is invertible in $\mathbb{Q}_S$, any $v \in \Delta$ is of the form $v_0 t$ with $t \in \mathbb{Q}_S$. Let $F_S = [0, 1) \times \prod_{p\in S_f} \mathbb{Z}_p$. Note that $\mathbb{Q}_S = \mathbb{Z}_S + F_S$. Write $t = z + f$ with $z \in \mathbb{Z}_S$ and $f \in F_S$. Then $v_0 f = v - v_0 z$ is in Δ. We have $\mathscr{H}_S(v_0 f) < \mathscr{H}(v_0)$, so $v_0 f = 0$.

Suppose that the result holds for some $d \geq 1$ and consider a lattice Δ in $\mathbb{Q}_S^{d+1}$. Take $v_0 \in \Delta - \{0\}$ such that $\mathscr{H}_S(v_0) \leq \mathscr{H}_S(v)$ for any $v \in (\mathbb{Q}_S v_0) \cap (\Delta - \{0\})$. The case $d = 1$ shows that $\Delta \cap (\mathbb{Q}_S v_0) = \mathbb{Z}_S v_0$, so $\Delta \cap (\mathbb{Q}_S v_0)$ is cocompact in $\mathbb{Q}_S v_0$. This implies that $\Delta' = \Delta + \mathbb{Q}_S v_0$ is discrete in $V = \mathbb{Q}_S^{d+1}/\mathbb{Q}_S v_0 \cong \mathbb{Q}_S^d$. Since Δ is cocompact in $\mathbb{Q}_S^{d+1}$, Δ' is cocompact in V. Thus Δ' is a lattice in V. By the inductive hypothesis, Δ' has a $\mathbb{Z}_S$-basis $v_1 + \mathbb{Q}_S v_0, \ldots, v_d + \mathbb{Q}_S v_0$ that is also a $\mathbb{Q}_S$-basis of V, with $v_1, \ldots, v_d \in \Delta$. The matrix g with columns $v_0, \ldots v_d$ is in $GL(d + 1, \mathbb{Q}_S)$ and $\Delta = g\mathbb{Z}_S^d$. □

As usual, we endow $\mathbb{R}$ and $\mathbb{Q}_p$ with the Haar measures such that

$$\lambda_{\mathbb{R}}([0, 1]) = \lambda_{\mathbb{Q}_p}(\mathbb{Z}_p) = 1,$$

and $\mathbb{Q}_S$ with $\lambda_{\mathbb{Q}_S} = \otimes_{\nu\in S}\lambda_{\mathbb{Q}_\nu}$. Let Δ be a lattice of $\mathbb{Q}_S^d$. We define its systole as

$$\alpha_1(\Delta) = \min_{v\in\Delta-\{0\}} \mathscr{H}_S(v),$$

and its covolume covΔ as the volume of $\mathbb{Q}_S^d/\Delta$. If we write Δ as $g\mathbb{Z}_S^d$ for some $g \in GL(d, \mathbb{Q}_S)$, it's easy to see that

$$\text{cov } g\mathbb{Z}_S^d = \mathscr{H}_S(\det g).$$

[4]Just note that $\mathscr{H}_S(uv_n) = \mathscr{H}_S(v_n)$ for any $u \in \mathbb{Z}_S^\times$ and remember that $(v_n)_p \neq 0$ since $v \neq 0$.

Thanks to Lemma 8.3.2 we identify, respectively, the space of lattices and lattices of covolume 1 of $\mathbb{Q}_S^d$ with $X_{d,S} = G_{d,S}/\Gamma_{d,S}$ and $X^1_{d,S} = G^1_{d,S}/\Gamma_{d,S}$. Again, these spaces are parametrized by the Siegel sets of $G_{d,S}$: for any $\alpha, \beta > 0$ we define

$$\mathscr{S}^{\alpha,\beta}_{d,S} = \mathscr{S}^{\alpha,\beta}_{d,\infty} \times \prod_{p \in S_f} GL(d, \mathbb{Z}_p).$$

Here is an effective S-adic Mahler's Criterion.

Lemma 8.3.3. *Consider a finite set of primes $S = \{\infty\} \cup S_f$ and an integer $d \geq 2$. If Δ is a lattice of $\mathbb{Q}_S^d$ of covolume 1, then $\Delta = g\mathbb{Z}_S^d$ for some $g \in G_{d,S}$ with $g_p \in GL(d, \mathbb{Z}_p)$ for $p \in S_f$ and*

$$||g_\infty||_\infty \leq \sqrt{d} \cdot \left(\frac{2}{\sqrt{3}}\right)^{\frac{(d-1)^2}{2}} \max\{1, \alpha_1(\Delta)^{-(d-1)}\}. \tag{8.3}$$

Proof. Thanks to Proposition 9.3.1, $\Delta = g\mathbb{Z}_S^d$ for some $g \in \mathscr{S}^{\frac{2}{\sqrt{3}},\frac{1}{2}}_{d,S}$. Further, we choose g with

$$\mathscr{H}_S(ge_1) = \alpha_1(\Delta).$$

Since g_p is in $GL(d, \mathbb{Z}_p)$, then $|\det g_p|_p = 1$ and $||ge_1||_p = 1$ for any $p \in S_f$. Thus g_∞ is in $SL^{\pm}(d, \mathbb{R})$ because

$$1 = cov(\Delta) = \mathscr{H}_S(\det g) = |\det g_\infty|_\infty,$$

and

$$\alpha_1(\Delta) = \mathscr{H}_S(ge_1) = ||g_\infty e_1||_{euc}.$$

We obtain inequality (8.3) by applying Lemma 8.3.1 to g_∞. □

To close this part we state a non-effective S-adic Mahler's Criterion. It follows directly form Lemma 8.3.3.

Corollary 8.3.4 (Mahler's Criterion)**.** *A subset Ω of $X^1_{d,S}$ is relatively compact if and only if*

$$\inf\{\alpha_1(\Delta) \mid \Delta \in \Omega\} > 0.$$

8.3.2 The compact in terms of α_1

Here we give a compact subset $\mathfrak{O}_{d,S}$ of $X^1_{d,S}$ with the property we want for $\Omega_{d,S}$, but defined in terms of α_1. We begin with some notation. The set

$$\mathfrak{S}_{d,S}(\varepsilon) = \{\Delta \in X^1_{d,S} \mid \alpha_1(\Delta) \geq \varepsilon\}$$

is compact for any $\varepsilon > 0$ by Mahler's Criterion (Lemma 8.3.4). Let $d \geq 3$. We define

$$\varepsilon_{\infty,d} = \frac{1}{2} \cdot \left(\frac{1}{2 \cdot 3^{2d} d^3 2^{d+2}}\right)^{(d-1)^2} \quad \text{and} \quad \varepsilon_{p,d} = \frac{1}{2} \cdot \left(\frac{1}{2 \cdot 3^{2d} d^3 p^{2d+1}}\right)^{(d-1)^2}.$$

For $S = \{\infty\} \cup S_f$ a finite set of primes we define

$$\varepsilon_{d,S} = \min_{\nu \in S} \varepsilon_{\nu,d} \quad \text{and} \quad \mathfrak{O}_{d,S} = \mathfrak{S}_{d,S}(\varepsilon_{d,S}).$$

This is the compact subset that meets all the closed H_S-obits in $X^1_{d,S}$.

Lemma 8.3.5. *Consider $d \geq 3$ and a finite set of primes $S = \{\infty\} \cup S_f$. Let H_S be the orthogonal group of a non-degenerate isotropic quadratic form on $\mathbb{Q}_S^d$. For any closed H_S-orbit Y in $X_{d,S}^1$ we have*

$$\mu_Y(Y \cap \mathfrak{D}_{d,S}) \geq \frac{1}{2}\mu_Y(Y).$$

Suppose that H_S is the orthogonal group of a non-degenerate quadratic form P on $\mathbb{Q}_S^d$, and that H_{p_0} is non-compact. To prove Lemma 8.3.5 we will approximate $\mu_Y(Y \cap \mathfrak{D}_{d,S})$ by averages of $\mathbb{1}_{\mathfrak{D}_{d,S}}$ along pieces of U_{p_0}-orbits, where U_{p_0} is a one-parameter unipotent subgroup of H_{p_0}. After justifying why this is possible, we'll introduce the main ingredient of the proof of Lemma 8.3.5: the effective refinements of Dani-Margulis' Recurrence of Unipotent Flows—see [Mar75] and [Dan86]. These are due to Kleinbock-Margulis [KM98] for $S = \{\infty\}$ and to Kleinbock-Tomanov [KT07] for general S.

Recall that H_S° denotes the image of $\mathrm{Spin}(P, \mathbb{Q}_S)$ in H_S. H_S° is a normal subgroup of H_S of finite index, thus a closed H_S-orbit in $X_{d,S}^1$ is a finite union of closed H_S°-orbits. There is no harm then if we work with the latter. Consider a closed H_S°-orbit Y of $X_{d,S}^1$, its H_S°-invariant measure μ_Y and a mesurable subset Ω of $X_{d,S}^1$. The next two results justify that $\mu_Y(Y \cap \Omega)$ can be approximated by averaging $\mathbb{1}_\Omega$ along pieces of suitable orbits of a one-parameter unipotent subgroup of H_{p_0}. The first is a version of Birkhoff's Theorem for every $\mathbb{Q}_\nu$. It follows from [Tem92, Chapter 6, Corollary 3.2]. For $T \geq 0$ we define

$$B_\nu(T) = \{t \in \mathbb{Q}_\nu \mid |t|_\nu \leq T\}.$$

Theorem 8.3.6. *Consider a prime ν. Let Φ be a measure-preserving, ergodic action of $\mathbb{Q}_\nu$ on a locally compact space Y_0 endowed with a finite measure μ_0. For any measurable subset Ω of Y_0, there is a measurable subset E_Ω of Y_0 of full measure such that*

$$\frac{\mu_0(\Omega)}{\mu_0(Y_0)} = \lim_{T \to \infty} \frac{\lambda_{\mathbb{Q}_\nu}(\{t \in B_\nu(T) \mid \Phi_t(y) \in \Omega\})}{\lambda_{\mathbb{Q}_\nu}(B_\nu(T))}$$

for any $y \in E_\Omega$.

Recall that we chose $p_0 \in S_f$ such that H_{p_0} is non-compact. Moore's ergodicity result will allow us to apply Birkhoff's Theorem:

Lemma 8.3.7. *Consider a finite set of primes $S = \{\infty\} \cup S_f$ and $d \geq 3$. Let H_S be the orthogonal group of a non-degenerate quadratic form on $\mathbb{Q}_S^d$, and suppose that H_{ν_0} is non-compact for some $\nu_0 \in S$. Let U_{ν_0} be a one-parameter unipotent subgroup of H_{ν_0} with non-trivial projection to each simple factor of H_{ν_0}[5]. The action of U_{ν_0} on any closed H_S°-orbit in $X_{d,S}^1$ is ergodic.*

Our proof of Lemma 8.3.7 relies on the next useful result, which we'll call the *Howe-Moore phenomenon*[6].

[5] In fact H_{ν_0} is always simple, except possibly when $d = 4$. In that case H_{ν_0} can be locally isomorphic to $SL(2, \mathbb{Q}_{\nu_0}) \times SL(2, \mathbb{Q}_{\nu_0})$.

[6] Another (perhaps more widely used) name for this is *Mautner's phenomenon*, like in the article [Moo80] of C. Moore.

Lemma 8.3.8. *Consider the group of $\mathbb{Q}_\nu$-points J of a semisimple $\mathbb{Q}_\nu$-group. Let π be a unitary representation of J and let J° be the subgroup of J generated by the unipotent elements. If $v \in \mathcal{H}_\pi$ is fixed by a unipotent element with non-trivial projection to each simple factor of J, then v is J°-invariant.*

Proof. The case $J = SL(2,\mathbb{R})$ is done in [Ben09, Proposition 3.4], and the proof extends to $SL(2,\mathbb{Q}_\nu)$. Now consider a general J.

We prove first that a vector $v \in \mathcal{H}_\pi$ is J°-invariant if it is fixed by a hyperbolic element[7] $h \in J$ with non-trivial projection to each simple factor of J. We take an h-invariant vector v of unit length. Consider the subgroup

$$U_h^+ = \left\{ g \in J \mid \lim_{n\to\infty} h^n g h^{-n} = e \right\}.$$

Since $\pi(h)v = v$, then

$$\langle \pi(g)v, v\rangle = \langle \pi(h^n g h^{-n})v, v\rangle$$

for any $n \in \mathbb{Z}$. If g is in U_h^+, we obtain that $\langle \pi(g)v, v\rangle = 1$ by letting $n \to \infty$, so v is fixed by g. This proves that v is U_h^+-invariant. In a similar way we see that v is U_h^--invariant, where

$$U_h^- = \left\{ g \in J \mid \lim_{n\to\infty} h^{-n} g h^{n} = e \right\}.$$

The groups $U_h^\pm$ have non-trivial projection to each simple factor of J since h has this property. Then J° is generated by U_h^+ and U_h^-—see [Mar91, Proposition 1.5.4 (ii)]—, so v is J°-invariant.

Suppose now that v is fixed by a non-trivial unipotent element u of J. By Jacobson-Morozov's Theorem u is in the image of a group morphism $\psi : SL(2,\mathbb{Q}_\nu) \to J$ with finite kernel. The vector v is then $SL(2,\mathbb{Q}_\nu)$-invariant because it is fixed by a non-trivial unipotent element of $SL(2,\mathbb{Q}_\nu)$. The image of ψ has non-trivial projection to each simple factor of J because it's generated by conjugates of u, which have this property. Since $\psi(SL(2,\mathbb{Q}_\nu))$ has non-trivial hyperbolic elements, v is J°-invariant thanks to the previous paragraph. □

We are ready to prove that unipotent groups act ergodically on closed H_S°-orbits.

Proof of Lemma 8.3.7. Let $Y = H_S^\circ g x_{d,S}^1$ be a closed H_S°-orbit in $X_{d,S}^1$. Since H_S is non-compact, then $g^{-1}H_S g = O(Q_S, \mathbb{Q}_S)$ for some non-degenerate integral quadratic form in d variables by Lemma 6.1.2. Let $J_S = g^{-1}H_S g$, $Y' = J_S x_{d,S}^1$ and $U'_{\nu_0} = g^{-1}U_{\nu_0}g$. We'll prove that $U'_{\nu_0} \curvearrowright Y'$ is ergodic.

Let π be the unitary representation of J_S° on $L^2(Y')$. Suppose that $\varphi \in L^2(Y')$ is U'_{ν_0}-invariant. Then φ is $J_{\nu_0}^\circ$-invariant by Lemma 8.3.8 because U_{ν_0} has non-trivial projection in each simple factor of H_{ν_0}. To see that φ is J_S°-invariant, consider the function $\Phi : J_S^\circ \to \mathbb{C}, h \mapsto \varphi(h x_{d,S}^1)$. Φ is $(J_S^\circ \cap \Gamma_{d,S})$-invariant on the right and $J_{p_0}^\circ$-invariant on the left. Since $J_{p_0}^\circ$ is normal in J_S°, then Φ is also $J_{p_0}^\circ$-invariant on the right. By the Strong Approximation Theorem—see [PR94, Theorem 7.12]—$J_{p_0}^\circ(J_S^\circ \cap \Gamma_{d,S})$ is dense in J_S°, so Φ is J_S°-invariant on the right. This proves that φ is $\mu_{Y'}$-almost surely constant, thus the action of U'_{p_0} on Y' is ergodic. □

[7] $h \in J$ is hyperbolic if $Ad(h) : Lie(J) \to Lie(J)$ is diagonalizable over $\mathbb{Q}_\nu$.

Before giving the statement of effective recurrence of unipotent flows, we extend the definition of covolume of a lattice of $\mathbb{Q}_S^d$ to discrete $\mathbb{Z}_S$-submodules of $\mathbb{Q}_S^d$ whose rank is not necessarily d, and we prove a finiteness lemma for these. Let Δ' be a discrete $\mathbb{Z}_S$-submodule of $\mathbb{Q}_S^d$. The covolume cov Δ', of Δ' is the volume of V/Δ', where V[8] is the $\mathbb{Q}_S$-module generated by Δ'. We give an explicit formula to calculate cov (Δ') that we'll use later. Let $e_1, \dots, e_d$ be the standard basis of $\mathbb{Q}^d$ and let $I = (i_1, \dots, i_k)$ be a k-tuple of integers $1 \leq i_1 < \cdots < i_k \leq d$. We denote $e_{i_1} \wedge \cdots \wedge e_{i_k}$ simply by e_I. On $\bigwedge^k \mathbb{R}^d$ we consider the only euclidean norm $||\cdot||_{euc}$ such that $(e_I)_I$ is an orthonormal basis, and on $\bigwedge^k \mathbb{Q}_p^d$ we consider the ultrametric norm given by

$$\left|\left|\sum_I a_I e_I\right|\right|_p = \max_I |a_I|_p.$$

Let $v_1, \dots, v_k \in \mathbb{Q}_S^d$ be a $\mathbb{Z}_S$-basis of Δ'. Then

$$\text{cov } \Delta' = ||(v_1 \wedge \cdots \wedge v_k)_\infty||_{euc} \prod_{p \in S_f} ||(v_1 \wedge \cdots \wedge v_k)_p||_p. \tag{8.4}$$

For $\Delta \in X_{d,S}$, we denote by $\Sigma(\Delta)$ the set of non-zero $\mathbb{Z}_S$-submodules of Δ and

$$\Sigma_{<1}(\Delta) = \{\Delta' \in \Sigma(\Delta) \mid \text{cov } \Delta' < 1\}.$$

Lemma 8.3.9. *Let $S = \{\infty\} \cup S_f$ be a finite set of primes and let Δ be a lattice of $\mathbb{Q}_S^d$. Then $\Sigma_{<1}(\Delta)$ is finite.*

Proof. For any $\Delta' \in \Sigma(\Delta)$, let $W_{\Delta'}$ be the $\mathbb{Q}_S$-submodule of $\mathbb{Q}_S^d$ generated by Δ' and consider

$$\mathscr{W} = \{W_{\Delta'} \mid \Delta' \in \Sigma_{<1}(\Delta)\}.$$

For $W \in \mathscr{W}$, let $\Delta'_W = \Delta \cap W$. We'll show that the map $\Sigma_{<1}(\Delta) \to \mathscr{W}, \Delta' \mapsto W_{\Delta'}$ is finite to one and that $\mathscr{W}$ is finite.

Take $W \in \mathscr{W}$ and $\Delta' \in \Sigma_{<1}(\Delta)$ such that $W_{\Delta'} = W$. Then Δ' is contained in Δ'_W, so

$$[\Delta'_W : \Delta'] = \frac{\text{cov } \Delta'}{\text{cov } \Delta'_W} < \frac{1}{\text{cov } \Delta'_W}.$$

To conclude note that Δ'_W has finitely many subgroups Λ of index, say $N > 0$. Indeed, any such Λ contains $N\Delta'_W$, and $\Delta'_W/(N\Delta'_W)$ is finite[9].

Let's prove that $\mathscr{W}$ is finite. It suffices to see that the subset $\mathscr{W}_k$ of elements of $\mathscr{W}$ of $\mathbb{Q}_S$-rank k is finite for $1 \leq k \leq d-1$. If $W \in \mathscr{W}_k$, let $v_1, \dots, v_k$ be a $\mathbb{Z}_S$-basis of Δ'_W. Then $v_1 \wedge \cdots \wedge v_k$ belongs to $\bigwedge^k \Delta$ and its S-height is cov $\Delta'_W < 1$. Since Δ is a lattice in $\mathbb{Q}_S^d$, $\bigwedge^k \Delta$ is a lattice in $\bigwedge^k \mathbb{Q}_S^d$. Moreover, $\mathbb{Z}_S^\times(v_1 \wedge \cdots \wedge v_k)$ doesn't depend on the chosen $\mathbb{Z}_S$-basis of Δ'_W and the map $\mathscr{W}_k \to \mathbb{Z}_S^\times \backslash \bigwedge^k \Delta$ is injective. To conclude note that there are finitely many $\mathbb{Z}_S^\times v \in \mathbb{Z}_S^\times \backslash \bigwedge^k \Delta$ with $\mathscr{H}_S(v) < 1$[10].

□

[8] We choose a Haar measure on V as follows: on V_∞ we take $\lambda_{V_\infty} = k_* \lambda_{\mathbb{R}^k}$, where $k \in O(d, \mathbb{R})$ sends $\mathbb{R}^k \times \{0\}$ to V_∞, and on V_p we choose λ_{V_p} so that $\lambda_{V_p}(V_p \cap \mathbb{Z}_p^d) = 1$.

[9] Because $\mathbb{Z}_S/N\mathbb{Z}_S$ is finite.

[10] This is a fact valid for any lattice Λ in $\mathbb{Q}_S^m$. Take $v \in \Lambda - \{0\}$ with $\mathscr{H}_S(v) < 1$. We'll see that $\mathbb{Z}_S^\times v$ has a representative in the finite set $A = \Lambda \cap ([-1,1] \times \prod_{p \in S_f} \mathbb{Z}_p)$. We showed in the proof of Lemma 8.3.2 that $v_\nu \neq 0$ for $\nu \in S$, so $||v||_{S_f} = \prod_{p \in S_f} ||v_p||_p$ is a unit in $\mathbb{Z}_S \hookrightarrow \mathbb{Q}_S$. We set $v' = ||v||_{S_f} v$. Note that $||v'_p||_p = 1$ for $p \in S_f$ and $||v'_\infty||_\infty = \mathscr{H}_S(v) < 1$, hence v' is in A.

If ν is a prime and $d \geq 2$, we define

$$C_{\nu,d} = \begin{cases} 3^{2d} d^3 2^{d+2} & \text{if } \nu = \infty, \\ 3^{2d} d^3 p^{2d+1} & \text{if } \nu = p, \end{cases}$$

and $\vartheta_d = \frac{1}{(d-1)^2}$. Here is the statement of recurrence of unipotent flows.

Proposition 8.3.10. *Let $S = \{\infty\} \cup S_f$ be a finite set of primes, $\nu \in S$ and $d \geq 2$. Consider a one-parameter unipotent subgroup $U_\nu = (u_t)_t$ of $SL(d, \mathbb{Q}_\nu)$ and a covolume 1 lattice Δ of $\mathbb{Q}_S^d$. Suppose that U_ν doesn't preserve the $\mathbb{Q}_S$-submodule generated by any $\Lambda \in \Sigma_{<1}(\Delta)$. There is $T_0 = T_0(U_\nu, \Delta)$ such that for any $T \geq T_0$ and $0 < \varepsilon < 1$,*

$$\lambda_{\mathbb{Q}_\nu}(\{t \in B_\nu(T) \mid \alpha_1(u_t \Delta) < \varepsilon\}) \leq C_{\nu,d} \varepsilon^{\vartheta_d} \lambda_{\mathbb{Q}_\nu}(B_\nu(T)).$$

Proposition 8.3.10 follows from results in the article [KT07] of Kleinbock and Tomanov. To state the latter we need several new definitions, so we postpone the proof of Proposition 8.3.10 to Subsection 8.3.4 to avoid a big detour here.

The last result we need to prove Lemma 8.3.5 says that for a fixed Δ, the hypothesis of Proposition 8.3.10 is verified by almost any conjugate of U_ν.

Lemma 8.3.11. *Consider a prime ν and $d \geq 3$. Let H_ν be the orthogonal group of a non-degenerate isotropic quadratic form on $\mathbb{Q}_\nu^d$ and let U_ν be a one-parameter unipotent subgroup of H_ν with non-trivial projection to each simple factor of H_ν. For any proper linear subspace V of $\mathbb{Q}_\nu^d$, the subset*

$$\{h \in H_\nu \mid h^{-1} U_\nu h \text{ preserves } V\}$$

of H_ν has measure 0.

Proof. We denote $\mathscr{C}(V)$ the set in the statement. Since $\mathscr{C}(V)$ is Zariski-closed, it has measure 0 or it contains a Zariski-connected component of H_ν. We'll show that the latter case implies $V = 0$ or $V = \mathbb{Q}_\nu^d$. Let H' be the Zariski-connected component of the identity of H_ν. If $\mathscr{C}(V)$ contains $h_0 H'$, then V is stable under the groups

$$(h')^{-1} (h_0^{-1} U_\nu h_0) h'$$

with $h' \in H'$. Let Z be an infinitesimal generator of $h_0^{-1} U_\nu h_0$. V is invariant under $Ad\, h'(Z)$ for $h' \in H'$. Note that the lie algebra $\mathfrak{h}_\nu$ of H_ν is generated by the $Ad\, h'(Z)$'s for $h' \in H'$ since Z has non-trivial projection to each simple factor of $\mathfrak{h}_\nu$. Thus V is $\mathfrak{h}_\nu$-invariant. Then $V = 0$ or $V = \mathbb{Q}_\nu^d$ because the natural action of $\mathfrak{h}_\nu$ on $\mathbb{Q}_\nu^d$ is irreducible. □

We are ready to prove that $\mathfrak{O}_{d,S}$ meets at least half of any closed H_S-orbit.

Proof of Lemma 8.3.5. Since H_S is non-compact, we take $\nu_0 \in S$ with H_{ν_0} non-compact. Let $C = C_{\nu_0,d}$ and $\vartheta = \vartheta_d$ be as in Proposition 8.3.10. Recall that

$$\mathfrak{O}_{d,S} = \{\Delta \in X_{d,S}^1 \mid \alpha_1(\Delta) \geq \varepsilon_{d,S}\},$$

and

$$\varepsilon_{d,S} \leq \varepsilon_{\nu_0,d} = \frac{1}{2} \cdot \left(\frac{1}{2C}\right)^{\vartheta^{-1}}.$$

Let $\varepsilon_1 = 2\varepsilon_{\nu_0,d}$. Then $0 < \varepsilon_{d,S} < \varepsilon_1 < 1$ and $C\varepsilon_1^{\vartheta} = \frac{1}{2}$.

Let's see that $\mathfrak{O}_{d,S}$ does the job. Once more, a closed H_S-orbit in $X^1_{d,S}$ breaks into finitely many closed H_S°-orbits, so we work with the latter. Let Y be such a closed H_S°-orbit and take $\Delta \in Y$. Let U_{ν_0} be a one-parameter unipotent subgroup of H_{ν_0} whose conjugates generate $H^\circ_{\nu_0}$. The action of U_{ν_0} on Y is ergodic by Lemma 8.3.7. By Birkhoff's Theorem 8.3.6 there is a co-null subset E of H_S° such that for any $h \in E$,

$$\begin{aligned}\frac{\mu_Y(\mathfrak{O}_{d,S} \cap Y)}{\mu_Y(Y)} &= \lim_{T\to\infty} \frac{\lambda_{\mathbb{Q}_{\nu_0}}(\{t \in B_{\nu_0}(T) \mid u_t h\Delta \in \mathfrak{O}_{d,S}\})}{\lambda_{\mathbb{Q}_{\nu_0}}(B_{\nu_0}(T))} \\ &= \lim_{T\to\infty} \frac{\lambda_{\mathbb{Q}_{\nu_0}}(\{t \in B_{\nu_0}(T) \mid h^{-1}u_t h\Delta \in h^{-1}\mathfrak{O}_{d,S}\})}{\lambda_{\mathbb{Q}_{\nu_0}}(B_{\nu_0}(T))}.\end{aligned}$$

Notice that

$$\mathfrak{S}_{d,S}(\varepsilon_1) = \{\Lambda \in X^1_{d,S} \mid \alpha_1(\Lambda) \geq \varepsilon_1)\}$$

is contained in the interior of $\mathfrak{O}_{d,S}$ because $\varepsilon_{d,S} < \varepsilon_1$. We choose $h_0 \in E$ close enough to I_d so that $\mathfrak{S}_{d,S}(\varepsilon_1)$ is still contained in $h_0^{-1}\mathfrak{O}_{d,S}$. Moreover, we ask that $h_0^{-1}U_{\nu_0}h_0$ does not preserve the $\mathbb{Q}_S$-module generated any $\Delta' \in \Sigma_{<1}(\Delta)$. This is possible since, by Lemma 8.3.11, the $h \in H_{\nu_0}$ such that $h^{-1}U_{\nu_0}h$ preserve $\langle\Delta'\rangle_{\mathbb{Q}_S}$ form a null subset of H_{ν_0}, and $\Sigma_{<1}(\Delta)$ is finite by Lemma 8.3.9. Thus

$$\frac{\lambda_{\mathbb{Q}_{\nu_0}}(\{t \in B_{\nu_0}(T) \mid h_0^{-1}u_t h_0\Delta \in h_0^{-1}\mathfrak{O}_{d,S}\})}{\lambda_{\mathbb{Q}_{\nu_0}}(B_{\nu_0}(T))} \geq \frac{\lambda_{\mathbb{Q}_{\nu_0}}(\{t \in B_{\nu_0}(T) \mid h_0^{-1}u_t h_0\Delta \in \mathfrak{S}_{d,S}(\varepsilon_1)\})}{\lambda_{\mathbb{Q}_{\nu_0}}(B_{\nu_0}(T))}.$$

By Proposition 8.3.10, for $T \gg 1$ we have

$$\frac{\lambda_{\mathbb{Q}_{\nu_0}}(\{t \in B_{\nu_0}(T) \mid h_0^{-1}u_t h_0\Delta \in \mathfrak{S}_{d,S}(\varepsilon_1)\})}{\lambda_{\mathbb{Q}_{\nu_0}}(B_{\nu_0}(T))} \geq 1 - C\varepsilon_1^{\vartheta} = \frac{1}{2},$$

so $\mu_Y(\mathfrak{O}_{d,S} \cap Y) \geq \frac{1}{2}\mu_Y(Y)$.

□

8.3.3 The main proof

Now we combine the results of 8.3.1 and 8.3.2 to show that $\Omega_{d,S}$ meets at least half of any closed H_S-orbit.

Proof of Lemma 8.3.5. Recall that $\Omega_{d,S} = \Omega_{d,S}(\mathcal{E}_d p_S^{2d^4})$ if $S_f \neq \emptyset$ and $\Omega_{\infty,d} = \Omega_{\infty,d}(\mathcal{E}_d 2^{d^4})$, where $\mathcal{E}_d = 2^{d^3} \cdot 3^{2d^4} d^{3d^3}$. Take $\Delta \in \mathfrak{O}_{d,S}$. By Lemma 8.3.3 we can write Δ as $g\mathbb{Z}_S^d$ for some

$$g \in SL^{\pm}(d,\mathbb{R}) \times \prod_{p\in S_f} GL(d,\mathbb{Z}_p)$$

with

$$||g_\infty||_\infty < \sqrt{d}\left(\frac{2}{\sqrt{3}}\right)^{\frac{(d-1)^2}{2}} \varepsilon_{d,S}^{-(d-1)} \leq \begin{cases} \mathcal{E}_d p_S^{2d^4} & \text{if } S_f \neq \emptyset, \\ \mathcal{E}_d 2^{d^4} & \text{if } S = \{\infty\}. \end{cases}$$

This shows that $\mathfrak{O}_{d,S}$ is contained in $\Omega_{d,S}$. Let Y be a closed H_S-orbit. Then

$$\mu_Y(Y \cap \Omega_{d,S}) \geq \mu_Y(Y \cap \mathfrak{O}_{d,S}) \geq \frac{1}{2}\mu_Y(Y)$$

by Lemma 8.3.5. □

8.3.4 Effective recurrence of unipotent flows

The purpose of this subsection is to explain how to obtain Proposition 8.3.10 from the fairly general [KT07, Theorem 9.3] of Kleinbock and Tomanov. We'll introduce three new concepts needed to state the result of Kleinbock and Tomanov and we'll establish the auxiliary results for the proof of Proposition 8.3.10, which is given at the end of the subsection.

Let Z be a metric space. We denote by $B_Z(z,r)$ the open ball with center $z \in Z$ and radius r. We say that Z is a *Besicovitch space* if there exist a positive integer N_Z with the following property:

- **Besicovitch property:** *For any bounded subset A of Z and any function $r : A \to (0,\infty)$, there is a finite or countable subset $\mathscr{B}$ of*

$$\mathscr{B}_r := \{B_Z(a, r(a)) \mid a \in A\} \tag{8.5}$$

that still covers A, and such that any point of Z belongs to at most N_Z elements of $\mathscr{B}$.

For example, $\mathbb{Q}_p$—more generally any ultrametric space—is a Besicovitch space with $N_{\mathbb{Q}_p} = 1$. Indeed, for any pair of open balls in $\mathbb{Q}_p$, either they are disjoint or one is contained in the other. Consider a bounded subset A of $\mathbb{Q}_p$ and a positive function r on A. If r is unbounded, let $a_0 \in A$ with $r(a_0) > diam(A)$. We can choose $\mathscr{B} = \{B_Z(a_0, r(a_0))\}$. If r is bounded, any point of A is in a unique maximal—with respect to the inclusion—element of $\mathscr{B}_r$. We take $\mathscr{B}$ as the subset of maximal elements of $\mathscr{B}_r$. Notice that $\mathscr{B}$ is at most countable because any two distinct elements of it are disjoint and $\mathbb{Q}_p$ is second-countable.

As a second example, $\mathbb{R}^d$ with its standard metric is a Besicovitch space according to Besicovitch's Covering Theorem. For a proof see [Mat95, p. 30]. It's easy to see that if three intervals of $\mathbb{R}$ meet, one of them is contained in the union of the other two, so $N_{\mathbb{R}} = 2$.

Next, we introduce a measure-theoretic analog of Besicovitch spaces. We say that a Borel measure λ on a metric space Z is *doubling* if for any $c > 1$

$$D_\lambda(c) = \sup\left\{\frac{\lambda(B_Z(z,cr))}{\lambda(B_Z(z,r))} \mid z \in supp\,\lambda, r > 0\right\} \tag{8.6}$$

is finite.

The Haar measure of $\mathbb{R}$ is doubling since $D_{\lambda_{\mathbb{R}}}(c) = c$. Let's see that the Haar measure $\lambda_{\mathbb{Q}_p}$ of $\mathbb{Q}_p$ is also doubling. We take the standard normalization $\lambda_{\mathbb{Q}_p}(\mathbb{Z}_p) = 1$. Then the measure of a closed ball of radius p^n is p^{-n} for any $n \in \mathbb{Z}$. It follows that

$$rp^{-1} \leq \lambda_{\mathbb{Q}_p}(B_{\mathbb{Q}_p}(z,r)) < r$$

for any $z \in \mathbb{Q}_p$ and any $r > 0$, so

$$\frac{\lambda_{\mathbb{Q}_p}(B_{\mathbb{Q}_p}(z, cr))}{\lambda_{\mathbb{Q}_p}(B_{\mathbb{Q}_p}(z, r))} < cp \tag{8.7}$$

for any $c > 1$. This shows that $D_{\lambda_{\mathbb{Q}_p}}(c) \leq cp$.

Lastly, we are interested in a class of functions that can't take small values for a long time. Let's formalize this intuition. Let Z be a metric space and let K be a field endowed with an absolute value $|\cdot|$. Consider a non-empty subset B of Z and a measurable function $F : Z \to K$. We define

$$B(F, \varepsilon) = \{b \in B \mid |F(b)| < \varepsilon\} \tag{8.8}$$

for any $\varepsilon > 0$. If λ is a Borel measure on Z and B meets $supp\,\lambda$, we define

$$||F||_{B,\lambda} = \sup\{|F(b)| \mid b \in B \cap supp\,\lambda\}.$$

Let $C, \vartheta > 0$. We say that F is (C, ϑ)-good with respect to λ if

$$\lambda(B(F, \varepsilon)) \leq C \left(\frac{\varepsilon}{||F||_{B,\lambda}}\right)^{\vartheta} \lambda(B)$$

for any open ball B of Z centered at a point in $supp\,\lambda$. When Z is a completion $\mathbb{Q}_\nu$ of $\mathbb{Q}$, we'll simply call (C, ϑ)-good a (C, ϑ)-good function with respect to the Haar measure $\lambda_{\mathbb{Q}_\nu}$. We will write$||\cdot||_B$ instead of $||\cdot||_{B,\lambda_{\mathbb{Q}_\nu}}$.

The main example of (C, ϑ)-good functions are polynomial maps. The next result for real polynomials is due to Kleinbock and Margulis in [KM98, Proposition 3.2].

Lemma 8.3.12. *Consider a non-zero polynomial $q(t) \in \mathbb{R}[t]$ of degree d. If $d \leq d_0$, then $q(t)$ defines a $\left(d_0(d_0+1)^{\frac{1}{d_0}}, 1/d_0\right)$-good function on $\mathbb{R}$.*

We prove now a p-adic analog of this result.

Lemma 8.3.13. *Consider a non-zero polynomial $q(t) \in \mathbb{Q}_p[t]$ of degree d. If $d \leq d_0$, then $q(t)$ defines a $(d_0^2 p, 1/d_0)$-good function on $\mathbb{Q}_p$.*

We break the proof of Lemma 8.3.13 into three easy lemmas. We fix a non-zero polynomial $q(t)$ of degree d with coefficients in $\mathbb{Q}_p$. Let m be a positive integer. We define $I_m(\varepsilon)$ as the set of integers $0 \leq a \leq p^m - 1$ such that $(p^m\mathbb{Z}_p + a) \cap \mathbb{Z}_p(q, \varepsilon)$ is non-empty.

Lemma 8.3.14. *Let $m \geq 0$. If $\#I_m(\varepsilon) \geq d + 1$, then*

$$||q||_{\mathbb{Z}_p} \leq \varepsilon p^{d(m-1)}.$$

Proof. Consider pairwise different elements $a_0, \ldots, a_d$ in $I_m(\varepsilon)$ and $t_i \in a_i + p^m\mathbb{Z}_p$ with $|q(t_i)|_p < \varepsilon$. Notice that

$$|a_i - a_j|_p \geq p^{-(m-1)}.$$

Using Lagrange's Interpolation Formula we write $q(t)$ as

$$q(t) = \sum_{i=0}^{d} q(t_i) \prod_{j \neq i} \frac{t - t_j}{t_i - t_j}.$$

For any $z \in \mathbb{Z}_p$ and any i we have

$$\left| q(t_i) \prod_{j \neq i} \frac{z - t_j}{t_i - t_j} \right|_p \leq \varepsilon p^{d(m-1)},$$

hence $|q(z)|_p \leq \varepsilon p^{d(m-1)}$. □

Lemma 8.3.15. *For any $m \geq 1$ and any $\varepsilon > 0$ we have*

$$\lambda_{\mathbb{Q}_p}(\mathbb{Z}_p(q, \varepsilon)) \leq p^{-m} \# I_m(p).$$

Proof. The measure of $\mathbb{Z}_p(q, \varepsilon)$—defined in (8.8)—less or equal than the measure of

$$\bigcup_{a \in I_m(\varepsilon)} a + p^m \mathbb{Z}_p$$

because the first set is contained in the second. □

Lemma 8.3.16. *Suppose that $q(t) \in \mathbb{Q}_p[t]$ is non-zero and has degree $\leq d_0$. Then*

$$\lambda_{\mathbb{Q}_p}(\mathbb{Z}_p(q, \varepsilon)) \leq d_0^2 p \left(\frac{\varepsilon}{||q||_{\mathbb{Z}_p}} \right)^{\frac{1}{d_0}}.$$

Proof. We choose $m_0 \geq 1$ such that

$$p^{m_0 - 1} < d_0 + 1 \leq p^{m_0}.$$

Then $p^{m_0 - 1} \leq d_0$ and $p^{m_0} \leq d_0 p$.

If $\lambda_{\mathbb{Q}_p}(\mathbb{Z}_p(q, \varepsilon)) = 0$ the inequality we want is true. Suppose now that $\lambda_{\mathbb{Q}_p}(\mathbb{Z}_p(q, \varepsilon))$ is positive and choose $m \geq 1$ such that

$$p^{-m} < \frac{\lambda_{\mathbb{Q}_p}(\mathbb{Z}_p(q, \varepsilon))}{d_0} \leq p^{-(m-1)}.$$

By Lemma 8.3.15 we have

$$\lambda_{\mathbb{Q}_p}(\mathbb{Z}_p(q, \varepsilon)) \leq p^{-(m+m_0)} \# I_{m+m_0}(\varepsilon),$$

and we also know that $d_0 p^{-(m+m_0)} < \lambda_{\mathbb{Q}_p}(\mathbb{Z}_p(q, \varepsilon))$, thus

$$\# I_{m+m_0}(\varepsilon) \geq d_0 + 1,$$

so we can use now Lemma 8.3.14:

$$||q||_{\mathbb{Z}_p} \leq \varepsilon p^{d_0 m_0} p^{d_0(m-1)} \leq \varepsilon (d_0 p)^{d_0} \left(\frac{d_0}{\lambda_{\mathbb{Q}_p}(\mathbb{Z}_p(q, \varepsilon))} \right)^{d_0}.$$

This is equivalent to the inequality of the statement. □

We are ready to prove that polynomial maps on $\mathbb{Q}_p$ are (C, ϑ)-good.

Proof of Lemma 8.3.13. Let B be a ball in $\mathbb{Q}_p$. We write it as $z + p^n\mathbb{Z}_p$ with $z \in \mathbb{Q}_p$ and $n \in \mathbb{Z}$. The degree of $Q(t) = q(z + p^n t)$ is also d and $||Q||_{\mathbb{Z}_p} = ||q||_B$. By Lemma 8.3.16 we have

$$\lambda_{\mathbb{Q}_p}(\mathbb{Z}_p(Q, \varepsilon)) \leq d_0^2 p \left(\frac{\varepsilon}{||q||_B}\right)^{\frac{1}{d_0}}. \tag{8.9}$$

From the equality

$$B(q, \varepsilon) = z + p^n(\mathbb{Z}_p(Q, \varepsilon))$$

we deduce that

$$\lambda_{\mathbb{Q}_p}(\mathbb{Z}_p(Q, \varepsilon)) = p^n \lambda_{\mathbb{Q}_p}(B(q, \varepsilon)) = \frac{\lambda_{\mathbb{Q}_p}(B(q, \varepsilon))}{\lambda_{\mathbb{Q}_p}(B)},$$

which combined with (8.9) yields

$$\lambda_{\mathbb{Q}_p}(B(q, \varepsilon)) \leq d_0^2 p \left(\frac{\varepsilon}{||q||_B}\right)^{\frac{1}{d_0}} \lambda_{\mathbb{Q}_p}(B).$$

□

We need two simple property of (C, ϑ)-good functions.

Lemma 8.3.17. *Consider two measurable functions $F, F_1 : \mathbb{Q}_\nu \to \mathbb{Q}_\nu$.*

(i) If F and F_1 are (C, ϑ)-good, then $\max\{|F|_\nu, |F_1|_\nu\}$ is (C, ϑ)-good.

(ii) If F^2 is (C, ϑ)-good, then F is $(C, 2\vartheta)$-good.

Proof. We start with (i). Set $F_m = \max\{|F|_\nu, |F_1|_\nu\}$ and let B be a ball in $\mathbb{Q}_\nu$. It's easy to see that

$$B(F_m, \varepsilon) = B(F, \varepsilon) \cap B(F_1, \varepsilon),$$

and $||F_m||_B = \max\{||F||_B, ||F_1||_B\}$. Suppose that $||F_m||_B = ||F||_B$. Since $B(F_m, \varepsilon)$ is contained in $B(F, \varepsilon)$ and F is (C, ϑ)-good, then

$$\lambda_{\mathbb{Q}_\nu}(B(F_m, \varepsilon)) \leq \lambda_{\mathbb{Q}_\nu}(B(F, \varepsilon)) \leq C \left(\frac{\varepsilon}{||F||_B}\right)^{\vartheta} \lambda_{\mathbb{Q}_\nu}(B).$$

Thus F is (C, ϑ)-good.

We pass to (ii). Notice that $||F^2||_B = ||F||_B^2$ and $B(F^2, \varepsilon^2) = B(F, \varepsilon)$ for any $\varepsilon > 0$. Since F^2 is (C, ϑ)-good, then

$$\begin{aligned}\lambda_{\mathbb{Q}_\nu}(B(F, \varepsilon)) = \lambda_{\mathbb{Q}_\nu}(B(F^2, \varepsilon^2)) &\leq C \left(\frac{\varepsilon^2}{||F^2||_B}\right)^{\vartheta} \lambda_{\mathbb{Q}_\nu}(B) \\ &= C \left(\frac{\varepsilon}{||F||_B}\right)^{2\vartheta} \lambda_{\mathbb{Q}_\nu}(B),\end{aligned}$$

so F is (C, ϑ)-good. □

Here is finally [KT07, Theorem 9.3] of Kleinbock and Tomanov. Recall that if Δ is a lattice of $\mathbb{Q}_S^d$ we denote by $\Sigma(\Delta)$ the set of non-zero $\mathbb{Z}_S$-submodules of Δ.

Theorem 8.3.18. *Consider a Besicovitch metric space Z, a doubling measure λ on Z and a finite set $S = \{\infty\} \cup S_f$ of primes. Let $B = B_Z(z_0, r)$, $\widetilde{B} = B_Z(z_0, 3^d r)$, and let F be a continuous function $\widetilde{B} \to GL(d, \mathbb{Q}_S)$. Suppose that the real numbers $C, \vartheta > 0$ and $\rho \in (0, 1)$ verify the following: for every $\Delta' \in \Sigma(\mathbb{Z}_S^d)$*

(i) The map $\psi_{\Delta'} : z \mapsto cov(F(z)\Delta')$ is (C, ϑ)-good with respect to λ on $\widetilde{B}$;

(ii) $||\psi_{\Delta'}||_{B,\lambda} \geq \rho$.

Then, for any $0 < \varepsilon \leq \rho$ one has

$$\lambda(\{z \in B \mid \alpha_1(F(z)\mathbb{Z}_S^d) < \varepsilon\}) \leq dC(N_Z D_\lambda(3)^2)^d \left(\frac{\varepsilon}{\rho}\right)^\vartheta \lambda(B),$$

with N_Z and $D_\lambda(3)$ as in (8.5) and (8.6), respectively.

The effective recurrence of unipotent flows—Proposition 8.3.10—follows easily from Theorem 8.3.18.

Proof of Proposition 8.3.10. We write Δ as $g\mathbb{Z}_S^d$ for some $g \in G_{d,S}^1$ and we define $F(t) = u_t g$ for $t \in \mathbb{Q}_\nu$. Since $u_t = \exp(tv)$ for some nilpotent $d \times d$ matrix v, then

$$F(t)_\nu = (q_{ij}(t))_{1 \leq i,j \leq d}$$

for polynomials $q_{ij}(t)$ with coefficients in $\mathbb{Q}_\nu$, of degree at most $d-1$. Take any $\Delta' \in \Sigma(\mathbb{Z}_S^d)$ and a basis $v_1, \ldots, v_k$ of it. By (8.4) we have

$$\psi_{\Delta'}(t) = cov(F(t)\Delta') = cov(\Delta', S - \{\nu\}) \cdot ||(F(t)v_1)_\nu \wedge \cdots \wedge (F(t)v_k)_\nu||_\nu,$$

where $cov(\Delta', S - \{\nu\})$ is the constant

$$\prod_{\nu \in S - \{\nu\}} ||(gv_1)_\nu \wedge \cdots (gv_k)_\nu||_\nu.$$

Writing the $(F(t)v_i)_\nu$ in terms of the canonical basis $e_1, \ldots, e_d$ of $\mathbb{Q}_\nu^d$ and expanding the wedge product we see that

$$(F(t)v_1)_\nu \wedge \cdots \wedge (F(t)v_k)_\nu = \sum_J Q_J(t) e_{j_1} \wedge \cdots \wedge e_{j_k}$$

for $Q_J(t) \in \mathbb{Q}_\nu[t]$ of degree at most $(d-1)^2$, with at least one $Q_J(t) \neq 0$. Here J runs over all the k-tuples of integers $(j_1, \ldots, j_k)$ with $1 \leq j_1 < \ldots < j_k \leq d$. Hence

$$\psi_{\Delta'} = \begin{cases} (\sum_J Q_J(t)^2)^{\frac{1}{2}} & \text{if } \nu = \infty, \\ \max_J |Q_J(t)|_p & \text{if } \nu = p. \end{cases}$$

Lemmas 8.3.12, 8.3.13 and 8.3.17 imply that $\psi_{\Delta'}$ is [11]

$$\begin{cases} (2^2(d-1)^2, \vartheta_d)\text{-good if } \nu = \infty, \\ ((d-1)^2 p, \vartheta_d)\text{-good if } \nu = p. \end{cases}$$

[11] In the case $\nu = \infty$ we replace the factor $(d_0 + 1)^{\frac{1}{d_0}}$ of Lemma 8.3.12 by 2, which is bigger for $d_0 \geq 2$. Here $d_0 = 2(d-1)^2$.

Take $\varepsilon \in (0,1)$. We apply Theorem 8.3.18 to $Z = \mathbb{Q}_\nu, \lambda = \lambda_{\mathbb{Q}_\nu}$, and F. Consider $\rho \in (\varepsilon, 1)$ and

$$B = B_\nu(T) := \{z \in \mathbb{Q}_\nu \mid |z|_\nu < T\}.$$

We already showed that condition (i) of Theorem 8.3.18 holds for any $\Delta' \in \Sigma(\mathbb{Z}_S^d)$. Now we'll show that (ii) holds if T is big enough. If $F(0) = cov(g\Delta') \geq 1$ we are done. Otherwise $g\Delta'$ belongs to the finite set[12]

$$\Sigma_{<1}(\Delta) = \{g\Delta'_1, \dots, g\Delta'_\ell\}.$$

We write

$$\psi_{\Delta'_i} = \begin{cases} \left(\sum_J Q_{i,J}(t)^2\right)^{\frac{1}{2}} & \text{if } \nu = \infty, \\ \max_J |Q_{i,J}(t)|_p. & \text{if } \nu = p. \end{cases}$$

for some polynomials $Q_{i,J}(t)$. Since (u_t) does not preserve the $\mathbb{Q}_S$-module generated by $g\Delta'_i$, some $Q_{i,J}(t)$ is not constant. Thus there is $t_i \in \mathbb{Q}_\nu$ such that $\psi_{\Delta'_i}(t_i) > 1$. Let

$$T_0 = T_0((u_t), \Delta) = \max_{1 \leq i \leq \ell} |t_i|_\nu.$$

Conditon (ii) is satisfied if $T \geq T_0$. Recall that

$$D_\lambda(3) \begin{cases} = 3 & \text{if } \nu = \infty, \\ \leq 3p & \text{if } \nu = p. \end{cases}$$

The Besicovitch constants of $\mathbb{R}$ and $\mathbb{Q}_p$ are 2 and 1, respectively. Theorem 8.3.18 implies that

$$\frac{\lambda(\{z \in B_\nu(T) \mid \alpha_1(u_t\Delta) < \varepsilon\})}{\lambda(B_\nu(T))} \leq \begin{cases} d(2^2(d-1)^2)(2 \cdot 3^2)^d \left(\varepsilon/\rho\right)^{\vartheta_d} & \text{if } \nu = \infty, \\ d((d-1)^2 p)(3p)^{2d} \left(\varepsilon/\rho\right)^{\vartheta_d} & \text{if } \nu = p. \end{cases}$$

Making ρ tend to 1 we obtain

$$\frac{\lambda(\{z \in B_\nu(T) \mid \alpha_1(u_t\Delta) < \varepsilon\})}{\lambda(B_\nu(T))} \leq \begin{cases} 3^{2d} d^3 2^{d+2} \varepsilon^{\vartheta_d} & \text{if } \nu = \infty, \\ 3^{2d} d^3 p^{2d+1} \varepsilon^{\vartheta_d} & \text{if } \nu = p, \end{cases}$$

as claimed. □

8.4 Transversal recurrence of closed H_S-orbits

Let H_S be the orthogonal group of a non-degenerate, isotropic diagonal quadratic form on $\mathbb{Q}_S^d$. In this section we prove a transversal recurrence phenomenon for closed H_S-orbits in $X^1_{d,S}$—Lemma 8.1.3—for $d \geq 3$. The idea of the proof is simple: Let $W_{d,S}$ be a transversal to H_S in $G^1_{d,S}$. If no point of Y returns to Y under a non-trivial element of $(W_{d,S})^{-1}W_{d,S}$, then the volume $\beta_{d,S}(W_{d,S}Y)$[13] of the box $W_{d,S}Y$ is equal to the product of the volumes of $W_{d,S}$

[12] It is finite because for any $1 \leq k < d$, the set $\{w_1 \wedge \cdots \wedge w_k \mid w_i \in \Delta\}$ is discrete in $\bigwedge^k \mathbb{Q}_S^d$.

[13] Recall that $\beta_{d,S}$ is the $G^1_{d,S}$-invariant measure on $X^1_{d,S}$.

and Y. Since $\beta_{d,S}(W_{d,S}Y)$ is at most $\beta_{d,S}(X^1_{d,S})$, $W_{d,S}$ can't be too big. The objective of this section is to formalize these ideas. It is divided into five parts: first we give a convenient description of $X^1_{d,S}$ and we fix the Haar measures on various groups we'll work with in 8.4.1. The transversal $W_{d,S}$ will be constructed working separately in each $G_{d,\nu}$. In 8.4.2 we do $\nu = \infty$, and $\nu = p$ in 8.4.3. These results are put together in 8.4.4 to get $W_{d,S}$. Finally, we prove Lemma 8.1.3 in 8.4.5.

8.4.1 Preliminary remarks

First we give a description of $X^1_{d,S}$ better suited for this section, changing the group $G^1_{d,S}$—a semi-direct product—by a direct product $G'_{d,S}$. If ν is a prime, we define

$$G'_{d,\nu} = \{g \in G_{d,\nu} \mid |\det g|_\nu = 1\},$$

and $G'_{d,S} = \prod_{\nu\in S} G'_{d,\nu}$. Let's see that $G'_{d,S}$ acts transitively on $X^1_{d,S}$, which justifies the identification of this space with $G'_{d,S}/\Gamma'_{d,S}$, where $\Gamma'_{d,S} = \Gamma_{d,S} \cap G'_{d,S}$. If g is in $G^1_{d,S}$,

$$|\det g_\infty|_\infty \cdot \prod_{p\in S_f} |\det g_p|_p = \mathscr{H}_S(\det g) = 1,$$

so $\det g_\infty$ is a unit in $\mathbb{Z}_S$. Then

$$diag(\det g_\infty^{-1}, 1, \dots, 1)$$

is in $GL(d, \mathbb{Z}_S)$. Let γ_g be the diagonal image of this matrix in $\Gamma_{d,S}$. Then $gx^1_{d,S} = (g\gamma_g)x^1_{d,S}$ and $g\gamma_g$ is in $G'_{d,S}$.

We fix now the Haar measures $\lambda_{G'_\nu}$ of the groups $G'_{d,\nu}$. As explained in Appendix A, a basis of the Lie algebra $\mathfrak{g}'_{d,\nu}$ determines naturally a normalization of $\lambda_{G'_\nu}$. Let $(x_1, \dots, x_d)$ be the coordinates on $\mathbb{Q}^d$ of the canonical basis $e_1, \dots, e_d$, and let $e_1^*, \dots, e_d^* \in (\mathbb{Q}^d)^*$ be the dual basis. We denote by E_{ij} the matrix of $e_i \otimes e_j^*$ and $F_k = E_{kk} - E_{dd}$. On $\mathfrak{g}'_{d,\infty} = \mathfrak{sl}(d, \mathbb{R})$ we take

$$(F_1, \dots, F_{d-1}, E_{12}, E_{23}, \dots, E_{d-1,d}, E_{13}, \dots, E_{d-2,d}, \dots, E_{1d}, E_{21}, \dots, E_{d,d-1}, E_{31}, \dots, E_{d,d-2}, \dots, E_{d,1}). \tag{8.10}$$

On $\mathfrak{g}'_{d,p} = \mathfrak{gl}(d, \mathbb{Q}_p)$ we consider the basis E_{ij}, $1 \le i, j \le d$. We endow $G'_{d,S}$ with the Haar measure $\otimes_{\nu\in S}\lambda_{G'_\nu}$ and $X^1_{d,S}$ with the $G'_{d,S}$-invariant measure $\beta_{d,S}$ induced by $\lambda_{G'_S}$.

Let ν be a prime and consider the orthogonal group H_ν of the non-degenerate diagonal quadratic form $a_1x_1^2 + \cdots + a_dx_d^2$. We'll work with the Haar measure λ_{H_ν} of H_ν determined by the basis

$$\beta_{d,H_\nu} = (H_{12}, H_{23}, \dots, H_{d-1,d}, H_{13}, \dots, H_{d-2,d}, \dots, H_{1d}), \tag{8.11}$$

of $\mathfrak{h}_\nu$, where $H_{ij} = E_{ij} - a_ia_j^{-1}E_{ji}$. If S is a finite set of primes and $H_S = \prod_{\nu\in S} H_\nu$, we define $\lambda_{H_S} = \otimes_{\nu\in S}\lambda_{H_\nu}$.

8.4.2 The transversal in the real factor

Let $P_\infty(x) = a_1x_1^2 + \cdots + a_dx_d^2$ with $a_1, \ldots, a_d \in \mathbb{R}^\times$, and $H_\infty = O(P_\infty, \mathbb{R})$. Consider the subgroup $W_{d,\infty}$ of lower-triangular matrices of $G'_{d,\infty}$ with positive entries in the main diagonal. Here we'll show that H_∞ and $W_{d,\infty}$ are transversal, and we'll estimate the volume of small neighborhoods of I_d in $W_{d,\infty}$.

First we fix the Haar measure λ_{W_∞} on $W_{d,\infty}$ given by the basis

$$\beta_{d,W} = (F_1, \ldots, F_{d-1}, E_{21}, E_{32}, \ldots, E_{d,d-1}, E_{3,1}, \ldots, E_{d,d-2}, \ldots, E_{d1}) \tag{8.12}$$

of its Lie algebra $\mathfrak{w}_{d,\infty}$. We prove now that $W_{d,\infty}$ is transversal to H_∞ and that $\lambda_{G'_\infty}$ decomposes nicely on $W_{d,\infty}H_\infty$.

Lemma 8.4.1. *Let H_∞ be the orthogonal group of a non-degenerate diagonal real quadratic form $P_\infty(x)$ in d variables.*

(*i*) *The multiplication map $W_{d,\infty} \times H_\infty \to G'_{d,\infty}$ is injective and the image $W_{d,\infty}H_\infty$ is open in $G'_{d,\infty}$.*

(*ii*) *On $W_{d,\infty}H_\infty$ we have $\lambda_{G'_\infty} = \lambda_{W_\infty} \otimes \lambda_{H_\infty}$.*

Proof. Since $P_\infty(x)$ is diagonal, the only lower-triangular matrices in H_∞ are those of the form $diag(\pm 1, \ldots, \pm 1)$. Hence $H_\infty \cap W_{d,\infty} = 1$. Take $w_1, w_2 \in W_{d,\infty}$ and $h_1, h_2 \in H_\infty$. Then

$$w_1h_1 = w_2h_2 \Leftrightarrow w_2^{-1}w_1 = h_2h_1^{-1},$$

but this last element is in $H_\infty \cap W_{d,\infty}$, so the equality holds if and only if $w_1 = w_2$ and $h_1 = h_2$. This proves that the multiplication map $\mathcal{M} : W_{d,\infty} \times H_\infty \to W_{d,\infty}H_\infty$ is injective.

We prove now that $W_{d,\infty}H_\infty$ is open. The group $W_{d,\infty} \times H_\infty$ acts on $G'_{d,\infty}$ by

$$(w, h) \cdot g = wgh^{-1},$$

and $W_{d,\infty}H_\infty$ is an orbit, thus it suffices to prove that $W_{d,\infty}H_\infty$ contains an open neighborhood of I_d in $G'_{d,\infty}$. This follows from the Inverse Function Theorem: The derivative

$$D\mathcal{M}_{(I_d,I_d)} : \mathfrak{w}_{d,\infty} \times \mathfrak{h}_\infty \to \mathfrak{sl}(d, \mathbb{R})$$

is the map $(v_1, v_2) \mapsto v_1 + v_2$, which is a linear isomorphism. This completes the proof of (*i*).

We pass to (*ii*). An homogeneous space of the form G_0/H_0 with G_0 and H_0 locally compact groups and H_0 compact admits a unique (up to multiplication by a positive scalar) Radon measure—see [Wei40, p. 45]. Thus $\lambda_{W_\infty} \otimes \lambda_{H_\infty}$ is the only $(W_{d,\infty} \times H_\infty)$-invariant measure on $W_{d,\infty}H_\infty$. Since $G'_{d,\infty}$ is unimodular, $\lambda_{G'_\infty}$ is $W_{d,\infty}$ invariant on the left and H_∞-invariant on the right, hence

$$\lambda_{G'_\infty} = c(\lambda_{W_\infty} \otimes \lambda_{H_\infty})$$

for some $c > 0$. To prove that $c = 1$ is suffices to see that the two measures are defined by the same—up to sign—multilinear map in $\bigwedge^{d^2-1}(\mathfrak{sl}(d, \mathbb{R}))^*$—see the conventions we made right before the statement of this lemma. The base-change matrix from the concatenation of the bases in (8.12) and (8.11) to the one of (8.10) has determinant 1 because it is unipotent, upper-triangular, so we are done. □

For the volume comparison argument in the proof of Lemma 8.1.3 we'll replace $W_{d,\infty}$ by a neighborhood of I_d in $W_{d,\infty}$. We use the following estimation of its volume, proved in A.3.1 of Appendix A. Let's fix notation: consider on $\mathfrak{gl}(d,\mathbb{R})$ the operator norm $||\cdot||_{op}$ with respect to the norm $||\cdot||_\infty$ on $\mathbb{R}^d$. The exponential map is a bijection between $\mathfrak{w}_{d,\infty}$ and $W_{d,\infty}$. For any $r>0$ we define

$$\mathfrak{B}_{\mathfrak{w}_\infty}(r)=\{v\in\mathfrak{w}_{d,\infty}\mid ||v||_{op}<r\}$$

and

$$W_{d,\infty}(r)=\exp(\mathfrak{B}_{\mathfrak{w}_\infty}(r)).$$

Recall that $c_d=\frac{d(d+1)}{2}-1$.

Lemma 8.4.2. *For any $0<r<\frac{1}{2}$ we have*

$$V_d^- r^{c_d}<\lambda_{W_\infty}(W_{d,\infty}(r))<V_d^+ r^{c_d},$$

where $V_d^-=\frac{2^{d-1}}{d^{2c_d}}$ and $V_d^+=2^{d^2-1}$.

8.4.3 The transversal in the p-adic factor

Let $H_p=O(P,\mathbb{Q}_p)$ for a diagonal quadratic form $P(x)=a_1x_1^2+\ldots+a_dx_d^2$ with $a_1,\ldots,a_d\in\mathbb{Q}_p^\times$. Consider also the subgroup $W_{d,p}$ of lower-triangular matrices of $G_{d,p}=GL(d,\mathbb{Q}_p)$. Now we'll see that H_p and an open subgroup of $W_{d,p}$ are transversal. We also compute the volume of small neighborhoods of I_d in $W_{d,p}$.

We'll work with the Haar measure λ_{W_p} on $W_{d,p}$ determined by the basis

$$(E_{11},\ldots,E_{dd},E_{21},E_{32},\ldots,E_{d,d-1},\ldots,E_{d1})$$

of its Lie algebra $\mathfrak{w}_{d,p}$.

This time $W_{d,p}\times H_p\to G_{d,p}$ is not injective, but it has finite kernel, and λ_{G_p} also decomposes nicely on $W_{d,p}H_p$.

Lemma 8.4.3. *Let $H_p=O(P,\mathbb{Q}_p)$ with P as above.*

(i) The image $W_{d,p}H_p$ of the multiplication map $W_{d,p}\times H_p\to G_{d,p}$ is open in $G_{d,p}$.

(ii) On $W_{d,p}H_p$ we have $\lambda_{G_p}=\lambda_{W_p}\otimes\lambda_{H_p}$.

Proof. The derivative at (I_d,I_d) of $W_{d,p}\times H_p\to G_{d,p}$ is the addition map

$$\mathfrak{w}_{d,p}\times\mathfrak{h}_p\to\mathfrak{gl}(d,\mathbb{Q}_p),\quad (v_1,v_2)\mapsto v_1+v_2,$$

which is a linear isomorphism. By the Inverse Function Theorem—see [Ser92, p. 73] for a proof that works also in the p-adic case—we get that $W_{d,p}H_p$ is a neighborhood of I_d in $G_{d,p}$. Thus $W_{d,p}H_p$ is open in $G_{d,p}$ since it's a $(W_{d,p}\times H_p)$-orbit in $G_{d,p}$.

We denote

$$\Lambda=\{(g,g^{-1})\mid g\in W_\infty\cap H_\infty\},$$

and we identify $W_{d,p}H_p$ with $(W_{d,p}\times H_p)/\Lambda$. It admits a $(W_{d,p}\times H_p)$-invariant Radon measure, unique up to multiplication by a positive constant, because Λ is finite. This traduces to a unique measure on $W_{d,p}H_p$ that is $W_{d,p}$-invariant on the left and H_p-invariant on the right. $\lambda_{W_p}\otimes\lambda_{H_p}$ and λ_{G_p} verify this condition, hence they differ by multiplication by some $c>0$. To see that $c=1$ we use the same argument as in the proof of Lemma 8.4.1. □

In the next lemma—proved in A.3.2 of Appendix A—ee shrink $W_{d,p}$ to obtain a *strict* transversal to H_p, and we compute the volume of small compact-open subgroups of $W_{d,p}$. We define

$$W_{d,p}(r) = \{w \in W_{d,p} \mid ||w - I_d||_p \leq r, ||w^{-1} - I_d||_p \leq r\}$$

for any $r > 0$. Recall that $c_d = \frac{d(d+1)}{2} - 1$.

Lemma 8.4.4. *Let p be a prime number. We set $\ell_p = 1$ if p is odd and $\ell_p = 2$ if $p = 2$. The multiplication map $W_{d,p}(p^{\ell_p}) \times H_p \to G_{d,p}$ is injective, $W_{d,p}(p^{-\ell_p})H_p$ is open in $G_{d,p}$ and*

$$\lambda_{W_p}(W_{d,p}(p^{-n})) = p^{-(c_d+1)n}$$

for any $n \geq 3$.

8.4.4 The S-adic transversal

Let $S = \{\infty\} \cup S_f$ be a finite set of primes. Consider $P(x) = a_1x_1^2 + \cdots + a_dx_d^2$ with $a_1, \ldots, a_d \in \mathbb{Q}_S^\times$ and let $H_S = O(P, \mathbb{Q}_S)$. Now we combine the results of the previous two sections to get the transversal to H_S in $G'_{d,S}$. The structure is the same as in the last two subsections.

We define

$$W_{d,S} = W_{\infty,d} \times \prod_{p \in S_f} W_{d,p}(p^{-3}),$$

and

$$W_{d,S}(r) = W_{\infty,d}(r) \times \prod_{p \in S_f} W_{d,p}(p^{-3})$$

for any $r > 0$. We endow H_S and $W_{d,S}$ with their respective (left for W_S) Haar measures

$$\lambda_{H_S} = \otimes_{\nu \in S} \lambda_{H_\nu}, \quad \lambda_{W_S} = \otimes_{\nu \in S} \lambda_{W_\nu},$$

with the normalizations chosen before in each factor.

For future reference we state here the fact that $W_{d,S}$ is transversal to H_S and the relation between the Haar measures of $W_{d,S}, H_S$ and $G'_{d,S}$. This follows directly from lemmas 8.4.1, 8.4.3 and A.3.4.

Lemma 8.4.5. *Let $S = \{\infty\} \cup S_f$ be a finite set of primes and let H_S be the orthogonal group of a non-degenerate diagonal quadratic form on $\mathbb{Q}_S^d$.*

(i) The multiplication map $W_{d,S} \times H_S \to G'_{d,S}$ is injective and $W_{d,S}H_S$ is open in $G'_{d,S}$.

(ii) On $W_{d,S}H_S$ we have

$$\lambda_{G'_S} = \lambda_{W_S} \otimes \lambda_{H_S}.$$

Now we estimate the volume of $W_{d,s}(r)$.

Lemma 8.4.6. *Let $S = \{\infty\} \cup S_f$ be a finite set of primes. For any $0 < r < \frac{1}{2}$ we have*

$$V_d^- p_S^{-3(c_d+1)} r^{c_d} < \lambda_{W_S}(W_{d,S}(r)) < V_d^+ p_S^{-3(c_d+1)} r^{c_d},$$

where $V_d^- = \frac{2^{d-1}}{d^{2c_d}}$ and $V_d^+ = 2^{d^2-1}$.

Proof. By Lemma 8.4.4 we have

$$\lambda_{W_S}(W_{d,S}(r)) = \lambda_{W_\infty}(W_{\infty,d}(r)) \cdot \prod_{p\in S_f} \lambda_{W_p}(W_{d,p}(p^{-3})) = \lambda_{W_\infty}(W_{\infty,d}(r))p_S^{-3(c_d+1)},$$

hence the result follows from the bounds for $\lambda_{W_\infty}(W_{\infty,d}(r))$ of Lemma 8.4.2, which hold when r is in $\left(0, \frac{1}{2}\right)$. □

8.4.5 The proof of Lemma 8.1.3

Here we'll finally prove the transversal recurrence for closed H_S-orbits after presenting the two last intermediate results we'll use.

Let $d \geq 3$. We consider $P(x) = a_1x_1^2+\cdots+a_dx_d^2$ with $a_1, \ldots, a_d \in \mathbb{Q}_S^\times$ and $H_S = O(P, \mathbb{Q}_S)$. Suppose that H_S is non-compact. Let $\Omega_{d,S}$ be the compact subset of $X^1_{d,S}$ of Lemma 8.1.2. Let Y be a closed H_S-orbit in $X^1_{d,S}$. The proof of Lemma 8.1.3 is based on two observations:

1. If no point of $Y \cap \Omega_{d,S}$ lands back in Y under any $w \in W_{d,S}(r) - \{I_d\}$, the volume of the box is $\lambda_{W_{d,S}}(W_{d,S}(r))\mu_Y(Y \cap \Omega_{d,S})$.

2. the volume of the box $W_{d,S}(r)(Y \cap \Omega_{d,S})$ is less or equal than the volume of $X^1_{d,S}$

Here are the last two intermedidate results we'll use in the main proof. We denote by Ψ^r_Y the map

$$W_{d,S}(r) \times (Y \cap \Omega_{d,S}) \to X^1_{d,S}, \quad (w, y) \mapsto wy.$$

Recall that $\mathcal{V}_{d,\infty} = \beta_{\infty,d}(X^1_{\infty,d})$. For the next lemma we define

$$B_d = \frac{2\mathcal{V}_{d,\infty}{}^{\frac{1}{c_d}}}{d(d-1)}.$$

Lemma 8.4.7. *Let $d \geq 3$ and let Y be a closed H_S-orbit in $X^1_{d,S}$. If Ψ^r_Y is injective and $r < \frac{1}{2}$, then*

$$r < B_d p_S^4 \mu_Y(Y)^{-\frac{1}{c_d}}.$$

Proof. Since d is fixed, to simplify the notation we'll omit the d in the subindices of $X^1_{d,S}, W_{d,S}$ and $\Omega_{d,S}$. Let y_0 be a base point in $Y \cap \Omega_S$ and let $\widetilde{Y}$ be a measurable subset of H_S such that

$$\widetilde{Y} \to Y \cap \Omega_S, \quad h \mapsto hy_0$$

is bijective. If Ψ^r_Y in injective, then

$$W_S(r)\widetilde{Y} \to X^1_{d,S}, \quad wh \mapsto why_0$$

is also injective, hence

$$\beta(W_S(r)(Y \cap \Omega_S)) = \lambda_{G'_S}(W_S(r)\widetilde{Y}).$$

We know that $\lambda_{G'_S} = \lambda_{W_S} \otimes \lambda_{H_S}$ on $W_S H_S$—see Lemma 8.4.5—, so

$$\begin{aligned}\lambda_{G'_S}(W_S(r)\widetilde{Y}) &= \lambda_{W_S}(W_S(r))\lambda_{H_S}(\widetilde{Y}) \\ &= \lambda_{W_S}(W_S(r))\mu_Y(Y \cap \Omega_S) \\ &> \left(V_d^- p_S^{-3(c_d+1)} r^{c_d}\right)\left(\frac{\mu_Y(Y)}{2}\right).\end{aligned}$$

To obtain the last inequality we used Lemma 8.4.6 and Lemma 8.1.2. The volume of $W_S(r)(Y \cap \Omega_S)$ is strictly smaller than $2\beta S, d(X^1_{d,S})$ and $\beta_{d,S}(X^1_{d,S}) < \mathcal{V}_{d,\infty}$ by Corollary A.4.2, hence

$$\frac{V_d^-}{2} p_S^{-3(c_d+1)} \mu_Y(Y) r^{c_d} < 2\mathcal{V}_{d,\infty}.$$

We finally get

$$r < \left(\frac{2^{d+1}}{(d(d-1))^{c_d}} p_S^{3(c_d+1)} \mathcal{V}_{d,\infty} \mu_Y(Y)^{-1}\right)^{\frac{1}{c_d}} < B_d p_S^4 \mu_Y(Y)^{-\frac{1}{c_d}}.$$

□

Lemma 8.4.8. *We have*

$$e^{2r} - 1 < 4r$$

for any $r \in \left(0, \frac{1}{2}\right)$.

Proof. The function $\frac{1}{r}(e^{2r} - 1)$ is increasing on $(0, \infty)$, so

$$\frac{e^{2r} - 1}{r} < 2(e - 1) < 4$$

if $0 < r < \frac{1}{2}$. □

We are ready to prove the transversal recurrence of closed H_S-orbits.

Proof of Lemma 8.1.3. Let Y be a closed H_S-orbit in $X^1_{d,S}$. Recall that

$$A_d = \left(\frac{4}{d(d-1)}\right)^{c_d} \mathcal{V}_{d,\infty} \qquad \text{and} \qquad B_d = \frac{2\mathcal{V}_{d,\infty}^{\frac{1}{c_d}}}{d(d-1)}.$$

We define

$$r_Y = B_d p_S^4 \mu_Y(Y)^{-\frac{1}{c_d}}.$$

Notice that $r_Y < \frac{1}{2}$ if and only if $\mu_Y(Y) > A_d p_S^{4c_d}$. Suppose that this is the case. Then $\Psi_Y^{r_Y}$ isn't injective by Lemma 8.4.7. Take $w \neq w'$ in $W_{d,S}(r_Y)$ and $y, y' \in Y \cap \Omega_{d,S}$ such that $w^{-1}w'y = y'$. We set $u = w^{-1}w'$. Then $u(Y \cap \Omega_{d,S})$ meets Y. We have $w_\nu \neq w'_\nu$ for some $\nu \in S$, hence $u_\nu \notin H_\nu$ by (i) of Lemma 8.4.1 or Lemma 8.4.3 if $\nu = \infty$ or $\nu = p$, respectively. Thus u is not in H_S. Notice that $||u_p||_p = 1$ for any $p \in S_f$ because u_p is in $W_{d,p}(p^{-3}) \subseteq GL(d, \mathbb{Z}_p)$. To conclude we estimate $||u_\infty - I_d||_\infty$. By definition of $W_{\infty,d}(r_Y)$,

$$w = \exp v, \quad w' = \exp v'$$

for some $v, v' \in \mathfrak{w}_{d,\infty}$ with $||v||_{op}, ||v'||_{op} < r_Y$. Then

$$\begin{aligned}
||u_\infty - I_d||_\infty &\leq ||w_\infty^{-1} w'_\infty - I_d||_{op} \\
&\leq ||w_\infty^{-1} w'_\infty - w'_\infty||_{op} + ||w'_\infty - I_d||_{op} \\
&\leq ||w_\infty^{-1} - I_d||_{op} ||w'_\infty||_{op} + ||w'_\infty - I_d||_{op} \\
&< (e^{r_Y} - 1) e^{r_Y} + (e^{r_Y} - 1) \\
&= e^{2r_Y} - 1 \\
&< 4r_Y = C_d^{(4)} p_S^4 \mu_Y(Y)^{-\frac{1}{c_d}},
\end{aligned}$$

where $C_d^{(4)} = \frac{2^3 \mathcal{V}_d^{\frac{1}{c_d}}}{d(d-1)}$. This completes the proof. □

Chapter 9

Generating sets of S-integral orthogonal groups

This chapter is based on a classical result of Siegel in his landmark article [Sie72]: *The integral orthogonal group of an integral quadratic form is finitely generated.* Here we'll obtain an effective S-adic extension of this fact. The case $S = \{\infty\}$ was treated by Li and Margulis in [LM16, Theorem 2]. Before giving their result, let's recall some notation: if Q is an integral quadratic form in d variables, b_Q is its matrix in the standard basis of $\mathbb{Q}^d$, $||Q||_\infty = ||b_Q||_\infty$ and $\delta_Q = \det b_Q$.

Theorem 9.0.1. *For any $d \geq 3$ there is a constant B_d with the following property: Let Q be a non-degenerate integral quadratic form in $d \geq 3$ variables. Then $O(Q, \mathbb{Z})$ is generated by the $\gamma \in O(Q, \mathbb{Z})$ with*

$$||\gamma||_\infty \leq B_d ||Q||_\infty^{3d^4} |\delta_Q|_\infty^{d^6}.$$

Consider now a finite set $S = \{\infty\} \cup S_f$ of primes. Our statements treat the interesting case, namely integral quadratic forms Q isotropic over $\mathbb{Q}_S$[1] We formulate our results separately for $\mathbb{R}$-isotropic and $\mathbb{R}$-anisotropic quadratic forms, as we did for our criteria of $\mathbb{Z}_S$-equivalence. For the explicit values of the constants $\mathcal{K}_d, \mathcal{F}_{1,d}$ and $\mathcal{F}_{2,d}$ in the next two theorems, see Appendix C.

Theorem 9.0.2. *Consider a non-degenerate $\mathbb{R}$-isotropic integral quadratic form Q in $d \geq 3$ variables and a finite set $S = \{\infty\} \cup S_f$ of primes with $S_f \neq \emptyset$. The group $O(Q, \mathbb{Z}_S)$ is generated by the $\xi \in O(Q, \mathbb{Z}_S)$ with*

$$\begin{aligned} &||\xi||_\infty < \mathcal{K}_d p_S^{20d^7} ||Q||_\infty^{d^4} |\delta_Q|_\infty^{3d^5}, \\ &||\xi||_p < p^{2d+2} |\delta_Q|_p^{-\frac{1}{2}} \qquad \text{for } p \in S_f. \end{aligned}$$

Theorem 9.0.3. *Consider an $\mathbb{R}$-anisotropic integral quadratic form Q in $d \geq 3$ variables and a finite set $S = \{\infty\} \cup S_f$ of primes. Suppose that Q is $\mathbb{Q}_{p_0}$-isotropic for some $p_0 > 2$ in*

[1] When Q is anisotropic over $\mathbb{Q}_S$, $O(Q, \mathbb{Z}_S)$ is finite because it is a discrete subgroup of the compact group $O(Q, \mathbb{Q}_S)$.

S_f. The group $O(Q,\mathbb{Z}_S)$ is generated by the $\xi \in O(Q,\mathbb{Z}_S)$ with

$$\begin{aligned} ||\xi||_{p_0} &\leq \mathcal{F}_{1,d} p_S^{14d^7} ||Q||_\infty^{\frac{1}{2}d^4} |\delta_Q|_\infty^{d^5}, \\ ||\xi||_p &\leq p^{2d+2} |\delta_Q|_p^{-\frac{1}{2}} \qquad \text{for } p \in S_f - \{p_0\}, \\ ||\xi||_\infty &\leq \mathcal{F}_{2,d} p_S^{4d^3} ||Q||_\infty^{\frac{d}{2}} |\delta_Q|_\infty^{d^3}. \end{aligned}$$

We establish these two results adapting the strategy of Li and Margulis for $S = \{\infty\}$. Here is the basic notation we'll use: let Q be a non-degenerate integral quadratic form in d variables. We denote by $\mathbf{H}^Q$ the orthogonal group of Q. If $S = \{\infty\} \cup S_f$ is a finite set of primes, we denote by Γ_S^Q the diagonal copy of $O(Q,\mathbb{Z}_S)$ in H_S^Q. We'll work with Γ_S^Q instead of $O(Q,\mathbb{Z}_S)$.

The chapter is organized as follows: In Section 9.1 we prove a lemma that constructs a generating set $\mathscr{G}_S^Q$ of Γ_S^Q from a generating set M_S^Q of H_S^Q and a fundamental set U_S^Q of Γ_S^Q in H_S^Q. Then, we give M_S^Q and U_S^Q respectively in Section 9.2 and Section 9.3. The description of U_S^Q depends on a certain finite subset $\mathscr{T}_S^Q$ of $\Gamma_{d,S}$ which will be carefully chosen in Section 9.4. We conclude with the proofs of the main results of the chapter in Section 9.5.

9.1 The basic lemma

The proofs of the two main results use the next lemma that gives a generating set of a subgroup Γ_0 of a group H_0.

Lemma 9.1.1. *Let Γ_0 be a subgroup of a group H_0. Suppose that M and U are subsets of H_0 such that*

$$H_0 = \bigcup_{n\geq 1} M^n = U\Gamma_0.$$

Then Γ_0 is generated by $(U^{-1}MU) \cap \Gamma_0$.

Proof. Let $A_n = U^{-1}M^nU$ for any positive integer n. Since $H_0 = \cup_{n\geq 1} A_n$, to show that $\Lambda := \langle A_1 \cap \Gamma_0 \rangle$ coincides with Γ_0 it suffices to prove that $A_n \cap \Gamma_0$ is contained in Λ for any $n \geq 1$. We show this by induction on n. This is true for $n = 1$ by the definition of Λ. Suppose now that $A_\ell \cap \Gamma_0 \subseteq \Lambda$ for $1 \leq \ell \leq n$ and consider $\gamma_{n+1} \in A_{n+1} \cap \Gamma_0$. Take $u_1, u_2 \in U$ and $m_1, \ldots, m_{n+1} \in M$ such that

$$\gamma_{n+1} = u_1^{-1} m_1 \cdots m_{n+1} u_2.$$

We write $m_{n+1}u_2$ as $u_3\gamma_1$ for some $u_3 \in U$ and $\gamma_1 \in \Gamma_0$. Then γ_1 and $\gamma_n = u_1^{-1}m_1 \cdots m_n u_3$ are respectively in $A_1 \cap \Gamma_0$ and $A_n \cap \Gamma_0$. By the inductive hypothesis, γ_1, γ_n belong to Λ, hence $\gamma_{n+1} = \gamma_n\gamma_1$ as well. □

When $H_0 = U\Gamma_0$ as in Lemma 9.1.1 we'll say that U is a *fundamental set* of Γ_0 in H_0. Lemma 9.1.1 builds a generating set of Γ_0 in terms of a generating set of the ambient group H_0 and a fundamental set of Γ_0.

9.2 A generating set of H_S^Q

Here we give a generating set of H_S^Q. Since H_S^Q is conjugated to the orthogonal group H_S of a standard quadratic form on $\mathbb{Q}_S^d$, the task reduces to finding a generating set M_ν of H_ν for $\nu \in S$. When $\nu = \infty$, we take M_∞ as any subset of H_∞ with non-empty interior meeting every connected component of H_∞.

For H_p we'll do something similar, replacing the connected components by H_p°-cosets of H_p. Recall that H_p° is the image in H_p of the corresponding *Spin* group.

Lemma 9.2.1. *Consider a prime $p > 2$ and an integer $d \geq 3$. Any orthogonal group H_p of a standard quadratic form on $\mathbb{Q}_p^d$ is generated by the $h \in H_p$ with $||h||_p \leq p^2$.*

Proof. □

9.3 A fundamental set of Γ_S^Q in H_S^Q

Now we construct a fundamental set U_S^Q of Γ_S^Q in H_S^Q by analogy with the classical case $S = \{\infty\}$, first treated by Siegel in [Sie39]. His argument relies on the reduction theory of real quadratic forms[2], which in turn is based on the concept of Siegel sets of $GL(d, \mathbb{R})$. This section has two parts: in 9.3.1 we introduce the Siegel sets of $GL(d, \mathbb{Q}_S)$, which we use in 9.3.2 to construct U_S^Q.

9.3.1 Siegel sets of GL(d)

We denote by $\mathbf{G}_d$ the $\mathbb{Q}$-group $\mathbf{GL}(d)$. Let $S = \{\infty\} \cup S_f$ be a finite set of primes. We introduce here the *Siegel sets* $\mathscr{S}_{d,S}^{\alpha,\beta}$ of $G_{d,S}$, a family of subsets of $G_{d,S}$ that depends on two positive parameters α, β. They play a key role in the study of S-arithmetic groups because any lattice in $\mathbb{Q}_S^d$ is of the form $g\mathbb{Z}_S^d$ for $g \in \mathscr{S}_{d,S}^{\alpha,\beta}$ when α and β are big enough.

Let's start with $S = \{\infty\}$. Consider the following subgroups of $G_{d,\infty}$:

$$\begin{aligned} K &= O(d, \mathbb{R}) \\ A &= \{diag(a_1, \cdots, a_d) \in G_{d,\infty} \mid a_i > 0 \text{ for every } 1 \leq i \leq d\}, \\ N &= \{\text{unipotent, upper-triangular matrices in } G_{d,\infty}\}. \end{aligned}$$

For $\alpha, \beta > 0$ we define

$$\begin{aligned} A_\alpha &= \{diag(a_1, \cdots, a_d) \in A \mid a_i \leq \alpha a_{i+1} \text{ for } 1 \leq i \leq d-1\}, \\ N_\beta &= \{n \in N \mid ||n - I_d||_\infty \leq \beta\}. \end{aligned}$$

The (α, β)-Siegel set of $G_{d,\infty}$ is defined as

$$\mathscr{S}_{d,\infty}^{\alpha,\beta} = KA_\alpha N_\beta.$$

[2]See Appendix B for the basic definitions and [Bor69, Chapitre I; §2, §5] for a complete discussion.

For a general $S = \{\infty\} \cup S_f$ we define the (α, β)-Siegel set of $G_{d,S}$ as

$$\mathscr{S}_{d,S}^{\alpha,\beta} = \mathscr{S}_{d,\infty}^{\alpha,\beta} \times \prod_{p \in S_f} GL(d, \mathbb{Z}_p).$$

Recall that $\Gamma_{d,S}$ is the diagonal copy of $GL(d, \mathbb{Z}_S)$ in $G_{d,S}$. The standard way to give a fundamental set of $\Gamma_{d,S}$ in $G_{d,S}$ is using the Siegel sets.

Proposition 9.3.1. *Consider a finite set of primes $S = \{\infty\} \cup S_f$ and $d \geq 2$. If $\alpha \geq \frac{2}{\sqrt{3}}$ and $\beta \geq \frac{1}{2}$, then*

$$G_{d,S} = \mathscr{S}_{d,S}^{\alpha,\beta} \Gamma_{d,S}.$$

See [Ben09, Lemma 2.2] and [PR94, Proposition 5.7] for the proofs for $S = \{\infty\}$ and $GL(d, \mathbb{Q}) \subseteq GL(d, \mathbb{A})$, respectively. The same argument gives Proposition 9.3.1.

9.3.2 Construction of U_S^Q

Let's see how to describe a fundamental set of Γ_S^Q in H_S^Q. We'll use some ideas from the reduction theory of quadratic forms on $\mathbb{Q}_S^d$.

Let $S = \{\infty\} \cup S_f$ be a finite set of primes. We say that a quadratic form R on $\mathbb{Q}_S^d$ is (α, β)-reduced if we can write it as $P \circ s$ for a standard quadratic form[3] P on $\mathbb{Q}_S^d$ and some $s \in \mathscr{S}_{d,S}^{\alpha,\beta}$. If B is a quadratic form on $\mathbb{Q}^d$, we write B_S when we consider it as quadratic form on $\mathbb{Q}_S^d$ via the diagonal embedding $Q \to \mathbb{Q}_S$. We say that B is (S, α, β)-reduced if B_S is (α, β)-reduced. Here are some basic properties of reduced quadratic forms.

Lemma 9.3.2. *Let $S = \{\infty\} \cup S_f$ be a finite set of primes. Consider an $(S, 2, 1)$-reduced quadratic form R in $d \geq 3$ variables with coefficients in $\mathbb{Z}_S$, and an integral quadratic form Q in d variables. Then:*

(i) R is integral and $p^{-2} \leq |\delta_R|_p \leq 1$ for $p \in S_f$.

(ii) If $Q = R \circ \gamma$ for some $\gamma \in GL(d, \mathbb{Z}_S)$, then $|\delta_R|_\infty \leq p_S^2 |\delta_Q|_\infty$,

$$p_S^{-1} \leq |\det \gamma|_\infty \leq |\delta_Q|_\infty^{\frac{1}{2}} \qquad \text{and} \qquad |\delta_Q|_p^{\frac{1}{2}} \leq |\det \gamma|_p \leq p |\delta_Q|_p^{\frac{1}{2}}$$

for $p \in S_f$.

Proof. Let $b_R, b_Q \in GL(d, \mathbb{Q})$ be the matrices of R and Q in the canonical basis of $\mathbb{Q}^d$. Write $R_S = P \circ s$ for $s \in \mathscr{S}_{d,S}^{2,1}$ and a standard quadratic form $P = (P_\nu)_{\nu \in S}$ on $\mathbb{Q}_S^d$. Let $c \in G_{d,S}$ be the matrix of P in the canonical basis of $\mathbb{Q}_S^d$.

Let's prove (i). Recall that $R = P_p \circ s_p$ and $s_p \in GL(d, \mathbb{Z}_p)$ for $p \in S_f$, so

$$|\delta_R|_p = |\det s_p|_p^2 \cdot |(\delta_P)_p|_p = |(\delta_P)_p|_p,$$

[3] Recall that this means that $P = (P_\nu)_{\nu \in S}$ and that each P_ν is a standard quadratic form on $\mathbb{Q}_\nu^d$, which are defined in Section 3.2 for $\nu = \infty$ and in Subsection 3.3.1 for $\nu = p$.

thus[4] $p^{-2} \leq |\delta_R|_p \leq 1$. The matrix $b_R \in M_d(\mathbb{Z}_S)$ verifies

$$||b_R||_p \leq ||{}^t s_p||_p ||c_p||_p ||s_p||_p \leq 1$$

for any $p \in S_f$, so b_R is integral.

Now suppose that we are in the situation of (ii). Since R and Q are $\mathbb{Z}_S$-equivalent, $\mathscr{H}_S(\delta_R) = \mathscr{H}_S(\delta_Q)$. Using (i) we get

$$p_S^2 |\delta_R|_\infty \leq \mathscr{H}_S(\delta_R) = \mathscr{H}_S(\delta_Q) \leq |\delta_Q|_\infty,$$

which proves the first inequality. For the second one, since ${}^t\gamma b_R \gamma = b_Q$ and $|\delta_R|_\infty \geq 1$ because R is integral, then

$$|\det \gamma|_\infty = \left(\frac{|\delta_Q|_\infty}{|\delta_R|_\infty}\right)^{\frac{1}{2}} \leq |\delta_Q|_\infty^{\frac{1}{2}} \quad \text{and} \quad |\det \gamma|_\infty^{-1} = \left(\frac{|\delta_R|_\infty}{|\delta_Q|_\infty}\right)^{\frac{1}{2}} \leq p_S.$$

Let's prove the third inequality. For $p \in S_f$ we have

$$|\det \gamma|_p = \left(\frac{|\delta_Q|_p}{|\delta_R|_p}\right)^{\frac{1}{2}},$$

so $|\delta_Q|_p^{\frac{1}{2}} \leq |\det \gamma|_p \leq p|\delta_Q|_p^{\frac{1}{2}}$ by (i). □

We denote by $\mathscr{R}_S^Q$ the set of rational quadratic forms that are $\mathbb{Z}_S$-equivalent to Q and $(S, 2, 1)$-reduced.

Lemma 9.3.3. *Let Q be a non-degenerate integral quadratic form in d variables. The set $\mathscr{R}_S^Q$ is finite for any finite set $S = \{\infty\} \cup S_f$ of primes.*

Proof. Any $R \in \mathscr{R}_S^Q$ is integral by Lemma 9.3.2, so

$$|\delta_R|_\infty \leq \mathscr{H}_S(\delta_R) = \mathscr{H}_S(\delta_Q).$$

Also, R is $(2,1)$-reduced as real quadratic form because the real factor of $\mathscr{S}_{d,S}^{\alpha,\beta}$ is the (α, β) Siegel set of $GL(d, \mathbb{R})$. By Proposition B.3.1 there are finitely many $(2,1)$-reduced integral quadratic forms on $\mathbb{R}^d$ of bounded determinant. □

Let's see how to obtain a fundamental set of Γ_S^Q in H_S^Q from $\mathscr{R}_S^Q$ and $\mathscr{S}_{d,S}^{2,1}$. Any $R \in \mathscr{R}_S^Q$ is in fact integral by Lemma 9.3.2. We choose $\tau_R \in \Gamma_{d,S}$ such that $R_S \circ \tau_R = Q_S$—in the next section we'll pick a convenient τ_R—and we define

$$\mathscr{T}_S^Q = \{\tau_R \mid R \in \mathscr{R}_S^Q\},$$

which is finite since $\mathscr{R}_S^Q$ is by Lemma 9.3.3.

[4] Since P_p is standard, then $|(\delta_P)_p|_p$ is either p^{-2}, p^{-1} or 1.

Lemma 9.3.4. *Let Q be a non-degenerate integral quadratic form in $d \geq 2$ variables. Consider a finite set of primes $S = \{\infty\} \cup S_f$ and the standard quadratic form P on $\mathbb{Q}_S^d$ that is $\mathbb{Q}_S$-equivalent to Q_S. Set*

$$U_S^Q = \left(g^{-1}\mathscr{S}_{d,S}^{2,1}\mathscr{T}_S^Q\right) \cap H_S^Q,$$

where $g \in G_{d,S}$ takes P to Q_S. Then $H_S^Q = U_S^Q\Gamma_S^Q$.

Proof. Take $h \in H_S^Q$. By Proposition 9.3.1 we can write gh as $s\gamma^{-1}$ for some $s \in \mathscr{S}_{d,S}^{2,1}$ and $\gamma = (\gamma_0, \ldots, \gamma_0) \in \Gamma_{d,S}$. Let $R = Q \circ \gamma_0$. From $Q_S = P \circ (gh)$ we obtain $Q_S \circ \gamma = P \circ s$, so R is in $\mathscr{R}_S^Q$. Consider $\tau \in \mathscr{T}_S^Q$ such that $R_S \circ \tau = Q_S$. Then $\tau^{-1}\gamma^{-1}$ is in Γ_S^Q because

$$Q_S \circ \gamma = R_S = Q_S \circ \tau^{-1}.$$

Notice also that $u = g^{-1}s\tau$ belongs to U_S^Q, and $h = u(\tau^{-1}\gamma^{-1})$, so we are done. □

9.4 Choosing a small generating set

Recall that Lemma 9.1.1 gives a generating set $\mathscr{G}_S^Q$ of Γ_S^Q from a generating set M_S^Q of H_S^Q—obtained in Section 9.2—and a fundamental set U_S^Q of Γ_S^Q in H_S^Q. We described such an U_S^Q in Section 9.3 in terms of a subset $\mathscr{T}_S^Q$ of $\Gamma_{d,S}$. Here, using our effective criteria of $\mathbb{Z}_S$-equivalence of quadratic forms—theorems 5.1.1 and 5.1.2—, we choose a $\mathscr{T}_S^Q$ that will allow us to control the size of the elements of $\mathscr{G}_S^Q$ in Section 9.5.

We state separately the results for $\mathbb{R}$-isotropic and $\mathbb{R}$-anisotropic quadratic forms.

Lemma 9.4.1. *Consider a non-degenerate $\mathbb{R}$-isotropic integral quadratic form Q in $d \geq 3$ variables, a finite non-empty set S_f of odd primes and $S = \{\infty\} \cup S_f$. For any $R \in \mathscr{R}_S^Q$ there is $\gamma_R \in GL(d, \mathbb{Z}_S)$ that takes R to Q with*

$$\begin{aligned} &||\gamma_R||_\infty \leq \mathcal{G}_d p_S^{19d^6+5d^4}||Q||^{d^3}|\delta_Q|_\infty^{2d^4+2d^2} && \\ &||\gamma_R||_p \leq p^2 && \text{for } p \in S_f. \end{aligned},$$

Here $\mathcal{G}_d = 2^{d^5}\mathcal{C}_{i,d}W_{2,d}{}^{d^3}$ with $\mathcal{C}_{i,d}$ as in Theorem 5.1.1 and $W_{2,d}$ as in Lemma B.3.1.

Proof. Any $R \in \mathscr{R}_S^Q$ is integral by Lemma 9.3.2, so Theorem 5.1.1 shows there is $\gamma_R \in GL(d, \mathbb{Z}_S)$ taking R to Q with

$$||\gamma_R||_\infty < \mathcal{C}_{i,d}p_S^{19d^6}(||R||_\infty||Q||_\infty)^{d^3}|\delta_R\delta_Q|_\infty^{d^2},$$

and $||\gamma_R||_p \leq p|\delta_R|_p^{-\frac{1}{2}}$ for $p \in S_f$.

We'll replace the terms in R by terms in Q. Recall that $|\delta_R|_\infty \leq p_S^2|\delta_Q|_\infty$—see Lemma 9.3.2. Note also that R is reduced as real quadratic form since R_S is (2,1)-reduced and

$$\mathscr{S}_{d,S}^{2,1} = \mathscr{S}_{d,\infty}^{2,1} \times \prod_{p \in S_f} GL(d, \mathbb{Z}_p).$$

Then, by Proposition B.3.1

$$||R||_\infty \leq 2^{d^2}W_{2,d}|\delta_R|_\infty^{2d} \leq 2^{d^2}W_{2,d}p_S^{4d}|\delta_Q|_\infty^{2d}.$$

To conclude we bound the norms of γ_R:

$$\begin{aligned}||\gamma_R||_\infty &\leq \mathcal{C}_{i,d} p_S^{19d^6}(2^{d^2} W_{2,d} p_S^{4d} |\delta_Q|_\infty^{2d})^{d^3} ||Q||_\infty^{d^3} (p_S^2 |\delta_Q|_\infty^2)^{d^2} \\ &\leq \mathcal{G}_d p_S^{19d^6+5d^4} ||Q||_\infty^{d^3} |\delta_Q|_\infty^{2d^4+2d^2},\end{aligned}$$

where $\mathcal{G}_d = 2^{d^5} \mathcal{C}_{i,d} W_{2,d}^{d^3}$ with $\mathcal{C}_{i,d}$ and $W_{2,d}$ respectively as in Theorem 5.1.1 and Lemma B.3.1. Also

$$||\gamma_R||_p \leq p|\delta_R|_p^{-\frac{1}{2}} \leq p^2$$

by Lemma 9.3.2, for $p \in S_f$. □

Lemma 9.4.2. *Consider an $\mathbb{R}$-anisotropic integral quadratic form Q in $d \geq 3$ variables and a finite set $S = \{\infty\} \cup S_f$ of primes with $2 \notin S$. Suppose that Q is $\mathbb{Q}_{p_0}$ isotropic for some $p_0 > 2$ in S_f. For any $R \in \mathscr{R}_S^Q$ there is $\gamma_R \in GL(d, \mathbb{Z}_S)$ that takes R to Q with*

$$\begin{aligned}&||\gamma_R||_{p_0} \leq \mathcal{H}_{1,d} p_S^{13d^6+2d^4} ||Q||_\infty^{\frac{1}{2}d^2(d-1)} |\delta_Q|_\infty^{d^3(d-1)+7}, \\ &||\gamma_R||_p \leq p^2 \qquad\qquad \text{for } p \in S_f, \\ &||\gamma_R||_\infty \leq \mathcal{H}_{2,d} p_S^{2d(d-1)} ||Q||_\infty^{\frac{1}{2}} |\delta_Q|_\infty^{d(d-1)}.\end{aligned}$$

Here $\mathcal{H}_{1,d} = 2^{d^5} \mathcal{C}_{a,d} W_{2,d}{}^{\frac{1}{2}d^2(d-1)}$ and $\mathcal{H}_{2,d} = 2^{d^3} d^{d+1} \cdot d! W_{2,d}{}^{\frac{d-1}{2}}$ with $\mathcal{C}_{a,d}$ as in Theorem 5.1.2 and $W_{2,d}$ as in Lemma B.3.1.

Proof. Any $R \in \mathscr{R}_S^Q$ is integral, and the upper bounds for $|\delta_R|_\nu$ and $||R||_\infty$ in the proof of Lemma 9.4.1 remain valid in the current situation. Consider $\gamma_R \in GL(d, \mathbb{Z}_S)$ taking R to Q as in Theorem 5.1.2. We have

$$\begin{aligned}||\gamma_R||_{p_0} &\leq \mathcal{C}_{a,d} p_S^{13d^6} (||R||_\infty ||Q||_\infty)^{\frac{1}{2}d^2(d-1)} |\delta_R \delta_Q|_\infty^{\frac{7}{2}} \\ &\leq \mathcal{C}_{a,d} p_S^{13d^6} (2^{d^2} W_{2,d} p_S^{4d} ||Q||_\infty |\delta_Q|_\infty^{2d})^{\frac{1}{2}d^2(d-1)} (p_S^2 |\delta_Q|_\infty^2)^{\frac{7}{2}} \\ &\leq \mathcal{H}_{1,d} p_S^{13d^6+2d^4} ||Q||_\infty^{\frac{1}{2}d^2(d-1)} |\delta_Q|_\infty^{d^3(d-1)+7},\end{aligned}$$

where $\mathcal{H}_{1,d} = 2^{d^5} \mathcal{C}_{a,d} W_{2,d}^{\frac{1}{2}d^2(d-1)}$, with $\mathcal{C}_{a,d}$ and $W_{2,d}$ respectively as in Theorem 5.1.2 and Lemma B.3.1. For $p \in S_f$,

$$||\gamma_R||_p \leq p|\delta_R|_p^{-\frac{1}{2}} \leq p^2,$$

and finally

$$\begin{aligned}||\gamma_R||_\infty &\leq d^{d+1} \cdot d! ||R||_\infty^{\frac{d-1}{2}} ||Q||_\infty^{\frac{1}{2}} \\ &\leq \mathcal{H}_{2,d} p_S^{2d(d-1)} ||Q||_\infty^{\frac{1}{2}} |\delta_Q|_\infty^{d(d-1)},\end{aligned}$$

where $\mathcal{H}_{2,d} = 2^{d^3} d^{d+1} \cdot d! W_{2,d}^{\frac{d-1}{2}}$.

□

9.5 Proofs of the main theorems

Everything is now in place. We complete now the proofs of our effective results on generators of $O(Q, \mathbb{Z}_S)$. We start with the $\mathbb{R}$-isotropic case.

Proof of Theorem 9.0.2. We write $Q_S = P \circ g$ for a standard quadratic form P on $\mathbb{Q}_S^d$ and $g \in G_{d,S}$. Set $H_S = O(P, \mathbb{Q}_S)$, so H_∞ is non-compact. For $p \in S_f$ we define

$$M_p = \{h \in H_p \mid ||h||_p \leq p^2\},$$

which generates H_p by Lemma 9.2.1. Consider

$$M_\infty = \{diag(a_1, \dots, a_d) \mid a_i = \pm 1\}$$

and

$$M_\infty(\varepsilon) = M_\infty \cup \{h \in H_\infty \mid ||h - I_d||_\infty < \varepsilon\}.$$

Note that $M_\infty(\varepsilon)$ generetes H_∞ since it has non-empty interior and M_∞ meets all the connected components of H_∞. Hence $M_S(\varepsilon) = M_\infty(\varepsilon) \times \prod_{p \in S_f} M_p$ generates H_S and $M_S^Q(\varepsilon) = g^{-1} M_S(\varepsilon) g$ generates $H_S^Q = g^{-1} H_S g$ for any $\varepsilon > 0$. For each $R \in \mathscr{R}_S^Q$ we define $\tau_R = (\gamma_R, \dots, \gamma_R) \in \Gamma_{d,S}$ with γ_R taking R to Q as in Lemma 9.4.1, and we set

$$\mathscr{T}_S^Q = \{\tau_R \mid R \in \mathscr{R}_S^Q\}.$$

Consider

$$U_S^Q = (g^{-1} \mathscr{S}_{d,S}^{2,1} \mathscr{T}_S^Q) \cap H_S^Q.$$

Then $H_S^Q = U_S^Q \Gamma_S^Q$ by Lemma 9.3.4, and

$$\mathscr{G}_S^Q(\varepsilon) = ((U_S^Q)^{-1} M_S^Q(\varepsilon) U_S^Q) \cap \Gamma_S^Q$$

generates Γ_S^Q according to Lemma 9.1.1. Letting $\varepsilon \to 0$ we see that

$$\mathscr{G}_S^Q = ((U_S^Q)^{-1} M_S^Q U_S^Q) \cap \Gamma_S^Q$$

generates Γ_S^Q [5], where $M_S^Q = g^{-1} M_S g$. For any $\widetilde{\xi} \in \mathscr{G}_S^Q$, let ξ be the corresponding matrix in $GL(d, \mathbb{Z}_S)$. Let's see that any ξ verifies the bounds of the statement. We write

$$\widetilde{\xi} = \tau^{-1} s^{-1} g (g^{-1} m g) g^{-1} t \eta = \tau^{-1} s^{-1} m t \eta$$

with $\tau, \eta \in \mathscr{T}_S^Q, m \in M_S$ and $s, t \in \mathscr{S}_{d,S}^{2,1}$. Let $b' = s^{-1} m t = \tau \widetilde{\xi} \eta^{-1}$, so b' is in $\Gamma_{d,S}$. For $p \in S_f$ we have

$$||b'_p||_p = ||s_p^{-1} m_p t_p||_p \leq p^2,$$

so $b := p_S^2 b'_\infty$ has integral coefficients. The equality $s_\infty b = p_S^2 m_\infty t_\infty$ [6] shows that $\mathscr{S}_{d,\infty}^{2,1} b$ meets $\mathscr{S}_{d,\infty}^{2,1}$, so

$$||b||_\infty \leq W_{3,d} |\det b|_\infty^{2d} \tag{9.1}$$

[5] The reason for considering this set instead of $\mathscr{G}_S^Q(\varepsilon)$ is that M_∞ is contained in $O(d, \mathbb{R})$, unlike $M_S(\varepsilon)$.

[6] Here is where we use that M_∞ is contained in $O(d, \mathbb{R})$.

by Corollary B.2.11. Note that the determinant of $\xi = \tau_\infty^{-1} b'_\infty \eta_\infty$ is ± 1 since it preserves Q, so

$$|\det b'_\infty|_\infty = \frac{|\det \tau_\infty|_\infty}{|\det \eta_\infty|_\infty} \leq p_S |\delta_Q|_\infty^{\frac{1}{2}}$$

by Lemma 9.3.2. Writing (9.1) in terms of b' yields

$$||b'_\infty||_\infty \leq W_{3,d} p_S^{4d^2-2} |\det b'|_\infty^{2d} \leq W_{3,d} p_S^{8d^2} |\delta_Q|_\infty^d.$$

We are ready to bound ξ:

$$\begin{aligned}
||\xi||_\infty = ||\tau_\infty^{-1} b'_\infty \eta_\infty||_\infty &\leq d^2 ||\tau_\infty^{-1}||_\infty ||\eta_\infty||_\infty ||b'_\infty||_\infty \\
&\leq d \cdot d! \frac{||\tau_\infty||_\infty^{d-1} ||\eta_\infty||_\infty}{|\det \tau_\infty|_\infty} ||b'_\infty||_\infty \\
&\leq d \cdot d! p_S (\mathcal{G}_d p_S^{19d^6+5d^4} ||Q||_\infty^{d^3} |\delta_Q|_\infty^{2d^4+2d^2})^d (W_{3,d} p_S^{8d^2} |\delta_Q|_\infty^d) \\
&\leq \mathcal{K}_d p_S^{20d^7} ||Q||_\infty^{d^4} |\delta_Q|_\infty^{3d^5},
\end{aligned}$$

where $\mathcal{K}_d = d \cdot d! \mathcal{G}_d^d W_{3,d}$ with $\mathcal{G}_d$ and $W_{3,d}$ as in Lemma 9.4.1 and Corollary B.2.11, respectively. We also have

$$||\xi||_p = ||\tau_p^{-1} s_p^{-1} m_p t_p \eta_p||_p \leq ||m_p||_p \frac{||\tau_p||_p^{d-1} ||\eta_p||_p}{|\det \tau_p|_p} \leq p^{2d+2} |\delta_Q|_p^{-\frac{1}{2}}$$

for $p \in S_f$.

□

Proof of Theorem 9.0.3. Let H_S be the orthogonal group of the standard quadratic form P on $\mathbb{Q}_S^d$ that is $\mathbb{Q}_S$-equivalent to Q_S and consider $g \in G_{d,S}$ taking P to Q_S. Since Q is $\mathbb{R}$-anisotropic and $\mathbb{Q}_{p_0}$-isotropic, $H_\infty = O(d, \mathbb{R})$ and H_{p_0} is non-compact. Consider again

$$M_p = \{h \in H_p \mid ||h||_p \leq p^2\},$$

which generate H_p by Lemma 9.2.1. As generating set of H_∞ we take $M_\infty = H_\infty$. Note that $M_S = \prod_{\nu \in S} M_\nu$ generates H_S and $M_S^Q = g^{-1} M_S g$ generates $H_S^Q = g^{-1} H_S g$. For each $R \in \mathscr{R}_S^Q$ we define $\tau_R = (\gamma_R, \ldots, \gamma_R) \in \Gamma_{d,S}$ with $\gamma_R \in GL(d, \mathbb{Z}_S)$ taking R to Q as in Lemma 9.4.2. Consider $\mathscr{T}_S^Q, U_S^Q$ and $\mathscr{G}_S^Q$ as in the proof of Theorem 9.0.2. Once more, the $\widetilde{\xi} \in \mathscr{G}_S^Q$ generate Γ_S^Q, so the corresponding $\xi \in GL(d, \mathbb{Z}_S)$ generate $O(Q, \mathbb{Z}_S)$.

Let's see that these ξ verify the inequalities of the statement. We write

$$\widetilde{\xi} = \tau^{-1} s^{-1} m t \eta$$

with $\tau, \eta \in \mathscr{T}_S^Q$, $m \in M_S$ and $s, t \in \mathscr{S}_{d,S}^{2,1}$. We consider again $b' = s^{-1} m t = \tau \widetilde{\xi} \eta^{-1} \in \Gamma_{d,S}$. In the present situation the inequality

$$||b'_\infty||_\infty \leq W_{3,d} p_S^{8d^2} |\delta_Q|_\infty^d$$

still holds. We are ready to bound ξ:

$$\begin{aligned}||\xi_{p_0}||_{p_0} = ||\tau_{p_0}^{-1}s_{p_0}^{-1}m_{p_0}t_{p_0}\eta_{p_0}||_{p_0} &\leq p_0^2|\det\tau_{p_0}|_{p_0}^{-1}||\tau_{p_0}||_{p_0}^{d-1}||\eta_{p_0}||_{p_0}\\ &\leq p_0^2|\delta_Q|_{p_0}^{-\frac{1}{2}}(\mathcal{H}_{1,d}p_S^{13d^6+2d^4}||Q||_\infty^{\frac{1}{2}d^2(d-1)}|\delta_Q|_\infty^{d^3(d-1)+7})^d\\ &\leq \mathcal{F}_{1,d}p_S^{14d^7}||Q||_\infty^{\frac{1}{2}d^4}|\delta_Q|_\infty^{d^5},\end{aligned}$$

where $\mathcal{F}_{1,d} = \mathcal{H}_{1,d}^d$ with $\mathcal{H}_{1,d}$ and in Lemma 9.4.2. For $p \in S_f - \{p_0\}$ we have

$$||\xi||_p \leq p^2|\delta_Q|_p^{-\frac{1}{2}}||\tau_p||_p^{d-1}||\eta_p||_p \leq p^{2d+2}|\delta_Q|_p^{-\frac{1}{2}}.$$

An finally the ∞-norm:

$$\begin{aligned}||\xi||_\infty &\leq d\cdot d!\frac{||\tau_\infty||_\infty^{d-1}||\eta_\infty||_\infty}{|\det\tau_\infty|_\infty}||b'_\infty||_\infty\\ &\leq d\cdot d!p_S(\mathcal{H}_{2,d}p_S^{2d(d-1)}||Q||_\infty^{\frac{1}{2}}|\delta_Q|_\infty^{d(d-1)})^d(W_{3,d}p_S^{8d^2}|\delta_Q|_\infty^d)\\ &\leq \mathcal{F}_{2,d}p_S^{4d^3}||Q||_\infty^{\frac{d}{2}}|\delta_Q|_\infty^{d^3},\end{aligned}$$

where $\mathcal{F}_{2,d} = d\cdot d!\mathcal{H}_{2,d}^d W_{3,d}$ with $\mathcal{H}_{2,d}$ and $W_{3,d}$ respectively as in Lemma 9.4.2 and Corollary B.2.11. □

Appendix A

Volume computations

This appendix gathers volume computations on various Lie groups. The explicit constants in our criteria of $\mathbb{Z}_S$-equivalence—theorems 5.1.1 and 5.1.2—depend on these.

There are four parts. Section A.1 explains how to choose a Haar measure on a real or p-adic Lie group form a basis of its Lie algebra. Then, in Section A.2 we estimate the volume of neighborhoods of the identity in orthogonal groups and we build bump functions on real orthogonal groups. Section A.3 deals with volume estimates in groups of lower-triangular matrices. Finally, we prove a formula for the volume of the space of covolume 1 lattices of $\mathbb{Q}_S^d$ in Section A.4.

A.1 Haar measure on Lie groups

We start with general remarks. Let ν be a prime and let H_0 be a closed subgroup of $GL(d, \mathbb{Q}_\nu)$. Let's fix a choice of Haar measure on H_0 and Lebesgue measure on its Lie algebra $\mathfrak{h}_0$. Let $(y_1, \dots, y_k)$ be the coordinates on $\mathfrak{h}_0$ with respect to a basis β on $\mathfrak{h}_0$. We take $\lambda_{\mathfrak{h}_0}$ such that

$$\lambda_{\mathfrak{h}_0}(\{(y_1, \dots, y_k) \in \mathfrak{h}_0 \mid |y_1|_\nu, \dots, |y_k|_\nu \leq 1\} = \begin{cases} 2^k & \text{if } \nu = \infty, \\ 1 & \text{if } \nu = p. \end{cases}$$

Let ω be the left-invariant volume form on H_0 such that

$$\omega_{I_d} = (dy_1 \wedge \cdots \wedge dy_k)_0.$$

We denote by λ_{H_0} the left Haar measure on H_0 given by integration with respect to ω. We'll say that a Haar measure ν_{H_0} on H_0 and a Lebesgue measure $\nu_{\mathfrak{h}_0}$ on $\mathfrak{h}_0$ are compatible if they can be obtained from the same basis of $\mathfrak{h}_0$.

A.2 Orthogonal groups

The aim of this section is to establish volume estimates for open neighborhoods of the identity in real and p-adic orthogonal groups—Lemma A.2.1 and Lemma A.2.12, respectively. These were used in the proof of the dynamical statements of Chapter 6 and Chapter 7.

A.2.1 Real orthogonal groups

We treat first the case of real orthogonal groups. The goal of this subsection is to prove Lemma A.2.1.

Let $||\cdot||_\infty$ be the norm on $M_d(\mathbb{R})$ of the maximum of the absolute values of the entries. If $P(x)$ is a non-degenerate quadratic form on $\mathbb{R}^d$ we denote by H_P the group $O(P,\mathbb{R})$. As before, let b_P be the matrix of P in the canonical basis $e_1,\dots,e_d$ of $\mathbb{R}^d$. Then

$$\mathfrak{h}_P = \{v \in \mathfrak{gl}(d,\mathbb{R}) \mid {}^t v b_P + b_P v = 0\}.$$

If $P(x) = a_1x_1^2 + \cdots + a_dx_d^2$, we consider the basis of $\mathfrak{h}_P$ formed by

$$H_{ij} = E_{ij} - a_i a_j^{-1} E_{ji} \tag{A.1}$$

with $1 \le i < j \le d$. Here E_{ij} is the matrix of $e_j^* \otimes e_i$ and $e_1^*,\dots,e_d^*$ is the dual standard basis of $(\mathbb{R}^d)^*$. We'll denote by λ_{H_P} and $\lambda_{\mathfrak{h}_P}$ the Haar measures of H_P and $\mathfrak{h}_P$ induced by this basis. We'll estimate the measure of small symmetric balls of H_P centered at the identity:

$$H_P(r) = \{h \in H_P \mid ||h - I_d||_\infty < r, ||h^{-1} - I_d||_\infty < r\}.$$

Lemma A.2.1. *For every $d \ge 3$ there are positive constants $\mathtt{R}_d, \mathtt{S}_d$ with the following property: if $P(x) = a_1x_1^2 + \cdots + a_dx_d^2$ with each $a_i \in \{\pm 1\}$, then*

$$\mathtt{R}_d r^{\frac{1}{2}d(d-1)} < \lambda_{H_P}(H_P(r)) < \mathtt{S}_d r^{\frac{1}{2}d(d-1)}$$

if $r \le \frac{2}{5d}$.

In Lemma A.2.1 we can take

$$\mathtt{R}_d = \left(\frac{1}{3d}\right)^{\frac{d(d-1)}{2}} \quad \text{and} \quad \mathtt{S}_d = \left(\frac{20d}{3}\right)^{\frac{d(d-1)}{2}}.$$

The idea to prove Lemma A.2.1 is simple: if r is small, $H_P(r)$ is parametrized by via the exponential map of H_P. We'll see that $\lambda_{H_P}(H_P(r))$ and $\lambda_{\mathfrak{h}_P}(\exp^{-1} H_P(r))$ are comparable. We break the proof into several auxiliary lemmas.

Let $G_\infty = GL(d,\mathbb{R})$ and $\mathfrak{g}_\infty = \mathfrak{gl}(d,\mathbb{R})$. To compare the sizes of $v \in \mathfrak{g}_\infty$ and $\exp v \in G_\infty$ it is convenient to work with a submultiplicative norm. Let $||\cdot||_{op}$ be the operator norm on $\mathfrak{g}_\infty$ with respect to the norm $||\cdot||_\infty$ on $\mathbb{R}^d$. For any linear subspace $\mathfrak{w}$ of $\mathfrak{g}_\infty$ we define

$$\mathfrak{w}(r) = \{v \in \mathfrak{w} \mid ||v||_{op} < r\}.$$

The next lemma gives open subset of $\mathfrak{g}_\infty$ and G_∞ where exp restricts to a diffeomorphism.

Lemma A.2.2. *For any $d \ge 2$, the exponential map of G_∞ is a diffeomorphism between $\mathfrak{g}_\infty(\log 2)$ and an open subset of G_∞.*

Proof. The inverse of exp, that we'll denote by log, is defined by the power series

$$\log g = \sum_{i=1}^{\infty} \frac{(-1)^{n+1}}{n}(g - I_d)^n,$$

that converges when $||g - I_d||_{op} < 1$. If v is in $\mathfrak{g}_\infty(\log 2)$, then

$$||\exp(v) - I_d||_{op} < e^{\log 2} - 1 = 1,$$

so we are done. □

The next result is useful to estimate the volume of $G_\infty(r)$.

Lemma A.2.3. *Let $d \geq 3$. For any $r \in \left(0, \frac{2}{5d}\right]$ we have*

$$\exp \mathfrak{g}_\infty \left(\frac{9}{10} r\right) \subseteq G_\infty(r) \subseteq \exp \mathfrak{g}_\infty \left(\frac{5d}{3} r\right) \subseteq \exp \mathfrak{g}_\infty(\log 2).$$

To prove Lemma A.2.3 we use the next two simple inequalities. The first one is immediate.

Lemma A.2.4. *If $s \in \left[0, \frac{2}{5}\right]$, then*

$$\frac{s}{1-s} \leq \frac{5}{3} s.$$

Lemma A.2.5. *If $s \in \left[0, \frac{2}{15}\right]$, then*

$$\frac{9}{10} s \leq \log(1+s).$$

Proof. Since $\log(1+s)$ is concave, the statement follows from the inequalities for $s \in \{0, 2/15\}$. □

Proof of Lemma A.2.3. Take $r \in \left(0, \frac{2}{5d}\right]$ and $g = \exp v \in G_\infty(r)$. We have

$$||g - I_d||_{op} \leq d||g - I_d||_\infty \leq dr < 1,$$

so $\log g = \sum_{n \geq 1} \frac{(-1)^{n+1}}{n} (g - I_3)^n$ converges. Moreover

$$\begin{aligned} ||\log g||_{op} &\leq \sum_{n \geq 1} ||g - I_d||_{op}^n \\ &\leq \frac{dr}{1 - dr} \leq \frac{5d}{3} r. \end{aligned}$$

We used Lemma A.2.4 in the last line. This proves the inclusion

$$G_\infty(r) \subseteq \exp \mathfrak{g}_\infty \left(\frac{5d}{3} r\right).$$

Since $r \leq \frac{2}{5d} \leq \frac{2}{15}$, $\frac{5d}{3} r \leq \frac{2}{3} < \log 2 = 0.693\ldots$, so log is a diffeomorphism from $G_\infty(r)$ to an open subset of $\mathfrak{g}_\infty$—see Lemma A.2.2.

Now take $v \in \mathfrak{g}_\infty(9r/10)$ and set $g = \exp v$. Thanks to Lemma A.2.5 we have

$$||v||_{op} \leq \log(1 + r),$$

so

$$||g - I_d||_\infty \leq ||g - I_d||_{op} \leq e^{||v||_{op}} - 1 < r.$$

The same argument with $-v$ gives the same upper bound for $||g^{-1} - I_3||_\infty$. This proves the inclusion

$$\exp \mathfrak{g}_\infty \left(\frac{9}{10} r\right) \subseteq G_\infty(r).$$

□

Now we recall the well-known relation between the Haar measures of a Lie group and its Lie algebra near the identity. Let $\psi(z)$ be the power series $\frac{1-e^{-z}}{z}$.

Lemma A.2.6. *Let H_0 be a Lie subgroup of G_∞ Suppose that ν_{H_0} and $\nu_{\mathfrak{h}_0}$ are compatible Haar measures on H_0 and $\mathfrak{h}_0$. The map*

$$D_{H_0}(v) = \det \psi(ad_{\mathfrak{h}_0} v)$$

is a density of $\log_* \lambda_{H_0}$ with respect to $\lambda_{\mathfrak{h}_0}$ on $\mathfrak{h}_0(\log 2)$.

Proof. Since ν_{H_0} and $\nu_{\mathfrak{h}_0}$ are compatible, there are coordinates $(y_1, \dots, y_k)$ on $\mathfrak{h}_0$ with respect to a basis of $\mathfrak{h}_0$ such that ν_{H_0} and $\nu_{\mathfrak{h}_0}$ are respectively given by the integration with respect to ω and $dy_1 \wedge \cdots \wedge dy_k$, where ω is the left-invariant volume form on H_0 with $\omega_{I_d} = (dy_1 \wedge \cdots \wedge dy_k)_0$. We just have to prove that

$$(\exp^* \omega)_v = D_{H_0}(v)(dy_1 \wedge \cdots \wedge dy_k)_v.$$

The derivative of $\exp : \mathfrak{h}_0 \to H_0$ at v—see [God17, p. 99]—is given by

$$D \exp_v = L_h \circ \psi(\operatorname{ad}_{\mathfrak{h}_0} v),$$

where $L_h : H_0 \to H_0$ is the left multiplication by $h = \exp v$. Thus

$$\begin{aligned}(\exp^* \omega)_v &= \psi(\operatorname{ad}_{\mathfrak{h}_0} v)^* L_h^* \omega_h \\ &= \psi(\operatorname{ad}_{\mathfrak{h}_0} v)^* \omega_{I_d} \\ &= \det \psi(\operatorname{ad}_{\mathfrak{h}_0} v)(dy_1 \wedge \cdots \wedge dy_k)_0.\end{aligned}$$

□

The next lemma gives positive lower and upper bounds of D_{H_P} near 0. Let n_d be $\frac{d(d-2)}{2}$ if d is even and $\frac{(d-1)^2}{2}$ if d is odd.

Lemma A.2.7. *Let P be a non-degenerate quadratic form on $\mathbb{R}^d$. For any $v \in \mathfrak{h}_P(1/2)$ we have*

$$5^{-n_d} < D_{H_P}(v) < 2^{n_d}.$$

We state a less sharp version of Lemma A.2.7 that we'll use later.

Corollary A.2.8. *Let P be a non-degenerate quadratic form on $\mathbb{R}^d$. For any $v \in \mathfrak{h}_P(1/2)$ we have*

$$5^{-\frac{1}{2}d(d-1)} < D_{H_P}(v) < 2^{\frac{1}{2}d(d-1)}.$$

Proof. The inequality follows from Lemma A.2.7 since $n_d < \frac{d(d-1)}{2}$. □

We introduce the function $\mathtt{f}(r) = \frac{1}{r}(e^r - 1 - r)$. To prove Lemma A.2.7 we use the next inequality.

Lemma A.2.9. *For any $z \in \mathbb{C}$ with $|z|_\infty < r$ we have*

$$1 - \mathtt{f}(r) < |\psi(z)|_\infty < 1 + \mathtt{f}(r).$$

Proof. We have

$$|\psi(z)-1|_\infty = \left|\sum_{n=1}^{\infty}(-1)^n\frac{z^n}{(n+1)!}\right|_\infty \leq \sum_{n=1}^{\infty}\frac{|z|_\infty^n}{(n+1)!} = \mathtt{f}(|z|_\infty) < \mathtt{f}(r). \tag{A.2}$$

By the triangle inequality we have

$$1-|\psi(z)-1|_\infty \leq |\psi(z)|_\infty \leq 1+|\psi(z)-1|_\infty. \tag{A.3}$$

The inequality of the statement follows from (A.2) and (A.3). □

Proof of Lemma A.2.7. Note that $D_{H_P}(v) = \prod_\eta \psi(\eta)$, where η runs through all the eigenvalues—with multiplicity—of $ad_{\mathfrak{h}_P} v$. Since $\psi(0) = 0$, the $\eta = 0$ don't contribute to $D_{H_P}(v)$, so we'll neglect them. Each η is the sum of two eigenvalues of v. Let $||\cdot||_{op}$ be the operator norm on $\mathfrak{gl}(d,\mathbb{C})$ with respect to $||\cdot||_\infty$ on $\mathbb{C}^d$. Suppose that $v \in \mathfrak{h}_P(1/2)$ and let λ be an eigenvalue of v. Then

$$|\lambda|_\infty \leq ||v||_{op} < \frac{1}{2}.$$

It follows that $|\eta|_\infty < 1$ for any η, and

$$\frac{1}{5} < 0.281\ldots = -\mathtt{f}(1) \leq |\psi(\eta)|_\infty \leq 1+\mathtt{f}(1) = 1.718\ldots < 2 \tag{A.4}$$

by Lemma A.2.9. To obtain the inequality of the statement we multiply (A.4) for all $\eta \neq 0$. There are at most n_d of these[1].

□

The last thing we need to prove the estimate of $\lambda_{H_P}(H_P(r))$—Lemma A.2.1—is an approximation of the volume of $\mathfrak{h}_P(1)$.

Lemma A.2.10. *If $P(x) = a_1x_1^2 + \ldots + a_dx_d^2$ with each $a_i \in \{\pm 1\}$, then*

$$\left(\frac{2}{d}\right)^{\frac{d(d-1)}{2}} \leq \lambda_{\mathfrak{h}_P}(\mathfrak{h}_P(1)) \leq 2^{\frac{d(d-1)}{2}}.$$

Proof. We define

$$\mathfrak{B}_P(r) = \{v \in \mathfrak{h}_P \mid ||v||_\infty < r\}.$$

Let $v = \sum_{i<j} v_{ij}H_{ij} \in \mathfrak{h}_P$. Since $a_i = \pm 1$ for every i, we have $||v||_\infty = \max_{i<j}|v_{ij}|_\infty$. Then $\lambda_{\mathfrak{h}_P}(\mathfrak{B}_P(r)) = (2r)^{dim\mathfrak{h}_P}$ by our choice of $\lambda_{\mathfrak{h}_P}$.

Note that

$$\mathfrak{B}_P(1/d) \subseteq \mathfrak{h}_P(1) \subseteq \mathfrak{B}_P(1)$$

since $\frac{1}{d}||\cdot||_{op} \leq ||\cdot||_\infty \leq ||\cdot||_{op}$ on $\mathfrak{gl}(d,\mathbb{R})$. Comparing their volumes we obtain the inequality of the statement.

□

[1]Since v is antisymmetric with respect to a non-degenerate symmetric bilinear form, the eigenvalues of v come in pairs: $\pm\lambda_1,\ldots,\pm\lambda_{\frac{d}{2}}$ if d is even and $\pm\lambda_1,\ldots,\pm\lambda_{\frac{d-1}{2}},0$ if d is odd.

Proof of Lemma A.2.1. Since $r \leq \frac{2}{5d}$, then

$$\exp \mathfrak{h}_P \left(\frac{9}{10} r\right) \subseteq H_P(r) \subseteq \exp \mathfrak{h}_P \left(\frac{5dr}{3}\right) \subseteq \exp \mathfrak{h}_P(\log 2)$$

by Lemma A.2.3. Recall that

$$D_{H_P}(v) \leq 2^{\frac{d(d-1)}{2}}$$

by Corollary A.2.8 since $r \leq \frac{2}{5d} < \frac{1}{2}$. Thus

$$\begin{aligned}
\lambda_{H_P}(H_P(r)) &\leq \lambda_{H_P}\left(\exp \mathfrak{h}_P \left(\frac{5dr}{3}\right)\right) \\
&= \int_{\mathfrak{h}_P(5dr/3)} D_{H_P}(v) \mathrm{d}\lambda_{\mathfrak{h}_P}(v) \\
&< 2^{\frac{d(d-1)}{2}} \lambda_{\mathfrak{h}_P}(\mathfrak{h}_P(1)) \left(\frac{5dr}{3}\right)^{\frac{d(d-1)}{2}} \\
&\leq \left(\frac{20d}{3}\right)^{\frac{d(d-1)}{2}} r^{\frac{d(d-1)}{2}}.
\end{aligned}$$

We used Lemma A.2.10 to obtain the last line. A similar argument gives the lower bound:

$$\begin{aligned}
\lambda_{H_P}(H_P(r)) &> 5^{-\frac{d(d-1)}{2}} \lambda_{\mathfrak{h}_P}\left(\mathfrak{h}_P \left(\frac{9r}{10}\right)\right) \\
&\geq \left(\frac{1}{3d}\right)^{\frac{d(d-1)}{2}} r^{\frac{d(d-1)}{2}}.
\end{aligned}$$

□

A.2.2 p-adic orthogonal groups

Now we treat the p-adic case, where we'll prove a formula—Lemma A.2.11—for the volume of small balls in orthogonal groups, rather than a simple estimate as in the real case. If H_0 is a Lie subgroup of $G_{d,p} = GL(d, \mathbb{Q}_p)$, we define

$$H_0(r) = \{h \in H_0 \mid ||h - I_d||_p \leq r, ||h^{-1} - I_d||_p \leq r\}.$$

Let $P(x) = a_1 x_1^2 + \ldots + a_d x_d^2$ with $a_1, \ldots, a_d \in \mathbb{Q}_p^\times$ and let $H_P = O(P, \mathbb{Q}_p)$. We consider here also the Haar measures λ_H and $\lambda_\mathfrak{h}$ of H_P and $\mathfrak{h}_P$ induced by the basis $H_{ij} = E_{ij} - a_i a_j^{-1} E_{ji}$, $i < j$ of $\mathfrak{h}_P$. We define

$$\mathscr{D}_P = \prod_{i<j} \min\{1, |a_i a_j^{-1}|_p\}.$$

Here is our volume formula.

Lemma A.2.11. *Let p be a prime number and let P be a non-degenerate diagonal quadratic form on $\mathbb{Q}_p^d$. For any integer $n \geq 3$ we have*

$$\lambda_H(H_P(p^{-n})) = \mathscr{D}_P \cdot p^{-\frac{1}{2}d(d-1)n}.$$

Corollary A.2.12. *Let $d \geq 3$ and let H be the orthogonal group of a standard quadratic form on $\mathbb{Q}_p^d$. Then*

$$\lambda_H(H(p^{-n})) = p^{-\frac{1}{2}d(d-1)n}.$$

Proof. If $P(x) = a_1x_1^2 + \cdots a_dx_d^2$ is a standard quadratic form on $\mathbb{Q}_p^d$, then $|a_k|_p = 1$ for $k \leq d-2$ and $p^{-1} \leq |a_{d-1}|_p, |a_d|_p \leq 1$. It follows that $|a_ia_j^{-1}|_p \geq 1$ if $i < j$, so $\mathscr{D}_P = 1$. □

We'll compare again the measure of $H_P(p^{-n})$ with the measure of open balls in $\mathfrak{h}_P$. The strategy is the same as in the real case: we'll determine neighborhoods $\mathfrak{U}$ of 0 in $\mathfrak{h}_P$ and U of I_d in H_P where $\exp : \mathfrak{U} \to U$ is bijective, we'll establish the relation between $\log_* \lambda_H$ and $\lambda_\mathfrak{h}$ on $\mathfrak{U}$ and we'll compute the volume of $\mathfrak{U}$.

Let $\mathfrak{g}_p = \mathfrak{gl}(d, \mathbb{Q}_p) \simeq M_d(\mathbb{Q}_p)$ and let $||\cdot||_p$ be the norm on $\mathfrak{g}_p$ of the maximum of the p-adic absolute values of the entries. For any linear subspace $\mathfrak{w}$ of $\mathfrak{g}_p$ we define

$$\mathfrak{w}(r) = \{v \in \mathfrak{w} \mid ||v||_p \leq r\}.$$

Lemma A.2.13. *Let p be a prime number and $d \geq 2$. The exponential map is a bijection between $\mathfrak{g}_p(p^{-n})$ and $G_{d,p}(p^{-n})$ for any integer $n \geq 3$.*

One has to be careful because exp doesn't converge in all of $\mathbb{Q}_p$. We handle this with the next lemma.

Lemma A.2.14. *Consider $t \in \mathbb{Q}_p$. If $0 < |t|_p \leq p^{-3}$, then:*

(i) $\left|\frac{t^m}{m!}\right|_p < |t|_p$ *for any integer $m > 1$.*

(ii) $\frac{t^m}{m!} \to 0$ *as $m \to \infty$.*

Proof. Notice that $\frac{m}{p-1} < 3(m-1)$ for any integer $m \geq 2$ and any prime number p. Then

$$3(m-1) > \frac{m}{p-1} = \sum_{j\geq 1} \frac{m}{p^j} \geq \sum_{j\geq 1} \left\lfloor \frac{m}{p^j} \right\rfloor = -\log_p |m!|_p,$$

so

$$|m!|_p^{-1} < p^{3(m-1)} \leq |t|_p^{-(m-1)}.$$

It follows that $\left|\frac{t^m}{m!}\right|_p < |t|_p$.

Since

$$\left|\frac{t^m}{m!}\right|_p \leq p^{-\log_p |m!|_p} p^{-3m} \leq p^{\frac{m}{p-1}} p^{-3m} = p^{m\left(\frac{1}{p-1}-3\right)}, \tag{A.5}$$

and $\frac{1}{p-1} - 3 < 0$, the last term of (A.5), and hence also the first, tend to 0 as $m \to \infty$. □

Proof of Lemma A.2.13. Consider $n \geq 3$ and $v \in \mathfrak{g}_p$ with $||v||_p \leq p^{-n}$. By Lemma A.2.14 we have

$$\left|\left|\frac{v^m}{m!}\right|\right|_p \leq \frac{||v||_p^m}{|m!|_p} < ||v||_p$$

for any $m \geq 2$, so

$$\exp(v) - I_d = v + \sum_{m\geq 2} \frac{v^m}{m!}$$

converges and $||\exp(v) - I_d||_p = ||v||_p$. This shows that exp sends $\mathfrak{g}_p(p^{-n})$ to $G_{d,p}(p^{-n})$.

Now consider $g \in G_{d,p}(p^{-n})$. We have

$$\left|\left|\frac{(g-I_d)^m}{m}\right|\right|_p \leq \frac{||g-I_d||_p^m}{|m|_p} \leq \frac{||g-I_d||_p^m}{|m!|_p} < ||g-I_d||_p$$

for $m \geq 2$, so

$$\log g = (g - I_d) + \sum_{m\geq 2} \frac{(-1)^{m+1}}{m}(g-I_d)^m$$

converges and $||\log g||_p = ||g - I_d||_p$. Thus $\log = \exp^{-1}$ sends $G_{d,p}(p^{-n})$ to $\mathfrak{g}_p(p^{-n})$, which proves our claim. □

The relation of $\log_* \lambda_H$ and $\lambda_\mathfrak{h}$ on $\mathfrak{h}_P(p^{-3})$ is very simple.

Lemma A.2.15. *Consider a prime number p and $d \geq 2$. Let H be the orthogonal group of a non-degenerate diagonal quadratic form on $\mathbb{Q}_p^d$. Then $\log_* \lambda_H = \lambda_\mathfrak{h}$ on $\mathfrak{h}(p^{-3})$.*

To prove Lemma A.2.15 we'll use the explicit formula of the function relating the two measures, which is proved in the same way as in the real case. Recall that $\psi(z)$ is the power series $\frac{1}{z}(1 - e^{-z})$.

Lemma A.2.16. *Let H_0 be a Lie subgroup of $G_{d,p}$ with Lie algebra $\mathfrak{h}_0$. Consider compatible Haar measures ν_{H_0} and $\nu_{\mathfrak{h}_0}$ on H_0 and $\mathfrak{h}_0$. Then*

$$D_{H_0}(v) = |\det \psi(ad_{\mathfrak{h}_0} v)|_p$$

is a density of $\log_* \nu_{H_0}$ with respect to $\nu_{\mathfrak{h}_0}$ on $H_0(p^{-3})$.

Proof of Lemma A.2.15. Since λ_H and $\lambda_\mathfrak{h}$ are compatible, then

$$\frac{\mathrm{d}\log_* \lambda_H}{\mathrm{d}\lambda_\mathfrak{h}}(v) = |\det \psi(ad_\mathfrak{h} v)|_p$$

on $\mathfrak{h}(p^{-3})$ by Lemma A.2.16. Thus it suffices to prove that $|\psi(\eta)|_p = 1$ for any eigenvalue η of $ad_\mathfrak{h} v$ when $v \in \mathfrak{h}_P(p^{-3})$.

Let's fix $v \in \mathfrak{h}_P(p^{-3})$. Let K be a finite extension of $\mathbb{Q}_p$ that has the eigenvalues λ of v. The p-adic absolute value extends uniquely to an ultrametric absolute value on K that we denote also by $|\cdot|_p$—see [Kob84, Theorem 11, chapter III]. On K^d we consider the norm

$$||(y_1, \ldots, y_d)||_p = \max_i |y_i|_p.$$

Let $y \in K^d$ be an eigenvector of v corresponding to $\lambda \in K$ with $||y||_p = 1$. Then

$$|\lambda|_p = ||vy||_p \leq ||v||_p \leq p^{-3}.$$

An eigenvalue η of $ad_\mathfrak{h} v$ is the sum of two eigenvalues of v, hence $|\eta|_p \leq p^{-3}$. By Lemma A.2.14 $|1 - e^{-\eta}|_p = |\eta|_p$, so

$$|\psi(\eta)|_p = \left|\frac{1-e^{-\eta}}{\eta}\right|_p = 1.$$

□

Now we compute the volume of $\mathfrak{h}_P(1)$.

Lemma A.2.17. *Let $P(x)$ be a non-degenerate diagonal quadratic form on $\mathbb{Q}_p^d$. Then*

$$\lambda_{\mathfrak{h}}(\mathfrak{h}_P(1)) = \mathscr{D}_P.$$

Proof. We write $P(x) = a_1x_1^2 + \cdots + a_dx_d^2$. Recall that the matrices $H_{ij} = E_{ij} - a_ia_j^{-1}E_{ji}$, $i < j$ form a basis of $\mathfrak{h}_P$. Take $v = \sum_{i<j} v_{ij}H_{ij} \in \mathfrak{h}_P$. Consider the norm

$$||v||' = \max_{i<j} |v_{ij}|_p$$

and let

$$\mathfrak{B}' = \{v \in \mathfrak{h}_P \mid ||v||' \leq 1\}.$$

Then $\lambda_{\mathfrak{h}}(\mathfrak{B}') = 1$ by our choice of Haar measure on $\mathfrak{h}_P$. The entries of v are v_{ij} and $a_ia_j^{-1}v_{ij}$ with $i < j$, in particular $||v||' \leq ||v||_p$. The ball $\mathfrak{h}_P(1)$ is an open subgroup of $\mathfrak{B}'$, hence

$$[\mathfrak{B}' : \mathfrak{h}_P(1)]\lambda_{\mathfrak{h}}(\mathfrak{h}_P(1)) = 1.$$

Notice that v is respectively in $\mathfrak{B}'$ and $\mathfrak{h}_P(1)$ if and only if $|v_{ij}|_p \leq 1$ and $|v_{ij}|_p \leq \min\{1, |a_ia_j^{-1}|_p\}$ for every $i < j$. Hence

$$\frac{1}{[\mathfrak{B}' : \mathfrak{h}_P(1)]} = \prod_{i<j} \min\{1, |a_ia_j^{-1}|_p\} = \mathscr{D}_P.$$

□

We are ready to compute the volume of $H_P(p^{-n})$.

Proof of Lemma A.2.11. Let $n \geq 3$. Then $\exp \mathfrak{h}_P(p^{-n}) = H_P(p^{-n})$ by Lemma A.2.13. By Lemma A.2.15 we know that $\log_* \lambda_H = \lambda_{\mathfrak{h}}$ on $\mathfrak{h}_P(p^{-3})$, so

$$\lambda_H(H_P(p^{-n})) = \lambda_{\mathfrak{h}}(\mathfrak{h}_P(p^{-n})) = \lambda_{\mathfrak{h}}(\mathfrak{h}_P(1))p^{-n\dim H_P} = \mathscr{D}_P \cdot p^{-\frac{1}{2}d(d-1)n}.$$

□

A.2.3 Bump functions in real orthogonal groups

Let $P(x) = a_1x_1^d + \cdots + a_dx_d^2$ with $a_i \in \{\pm 1\}$ and let $H = O(P, \mathbb{R})$. In this section we construct, for every small enough neighborhood $\mathcal{U}$ of I_d in H, a smooth bump function $\psi_{\mathcal{U}}$ on H supported at $\mathcal{U}$. We'll give explicit upper bounds of the L^2-norms of $\psi_{\mathcal{U}}$ and its first order derivatives in terms of the size of $\mathcal{U}$. We'll use the notation and conventions for the Haar measures introduced in Subsection A.2.1.

Here is our main statement. We define $\mathcal{M}_d = 10^{d^2}d^{\frac{1}{4}(d+2)^2}$.

Lemma A.2.18. *Consider $d \geq 3$. Let $P(x) = a_1x_1^2 + \cdots + a_dx_d^2$ with each $a_i \in \{\pm 1\}$ and $H = O(P, \mathbb{R})$. For any $r \in \left(0, \frac{2}{5d}\right]$ there is a smooth function $\psi_r : H \to [0, \infty)$ with support in $H(r)$ such that $||\psi_r||_{L^1} = 1$,*

$$||\psi_r||_{L^2} < \mathcal{M}_d r^{-\frac{1}{4}d(d-1)},$$

and for any $v \in \mathfrak{h}$

$$||v(\psi_r)||_{L^2} \leq \mathcal{M}_d ||v||_\infty r^{-(\frac{1}{4}d(d-1)+1)}.$$

The maps ψ_r will be obtained by precomposing with the logarithm map suitable smooth functions in $\mathfrak{h}$. As usual, we'll break the proof of Lemma A.2.18 into small auxiliary results—four in this case.

In first lemma we forget about the orthogonal group, and work in an euclidean space. The proof is straightforward, so we'll omit it. Let m be a positive integer. We denote

$$\mathbb{B}^m(r) = \{x \in \mathbb{R}^m \mid ||x||_\infty < r\}.$$

If F' is a map $\mathbb{R}^m \to \mathbb{R}$, we define

$$F'_{[r]}(x) = r^{-m} F'(r^{-1}x).$$

We endow the space of linear maps $\mathbb{R}^m \to \mathbb{R}$ with the operator norm with respect to the norms $||\cdot||_\infty$ on $\mathbb{R}^m$ and $\mathbb{R}$.

Lemma A.2.19. *Let $F' : \mathbb{R}^m \to [0, \infty)$ be a $\mathcal{C}^1$ function with support in $\mathbb{B}^m(1)$ and let $r > 0$.*

(a) *The map $F'_{[r]}$ has support in $\mathbb{B}^m(r)$.*

(b) $||F'_{[r]}||_{L^1} = ||F'||_{L^1}$.

(c) $||F'_{[r]}||_{L^2} = r^{-\frac{m}{2}} ||F'||_{L^2}$.

(d) *Suppose that $r \leq 1$. Let V be a vector field on $\mathbb{B}_m(1)$. Then*

$$||V(F'_{[r]})||_{L^2} \leq 2^{\frac{m}{2}} M_{F'} M_V r^{-(\frac{m}{2}+1)},$$

where

$$M_{F'} = \sup_{x \in \mathbb{B}^m(1)} ||D_x F'||_{op} \text{ and } M_V = \sup_{x \in \mathbb{B}^m(1)} ||V_x||_\infty.$$

Let $P(x)$ and $H = O(P, \mathbb{R})$ be as in Lemma A.2.18. We give now the basic building block to construct the ψ_r's: a smooth bump function supported on the unit ball of $\mathfrak{h}$. Recall that any $y \in \mathfrak{h}$ is of the form

$$y = \sum_{i<j} y_{ij} H_{ij},$$

where $H_{ij} = E_{ij} - a_i a_j^{-1} E_{ji}$. We define $F : \mathfrak{h} \to [0, 1]$ as

$$F(y) = \prod_{i<j} \mathfrak{b}(y_{ij}),$$

where $\mathfrak{b} : \mathbb{R} \to [0, 1]$ is a smooth function with support in $[-1, 1]$, $\int_{-1}^{1} \mathfrak{b}(t)\mathrm{d}t = 1$ and $|\mathfrak{b}'(t)|_\infty \leq 2$ for any $t \in \mathbb{R}$. We consider once more

$$\mathfrak{B}(r) = \{y \in \mathfrak{h} \mid ||y||_\infty < r\}.$$

The map F is smooth and has support in $\mathfrak{B}(1)$. Let's estimate M_F—see Lemma A.2.19.

Lemma A.2.20. *For any $y \in \mathfrak{h}$ we have $||D_y F||_{op} < d^2$.*

Proof. We have

$$\left|\frac{\partial F}{\partial y_{i_0,j_0}}\right|_\infty = \left|\frac{b'(y_{i_0,j_0})}{b(y_{i_0,j_0})}\prod_{i<j} b(y_{ij})\right|_\infty \leq 2,$$

hence

$$|(D_yF)v|_\infty = \left|\sum_{i<j}\frac{\partial F}{\partial y_{ij}}v_{ij}\right|_\infty \leq \sum_{i<j} 2||v||_\infty = d(d-1)||v||_\infty.$$

The conclusion follows from this inequality. □

Recall that $||\cdot||_{op}$ is the operator norm on $\mathfrak{gl}(d,\mathbb{R})$ with respect to $||\cdot||_\infty$ on $\mathbb{R}^d$ and that

$$\mathfrak{h}(r) = \{v \in \mathfrak{h} \mid ||v||_{op} < r\}.$$

For $v \in \mathfrak{h}$ we denote by $\widetilde{v}$ the vector field $y \mapsto \frac{Id - e^{-ad\, y}}{ad\, y}(v)$ on $\mathfrak{h}$. This is simply, near 0, the left-invariant vector field determined by v in exponential coordinates. Let's estimate $M_{\widetilde{v}}$.

Lemma A.2.21. *If $v \in \mathfrak{h}$ and $y \in \mathfrak{h}(1)$, then*

$$||\widetilde{v}_y||_\infty \leq 5d||v||_\infty.$$

Proof. Recall that $||\cdot||_{op}$ is the operator norm on $\mathfrak{h}$ with respect to $||\cdot||_\infty$ on $\mathbb{R}^d$. We denote also by $||\cdot||_{op}$ the operator norm on $\mathfrak{gl}(\mathfrak{h})$ with respect to $||\cdot||_{op}$ on $\mathfrak{h}$. Notice that

$$||ad\, y(y')||_{op} = ||yy' - y'y||_{op} \leq 2||y||_{op}||y'||_{op},$$

so $||ad\, y||_{op} \leq 2||y||_{op}$. We conclude as follows:

$$\begin{aligned}||\widetilde{v}_y||_\infty \leq ||\widetilde{v}_y||_{op} &\leq \left|\left|Id - \frac{ad\, y}{2!} + \frac{(ad\, y)^2}{3!} - \cdots\right|\right|_{op} ||v||_{op} \\ &\leq \left(1 + \frac{1}{2}(e^{||ad\, y||_{op}} - 1)\right)||v||_{op} \\ &\leq \frac{1}{2}(e^2+1)d||v||_\infty \leq 5d||v||_\infty.\end{aligned}$$

□

For $r \in \left(0, \frac{2}{5d}\right]$ we define $\psi'_r : H \to [0,\infty)$ as

$$\psi'_r(h) = F_{[r_1]}(\log h)\mathbb{1}_{H(r)}(h),$$

where $r_1 = \frac{9}{10d}r$. This function verifies almost all the properties we want in Lemma A.2.18. Let $\mathcal{M}_{d,1} = 5d^3(20d)^{\frac{1}{4}d(d-1)+1}$.

Lemma A.2.22. *For any $r \in \left(0, \frac{2}{5d}\right]$ the map $\psi'_r : H \to [0,\infty)$ is smooth, has support in $H(r)$ and:*

(i) $5^{-\frac{1}{2}d(d-1)} \leq ||\psi'_r||_{L^1(H)} \leq 2^{\frac{1}{2}d(d-1)}$,

(*ii*) $||\psi_r'||_{L^2(H)} \leq \mathcal{M}_{d,1} r^{-\frac{1}{4}d(d-1)}$,

(*iii*) $||v(\psi_r')||_{L^2(H)} \leq \mathcal{M}_{d,1}||v||_\infty r^{-(\frac{1}{4}d(d-1)+1)}$ *for any* $v \in \mathfrak{h}$.

Proof. Since $r \in \left(0, \frac{2}{5d}\right]$, $\exp : \mathfrak{h}\left(\frac{9r}{10}\right) \to H(r)$ is injective by Lemma A.2.2. Note that $\mathfrak{B}(r_1) \subseteq \mathfrak{h}\left(\frac{9r}{10}\right)$ since $||v||_{op} \leq d||v||_\infty$. The map $F_{[r_1]} : \mathfrak{h} \to [0,\infty)$ is smooth and has support in $\mathfrak{B}(r_1)$, so ψ_r' is smooth and has support in $\exp \mathfrak{B}(r_1)$, which is contained in $H(r)$.

In the computations that follow we'll use the properties of $F_{[r_1]}$ in Lemma A.2.19. By Lemma A.2.6 we have

$$\int_H \psi_r'(h)\mathrm{d}\lambda_H(h) = \int_{\mathfrak{B}(r_1)} F_{[r_1]}(v)D_P(v)\mathrm{d}\lambda_{\mathfrak{h}}(v),$$

so (i) results from the fact that $5^{-\frac{1}{2}d(d-1)} < D_P < 2^{\frac{1}{2}d(d-1)}$ on $\mathfrak{h}(1/2)$—see Corollary A.2.8. Now note that

$$\begin{aligned}||\psi_r'||_{L^2(H)} &= \left(\int_{\mathfrak{B}(r_1)} F_{[r_1]}^2(v)D_P(v)\mathrm{d}\lambda_{\mathfrak{h}}(v)\right)^{\frac{1}{2}} \\ &\leq 2^{\frac{1}{4}d(d-1)}||F_{[r_1]}||_{L^2(\mathfrak{h})} \\ &= (2r_1^{-1})^{\frac{1}{4}d(d-1)}||F||_{L^2(\mathfrak{h})}.\end{aligned}$$

We have $||F||_{L^2(\mathfrak{h})} = ||\mathfrak{b}||_{L^2(\mathbb{R})}^{dim\mathfrak{h}} \leq 1$ since $\mathfrak{b}^2 \leq \mathfrak{b}$ and $||\mathfrak{b}||_{L^1(\mathbb{R})} = 1$. Thus

$$||\psi_r'||_{L^2(H)} \leq (2r_1^{-1})^{\frac{1}{4}d(d-1)} = \left(\frac{20d}{9}\right)^{\frac{1}{4}d(d-1)} r^{-\frac{1}{4}d(d-1)} < \mathcal{M}_{d,1} r^{-\frac{1}{4}d(d-1)},$$

so (ii) is established. For $v \in \mathfrak{h}$ we have

$$\begin{aligned}||v(\psi_r')||_{L^2(H)} &\leq 2^{\frac{1}{4}d(d-1)}||\widetilde{v}(F_{[r_1]})||_{L^2(\mathfrak{h})} \\ &\leq 2^{\frac{1}{4}d(d-1)}\left(2^{\frac{1}{4}d(d-1)}M_F M_{\widetilde{v}} \cdot r_1^{-(\frac{1}{4}d(d-1)+1)}\right) \\ &= 2^{\frac{1}{2}d(d-1)}\left(\frac{10d}{9}\right)^{\frac{1}{4}d(d-1)} M_F M_{\widetilde{v}} \cdot r^{-(\frac{1}{4}d(d-1)+1)}.\end{aligned}$$

Recall that $M_F < d^2$ and $M_{\widetilde{v}} \leq 5d||v||_\infty$ by lemmas A.2.20 and A.2.21, so

$$||v(\psi_r')||_{L^2(H)} < \mathcal{M}_{d,1} r^{-(\frac{1}{4}d(d-1)+1)}.$$

□

To prove Lemma A.2.18 we just have to normalize ψ_r'.

Proof of Lemma A.2.18. Consider $r \in \left(0, \frac{2}{5d}\right]$ and $\psi_r' : H \to [0,\infty)$ as in Lemma A.2.22. We set $I_r = ||\psi_r'||_{L^1(H)}^{-1}$ and $\psi_r = I_r\psi_r'$. Then $||\psi_r||_{L^1(H)} = 1$. By Lemma A.2.22 we have $I_r \leq 5^{\frac{1}{2}d(d-1)}$, thus

$$||\psi_r||_{L^2(H)} \leq 5^{\frac{1}{2}d(d-1)}\mathcal{M}_{d,1} r^{-\frac{1}{4}d(d-1)} < \mathcal{M}_d r^{-\frac{1}{4}d(d-1)},$$

and for any $v \in \mathfrak{h}$

$$||v(\psi_r)||_{L^2(H)} \leq 5^{\frac{1}{2}d(d-1)}\mathcal{M}_{d,1}||v||_\infty r^{-(\frac{1}{4}d(d-1)+1)} \leq \mathcal{M}_d||v||_\infty r^{-(\frac{1}{4}d(d-1)+1)}.$$

□

A.3 Triangular groups

Let H_S be the orthogonal group of a diagonal quadratic form on $\mathbb{Q}_S^d$. To prove the transversal recurrence of closed H_S-orbits in $X^1_{d,S}$—Lemma 8.1.3—in Section 8.4, we thickened any such orbit using a subgroup $W_{d,S} = \prod_{\nu\in S} W_{d,\nu}$ of lower-triangular matrices in $GL(d, \mathbb{Q}_S)$. Here we prove the volume estimates for the open subsets $W_{d,\nu}(r)$ of $W_{d,\nu}$ that we introduced: Lemma A.3.1 for $\nu = \infty$ and Lemma A.3.4 for $\nu = p$.

A.3.1 Real triangular groups

The objective of this subsection is to prove Lemma A.3.1. The strategy we follow is the same as for Lemma A.2.1 above.

Let $W_{d,\infty}$ be the group of lower-triangular matrices in $GL(d, \mathbb{R})$ with positive entries in the main diagonal. The Haar measure of $W_{d,\infty}$ determined by the basis

$$\beta_{d,W} = (F_1, \dots, F_{d-1}, E_{21}, E_{32}, \dots, E_{d,d-1}, E_{3,1}, \dots, E_{d,d-2}, \dots, E_{d1})$$

of its Lie algebra $\mathfrak{w}_{d,\infty}$ will be denoted by λ_{W_∞}. Recall that $F_k = E_{kk} - E_{dd}$ for $1 \le k < d$.

The exponential map is a bijection between $\mathfrak{w}_{d,\infty}$ and $W_{d,\infty}$. For any $r > 0$ we define

$$\mathfrak{w}_{d,\infty}(r) = \{v \in \mathfrak{w}_{d,\infty} \mid ||v||_{op} < r\}$$

and

$$W_{d,\infty}(r) = \exp(\mathfrak{w}_{d,\infty}(r)).$$

We introduce $c_d = \frac{d(d+1)}{2} - 1$.

Lemma A.3.1. *For any $0 < r < \frac{1}{2}$ we have*

$$V_d^- r^{c_d} < \lambda_{W_\infty}(W_{d,\infty}(r)) < V_d^+ r^{c_d},$$

where $V_d^- = \frac{2^{d-1}}{d^{2c_d}}$ and $V_d^+ = 2^{d^2-1}$.

To prove Lemma A.3.1 we'll use the next two auxiliary results.

Lemma A.3.2. *Let $v = \sum_{j<i} v_{ij}E_{ij} \in \mathfrak{w}_{d,\infty}$. The eigenvalues of $ad\, v : \mathfrak{w}_{d,\infty} \to \mathfrak{w}_{d,\infty}$ are 0 with multiplicity $d-1$ and $\eta_{ij} = v_{ii} - v_{jj}$ for $1 \le j < i \le d$.*

Proof. Consider

$$\mathfrak{a} = \bigoplus_{k=1}^{d-1} \mathbb{R}F_i \quad \text{and} \quad \mathfrak{n} = \bigoplus_{i>j} \mathbb{R}E_{ij}.$$

Notice that $\mathfrak{w}_{d,\infty} = \mathfrak{a} \oplus \mathfrak{n}$. Write $v = v_1 + v_2$ with $v_1 \in \mathfrak{a}$ and $v_2 \in \mathfrak{n}$. The matrices of $ad\, v_1$ and $ad\, v_2$ in the basis $\beta_{d,W}$ are diagonal and strictly lower-diagonal. Hence the eigenvalues of $ad\, v$ are the diagonal entries of $ad\, v_1$. Since $[v_1, F_k] = 0$ for $1 \le k \le d-1$, 0 is an eigenvalue with multiplicity (at least) $d-1$. For $i > j$ we have $[v_1, E_{ij}] = (v_{ii} - v_{jj})E_{ij}$, which gives the eigenvalues η_{ij}. □

Lemma A.3.3. *We have*

$$\left(\frac{2}{d^2}\right)^{c_d} \leq \lambda_{\mathfrak{w}_{d,\infty}}(\mathfrak{w}_{d,\infty}(1)) \leq 2^{c_d}.$$

Proof. For

$$v = \sum_{k=1}^{d-1} v_{kk}F_k + \sum_{i>j} v_{ij}E_{ij} = \begin{pmatrix} v_{11} & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ v_{d-1,1} & \cdots & v_{d-1,d-1} & 0 \\ v_{d1} & \cdots & v_{d,d-1} & -(v_{11}+\cdots+v_{d-1,d-1}) \end{pmatrix} \in \mathfrak{w}_{d,\infty}$$

we define

$$||v||' = \max_{i\geq j} |v_{ij}|_\infty$$

and

$$\mathfrak{B}'(r) = \{v \in \mathfrak{w}_{d,\infty} \mid ||v||' < r\},$$

so $\lambda_{\mathfrak{w}_\infty}(\mathfrak{B}'(1)) = 2^{c_d}$ by our choice of $\lambda_{\mathfrak{w}_\infty}$. Notice that

$$||\cdot||' \leq ||\cdot||_\infty \leq ||\cdot||_{op} \leq d||\cdot||_\infty \leq d^2||\cdot||',$$

so

$$\mathfrak{B}'\left(\frac{1}{d^2}\right) \subseteq \mathfrak{w}_{d,\infty}(1) \subseteq \mathfrak{B}'(1).$$

The comparison of the volumes of these balls gives the inequality of the statement. □

We are ready to estimate the volume of $W_{d,\infty}(r)$.

Proof of Lemma A.3.1. We consider again the analytic map $\psi(z) = \frac{1}{z}(1-e^{-z})$. The exponential map is a bijection $\mathfrak{w}_{d,\infty} \to W_{d,\infty}$ and, like in the proof of Lemma A.2.6, the positive function

$$D(v) = \det \psi(\operatorname{ad} v)$$

is a density of $log_*\lambda_{W_\infty}$ with respect to $\lambda_{\mathfrak{w}_\infty}$.

Consider $v = \sum_{i\geq j} v_{ij}E_{ij} \in \mathfrak{w}_{d,\infty}$ with $||v||_{op} < \frac{1}{2}$. Aside from the 0 with multiplicity $d-1$[2], the eigenvalues of $\operatorname{ad} v$ are $\eta_{ij} = v_{ii} - v_{jj}$ for $1 \leq j < i \leq d$ according to Lemma A.3.2, so

$$D(v) = \prod_{i>j} \psi(\eta_{ij}).$$

For $i > j$ we have

$$|\eta_{ij}|_\infty = |v_{ii} - v_{jj}|_\infty \leq 2||v||_\infty \leq 2||v||_{op} < 1.$$

Since ψ[3] is decreasing on $\mathbb{R}$, we have

$$\frac{1}{2} < 0.632\ldots = \psi(1) < \psi(\eta_{ij}) < \psi(-1) = 1.718\ldots < 2,$$

[2]They don't contribute to the density since $\psi(0) = 1$.

[3]From the identity $z^2e^z\psi'(z) = z + 1 - e^z$ we readily see that $\psi' < 0$ on $\mathbb{R}^\times$

hence

$$2^{-\frac{d(d-1)}{2}} \leq D(v) \leq 2^{\frac{d(d-1)}{2}}.$$

For any $0 < r \leq \frac{1}{2}$ we have

$$\begin{aligned}\lambda_{W_\infty}(W_{d,\infty}(r)) &= \int_{\mathfrak{w}_{d,\infty}(r)} D(v)\mathrm{d}\lambda_{\mathfrak{w}_\infty}(v) \\ &< 2^{\frac{d(d-1)}{2}} \lambda_{\mathfrak{w}_\infty}(\mathfrak{w}_{d,\infty}(1)) r^{c_d} \\ &< 2^{d^2-1} r^{c_d}.\end{aligned}$$

We used Lemma A.3.3 to get the last line. In the same fashion we obtain

$$\lambda_{W_\infty}(W_{d,\infty}(r)) > 2^{-\frac{d(d-1)}{2}} \left(\frac{2}{d^2}\right)^{c_d} r^{c_d} = \frac{2^{d-1}}{d^{2c_d}} r^{c_d}.$$

□

A.3.2 p-adic triangular groups

Here we work with the group $W_{d,p}$ of lower-triangular matrices in $GL(d, \mathbb{Q}_p)$. The main result is Lemma A.3.4.

We endow $W_{d,p}$ with the Haar measure λ_{W_p} determined by the basis

$$(E_{11}, \ldots, E_{dd}, E_{21}, E_{32}, \ldots, E_{d,d-1}, \ldots, E_{d1})$$

of its Lie algebra $\mathfrak{w}_{d,p}$. We'll compute the measure of small compact-open subgroups of $W_{d,p}$ of the following form: For $r > 0$, set

$$W_{d,p}(r) = \{w \in W_{d,p} \mid ||w - I_d||_p \leq r, ||w^{-1} - I_d||_p \leq r\}.$$

We consider also the orthogonal group H_p of a non-degenerate diagonal quadratic form $P(x) = a_1 x_1^2 + \cdots + a_d x_d^2$ on $\mathbb{Q}_p^d$.

Lemma A.3.4. *Let p be a prime number. We set $\ell_p = 1$ if p is odd and $\ell_p = 2$ if $p = 2$. The multiplication map $W_{d,p}(p^{\ell_p}) \times H_p \to G_{d,p}$ is injective, $W_{d,p}(p^{-\ell_p})H_p$ is open in $G_{d,p}$ and*

$$\lambda_{W_p}(W_{d,p}(p^{-n})) = p^{-(c_d+1)n}$$

for any $n \geq 3$.

To compute the volume of $W_{d,p}(p^{-n})$ we use the next two lemmas. The proof of the first one is the same as in Lemma A.3.2.

Lemma A.3.5. *Let $\mathfrak{w}_{d,p} = Lie(W_{d,p})$. Consider $v = (v_{ij})_{1 \leq i,j \leq d} \in \mathfrak{w}_{d,p}$. The eigenvalues of $ad\, v : \mathfrak{w}_{d,p} \to \mathfrak{w}_{d,p}$ are $\eta_{ij} = v_{ii} - v_{jj}$ for $1 \leq j < i \leq d$ and 0 with multiplicity d.*

We use once more the analytic function $\psi(\theta) = \frac{1}{\theta}(1 - e^{-\theta})$.

Lemma A.3.6. *Let p be a prime number. Then $\psi(\theta)$ converges for any $\theta \in p^3\mathbb{Z}_p$ and $|\psi(\theta)|_p = 1$.*

Proof. Notice that

$$\psi(\theta) = \sum_{j=0}^{\infty} \frac{(-1)^j}{(j+1)!}\theta^j.$$

We have

$$\left|\frac{(-1)^j}{(j+1)!}\theta^j\right|_p < \left|\frac{\theta^{j+1}}{(j+1)!}\right|_p,$$

and the right-hand side term tends to 0 as $j \to \infty$ by (ii) of Lemma A.2.14, so $\psi(\theta)$ converges. We also have

$$\left|\frac{(-1)^j}{(j+1)!}\theta^j\right|_p < 1$$

for any $j \leq 1$ by (i) of Lemma A.2.14, thus $|\psi(\theta)|_p = 1$. □

We are ready to prove the main result of this subsection.

Proof of Lemma A.3.4. The matrices in $W_{d,p} \cap H_p$ are of the form $diag(\pm 1, \ldots, \pm 1)$, so $W_{d,p}(p^{-\ell_p}) \cap H_p = 1$. This implies that $W_{d,p}(p^{-\ell_p}) \times H_p \to G_{d,p}$ is injective.

The exponential map is a bijection between

$$\mathfrak{w}_{d,p}(p^{-n}) = \{v \in \mathfrak{w}_{d,p} \mid ||v||_p \leq p^{-n}\}$$

and $W_{d,p}(p^{-n})$ for any $n \geq 3$ by Lemma A.2.13, and the map

$$D(v) = |\det \psi(\operatorname{ad} v)|_p$$

is a density of $\log_* \lambda_{W_p}$ with respect to $\lambda_{\mathfrak{w}_p}$ on $\mathfrak{w}_{d,p}(p^{-n})$. If

$$v = \sum_{1 \leq j \leq i \leq d} v_{ij} E_{ij}$$

then

$$D(v) = \left|\prod_{j \leq i} \psi(v_{ii} - v_{jj})\right|_p.$$

by Lemma A.3.5. When $||v||_p \leq p^{-3}$, $D(v) = 1$ by Lemma A.3.6. Hence

$$\lambda_{W_p}(W_{d,p}(p^{-n})) = \lambda_{\mathfrak{w}_p}(\mathfrak{w}_{d,p}(p^{-n})) = p^{-(c_d+1)n}$$

for $n \geq 3$. □

A.4 The volume of $X^1_{d,S}$

Here we prove a formula—Lemma A.4.1—for the volume of the space $X^1_{d,S}$ of covolume 1 lattices of $\mathbb{Q}_S^d$. From it we deduce the bound in Corollary A.4.2, which was used in Section 8.4.

As in that section, we identify $X^1_{d,S}$ with $G'_{d,S}/\Gamma'_{d,S}$. Recall that $G'_{d,S} = \prod_{\nu \in S} G'_{d,\nu}$,

$$G'_{d,\nu} = \{g \in GL(d, \mathbb{Q}_\nu) \mid |\det g|_\nu = 1\},$$

and $\Gamma'_{d,S} = G'_{d,S} \cap \Gamma_{d,S}$. We work with the $G'_{d,S}$-invariant measure $\beta_{d,S}$ on $X^1_{d,S}$ induced by the Haar measure of $G'_{d,S}$ fixed in 8.4.1. We denote the volume of $X^1_{d,S}$ by $\mathcal{V}_{d,S}$.

Lemma A.4.1. *For any finite set of primes $S = \{\infty\} \cup S_f$ we have*

$$\mathcal{V}_{d,S} = \mathcal{V}_{d,\infty} \prod_{p \in S_f} \prod_{j=1}^{d} \left(1 - \frac{1}{p^j}\right).$$

We record an immediate consequence of Lemma A.4.1.

Corollary A.4.2. *For any finite set $S = \{\infty\} \cup S_f$ of primes and any integer $d \geq 2$ we have $\mathcal{V}_{d,S} \leq \mathcal{V}_{d,\infty}$.*

We'll deduce Lemma A.4.1 from the next lemma. Let Γ be a lattice in a locally compact group G. A measurable subset U of G is a *fundamental domain* of Γ in G if any $g \in G$ can be written as $u\gamma$ with $u \in U$ and $\gamma \in \Gamma$ in a unique way.

Lemma A.4.3. *Let $S = \{\infty\} \cup S_f$ be a finite set of primes. Consider a fundamental domain $U_{d,\infty}$ for $\Gamma_{d,\infty}$ in $SL^{\pm}(d, \mathbb{R})$. Then*

$$U_{d,S} = U_{d,\infty} \times \prod_{p \in S_f} GL(d, \mathbb{Z}_p)$$

is a fundamental domain of $\Gamma'_{d,S}$ in $G'_{d,S}$.

Proof. First we'll show that the group

$$G''_{d,S} = SL^{\pm}(d, \mathbb{R}) \times \prod_{p \in S_f} GL(d, \mathbb{Z}_p)$$

acts transitively on $X^1_{d,S}$. Any lattice Δ of $\mathbb{Q}_S^d$ of covolume 1 is of the form $g'\mathbb{Z}_S^d$ for some $g' \in G'_{d,S}$. Suppose that $S_f = \{p_1, \ldots, p_k\}$. Since

$$GL(d, \mathbb{Q}_p) = GL(d, \mathbb{Z}_p) GL(d, \mathbb{Z}[1/p])$$

for any prime p[4], we write $g'_{p_1} = k_{p_1}\gamma_{p_1}$ with $k_{p_1} \in GL(d, \mathbb{Z}_{p_1})$ and $\gamma_{p_1} \in GL(d, \mathbb{Z}[1/p_1])$. Note that $\det \gamma_{p_1} = \det(k_{p_1}^{-1} g'_{p_1}) \in \mathbb{Z}_p^{\times}$, so γ_{p_1} is in $SL^{\pm}(d, \mathbb{Z}[1/p_1])$. Then $\Delta = g^{\bullet}\mathbb{Z}_S^d$, where $g^{\bullet} = g'\widetilde{\gamma_{p_1}}^{-1}$ and $\widetilde{\gamma_{p_1}} = (\gamma_{p_1}, \ldots, \gamma_{p_1}) \in \Gamma'_{d,S}$. Remark that $g^{\bullet}$ is still in $G'_{d,S}$ and $g'_{p_1} \in GL(d, \mathbb{Z}_{p_1})$. Moreover, if g'_i already was in $GL(d, \mathbb{Z}_{p_i})$ for some $i > 1$, the same is true for $g^{\bullet}_{p_i}$ since $\gamma_{p_1} \in GL(d, \mathbb{Z}_{p_i})$. Hence, continuing this process with $p_2, \ldots, p_k$ express Δ as $g''\mathbb{Z}_S^d$ for some $g'' \in G''_{d,S}$.

We identify $X^1_{d,S}$ with $G''_{d,S}/\Gamma''_{d,S}$, where $\Gamma''_{d,S} = G''_{d,S} \cap \Gamma'_{d,S}$—this is the diagonal copy of $\Gamma_{d,\infty} = GL(d, \mathbb{Z})$ in $G''_{d,S}$. We'll see that $U_{d,S}$ is a fundamental domain of $\Gamma''_{d,S}$ in $G''_{d,S}$, which is equivalent to our statement. Since $SL^{\pm}(d, \mathbb{R}) = U_{d,\infty}\Gamma_{d,\infty}$, then $G''_{d,S} = U_{d,S}\Gamma''_{d,S}$. Consider now $u, v \in U_{d,S}$, $\gamma_1, \gamma_2 \in \Gamma_{d,\infty}$ and $\widetilde{\gamma_i} = (\gamma_i, \ldots, \gamma_i) \in \Gamma''_{d,S}$. If $u\widetilde{\gamma_1} = v\widetilde{\gamma_2}$, comparing the real coordinates we see that $\gamma_1 = \gamma_2$, so $u = v$. □

[4]Since $\mathbb{Z}[1/p]$ and $SL(d, \mathbb{Z}[1/p])$ are dense in $\mathbb{Q}_p$ and $SL(d, \mathbb{Q}_p)$, respectively.

Proof of Lemma A.4.1. Consider a fundamental domain $U_{d,\infty}$ of $\Gamma_{d,\infty}$ in $SL^{\pm}(d,\mathbb{R})$ and

$$U_{d,S} = U_{d,\infty} \times \prod_{p \in S_f} GL(d,\mathbb{Z}_p).$$

By Lemma A.4.3,

$$\mathcal{V}_{d,S} = \lambda_{G_{d,S}}(U_{d,S}) = \mathcal{V}_{d,\infty} \times \prod_{p \in S_f} \lambda_{G_{d,p}}(GL(d,\mathbb{Z}_p)),$$

so the result follows from Lemma A.4.4 □

A.4.1 The volume of $GL(d,\mathbb{Z}_p)$

Lemma A.4.4. *For any prime p and any integer $d \geq 2$ we have*

$$\lambda_{G_{d,p}}(GL(d,\mathbb{Z}_p)) = \prod_{j=1}^{d} \left(1 - \frac{1}{p^j}\right).$$

The proof of Lemma A.4.4 is based on three intermediate lemmas. The first one is a formula for the volume of $G_{d,p}(p^{-n})$ for $n \geq 3$. We omit the proof of the first one, since its very similar to Lemma A.2.15.

Lemma A.4.5. *Let p be a prime and consider $n \geq 3$. Then*

$$\lambda_{G_{d,p}} G_{d,p}(p^{-n}) = p^{-d^2 n}$$

To determine the volume of $GL(d,\mathbb{Z}_p) = G_{d,p}(1)$ we just need to compute the index of $G_{d,p}(p^{-n})$ in $G_{p,d}(1)$, which is the cardinality of $GL(d,\mathbb{Z}/p^n\mathbb{Z})$. We need a definition. Consider positive integers d and N. A complete flag of $(\mathbb{Z}/N\mathbb{Z})^d$ is a sequence

$$0 = A_0 \subseteq A_1 \subseteq \ldots \subseteq A_d = (\mathbb{Z}/N\mathbb{Z})^d,$$

where A_i is a free $\mathbb{Z}/N\mathbb{Z}$-submodule of $(\mathbb{Z}/N\mathbb{Z})^d$ of rank i. We denote by $F_N(d)$ the number of complete flags of $(\mathbb{Z}/N\mathbb{Z})^d$. In the following lemma, $\varphi(N) = \#(\mathbb{Z}/N\mathbb{Z})^\times$ is Euler's phi function.

Lemma A.4.6. *For any prime p and any integers $n, d > 0$ we have*

$$F_{p^n}(d) = \frac{p^{\frac{1}{2}d(d+1)n}}{\varphi(p^n)^d} \prod_{j=1}^{d} (1 - p^{-j}).$$

Proof. We'll prove the result by induction on d. The base case $d = 1$ is immediate.

Suppose that the formula holds for $d-1$. The number of flags of $M_d = (\mathbb{Z}/p^n\mathbb{Z})^d$ having A_1 equal to a fixed line ℓ of M_d is $F_{p^n}(d-1)$ since M_d/ℓ is a free $(\mathbb{Z}/p^n\mathbb{Z})$-module of rank $d-1$. Thus

$$F_{p^n}(d) = \#\{\text{lines in } M_d\} \cdot F_{p^n}(d-1).$$

An element $(a_1, \ldots, a_d)$ of M_d generates a line if some a_i is invertible in $\mathbb{Z}/p^n\mathbb{Z}$. There are $p^{dn} - p^{d(n-1)}$ such elements, thus

$$\#\{\text{lines in } M_d\} = \frac{p^{dn}}{\varphi(p^n)}(1 - p^{-d}),$$

since each line has $\varphi(p^n)$ generators. This proves the formula for $F_{p^n}(d)$. □

Lemma A.4.7. *For any prime p and any $d \geq 2$ we have*

$$\#GL(d, \mathbb{Z}/p^n\mathbb{Z}) = p^{d^2 n} \prod_{j=1}^{d} \left(1 - \frac{1}{p^j}\right).$$

Proof. The group $GL(d, \mathbb{Z}/p^n\mathbb{Z})$ acts transitively on the set of complete flags of $M_d = (\mathbb{Z}/p^n\mathbb{Z})^d$. The stabilizer of

$$0 \subseteq \langle e_1 \rangle \subseteq \ldots \subseteq \langle e_1, \ldots, e_{d-1} \rangle \subseteq M_d,$$

where $e_1, \ldots, e_d$ is the standard basis of M_d, is the subgroup of upper-triangular matrices in $GL(d, \mathbb{Z}/p^n\mathbb{Z})$, whose cardinality is[5] $\varphi(p^n)^d p^{\frac{d(d-1)}{2}n}$. Then

$$\#GL(d, \mathbb{Z}/p^n\mathbb{Z}) = \varphi(p^n)^d p^{\frac{d(d-1)}{2}n} F_{p^n}(d),$$

and the formula follows from Lemma A.4.6. □

Now we can compute the volume of $GL(d, \mathbb{Z}_p)$.

Proof of Lemma A.4.4. Consider an integer $n \geq 3$. We have

$$\begin{aligned} \lambda_{G_{d,p}}(GL(d, \mathbb{Z}_p)) &= [G_{d,p}(1) : G_{d,p}(p^{-n})]\, \lambda_{G_{d,p}}(G_{d,p}(p^{-n})) \\ &= \#GL(d, \mathbb{Z}/p^n\mathbb{Z})\, \lambda_{G_{d,p}}(G_{d,p}(p^{-n})), \end{aligned}$$

so the formula is obtained from Lemma A.4.7 and Lemma A.4.5. □

[5] The entries in the main diagonal are in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ and the entries above the main diagonal can be chosen freely in $\mathbb{Z}/p^n\mathbb{Z}$.

Appendix B

Effective Reduction Theory

As we mentioned in Chapter 2, C. Hermite and H. Minkowski developed (probably motivated by the $\mathbb{Z}$-classification problem) a reduction theory for real and integral quadratic forms building on the work of C.F. Gauss for binary quadratic forms. In this appendix we prove quantitative versions with explicit constants of some of its classical results. The main one is the bound of the norm of a reduced integral quadratic form in Proposition B.3.1, which played an important role in the proofs of Lemma 9.4.1 and Lemma 9.4.2 in Chapter 9.

There are three sections: We reintroduce the Siegel sets of $GL(d,\mathbb{R})$ and we recall when a real quadratic form R is reduced in terms of these in Section B.1. The base of the reduction theory over $\mathbb{R}$ is the case R definite positive, treated in Section B.2, where we discuss the concept—introduced by Minkowski—of successive minima of R with respect to a lattice of $\mathbb{R}^d$. We close with the proof of Proposition B.3.1 in Section B.3. The proofs we give are based on the exposition of reduction theory in the book of Cassels [Cas78, Chapter 12].

B.1 Basic definitions

We denote the group $GL(d,\mathbb{R})$ by $G_{d,\infty}$. Consider the following subgroups of $G_{d,\infty}$:

$$\begin{aligned} K &= O(d,\mathbb{R}) \\ A &= \{diag(a_1,\cdots,a_d) \in G_{d,\infty} \mid a_i > 0 \text{ for } 1 \leq i \leq d\}, \\ N &= \{\text{unipotent, upper-triangular matrices in } G_{d,\infty}\}. \end{aligned}$$

For $\alpha,\beta > 0$ we define

$$\begin{aligned} A_\alpha &= \{diag(a_1,\cdots,a_d) \in A \mid a_i \leq \alpha a_{i+1} \text{ for } 1 \leq i \leq d-1\}, \\ N_\beta &= \{n \in N \mid ||n - I_d||_\infty \leq \beta\}. \end{aligned}$$

The (α,β)-Siegel set of $G_{d,\infty}$ is defined as

$$\mathscr{S}_{d,\infty}^{\alpha,\beta} = KA_\alpha N_\beta.$$

Recall that $\mathscr{S}_{d,\infty}^{\alpha,\beta}$ is a fundamental set of $\Gamma_{d,\infty} = GL(d,\mathbb{Z})$ in $G_{d,\infty}$ if $\alpha \geq \frac{2}{\sqrt{3}}$ and $\beta \geq \frac{1}{2}$—see Proposition 9.3.1.

Let $Q_{p,q}$ be the quadratic form $x_1^2 + \cdots + x_q^2 - x_{q+1}^2 - \cdots - x_{p+q}^2$ and set $d = p + q$. We'll say that a quadratic form R on $\mathbb{R}^d$ is (α, β)-*reduced* if $R = Q_{p,q} \circ s$ for some $s \in \mathscr{S}_{d,\infty}^{\alpha,\beta}$, where p, q is the signature of R.

B.2 Positive definite quadratic forms

The purpose of this section is to prove an upper bound of the norm of an integral matrix that takes a positive definite reduced quadratic form to another.

Proposition B.2.1. *For $i \in \{1, 2\}$, let R_i be an (α_i, β_i)-reduced positive definite quadratic form on $\mathbb{R}^d$, where $\alpha_i, \beta_i \geq 1$. If b is an integral $d \times d$ matrix such that $R_1 \circ b = R_2$, then*

$$||b||_\infty \leq W_d \alpha_1^{d-1} \alpha_2^{(d-1)^2} \beta_1^d \beta_2^{d(d-1)} |\det b|_\infty^{2d},$$

where $W_d = d^{\frac{3d}{2}} (d!)^{d+1} (d+1)^{d^2}$.

Here is the main idea to prove Proposition B.2.1: A positive definite quadratic form R on $\mathbb{R}^d$ determines a basis $v_1, \ldots, v_d \in \mathbb{Z}^d$ of $\mathbb{R}^d$ as follows: v_1 is the R-shortest vector of $\mathbb{Z}^d$, v_{j+1} is the R-shortest vector in $\mathbb{Z}^d - (\mathbb{R}v_1 \oplus \cdots \oplus \mathbb{R}v_j)$. In Lemma B.2.7 we'll see that the ∞-norms of $v_1, \cdots, v_d$ are bounded in terms of α and β when R is (α, β)-reduced. A similar thing is true if we replace $\mathbb{Z}^d$ by any lattice $\Delta \subseteq \mathbb{Z}^d$ of $\mathbb{R}^d$—see Lemma B.2.3. Thanks to this we'll show that, if R_1, R_2 and b are as in Proposition B.2.1, $b\tau_2 = b\tau_1$ for some non-singular $\tau_i \in M_d(\mathbb{Z})$ with norm bounded in terms of α_i and β_i, from where the bound for b is easily obtained.

This section has three parts. In B.2.1 we introduce extremal vectors of a lattice Δ of $\mathbb{R}^d$ with respect to a positive definite quadratic form R, and we prove in Lemma B.2.3 a bound for these when R is reduced and $\Delta \subseteq \mathbb{Z}^d$. Then, in B.2.2 we define the succesive R-minima of Δ and we show in Lemma B.2.7 that if they are attained by a basis $v_1, \ldots, v_d \in \Delta$, the $v_i's$ are R-extremal, hence the bound of Lemma B.2.3 applies when R is reduced. The proof of Proposition B.2.1 is completed in B.2.3.

B.2.1 Extremal vectors in lattices

Consider a positive definite quadratic form R on $\mathbb{R}^d$ and a lattice Δ of $\mathbb{R}^d$. For $r > 0$ we define $E_r^-(\Delta, R)$ and $E_r^\circ(\Delta, r)$ as the respective linear spans of the $v \in \Delta$ with $R(v) \leq r, R(v) < r$. A vector $v \in \Delta$ is said to be R-*extremal* if v does not belong to $E_{R(v)}^\circ(\Delta, R)$. When R is (α, β)-reduced, the norm of an R-extremal vector is bounded in terms of α and β.

Lemma B.2.2. *Let R be a positive definite, (α, β)-reduced quadratic form on $\mathbb{R}^d$, where $\alpha, \beta \geq 1$. Any R-extremal vector v of $\mathbb{Z}^d$ verifies*

$$||v||_\infty \leq \sqrt{d} \cdot d! \alpha^{d-1} \beta^d.$$

Proof. Consider $a = diag(a_1, \cdots, a_d) \in A_\alpha$ and $n = (n_{ij}) \in N_\beta$ such that $R = Q_{d,0} \circ (an)$. We set

$$w = nv = (w_1, \cdots, w_d).$$

First we bound $|w_k|_\infty$ for $1 \leq k \leq d$. Consider two cases:

- **Case I: there is $j \leq k$ such that $R(v) \leq R(e_j)$.** Then

$$a_k^2 w_k^2 \leq R(v) \leq R(e_j),$$

which implies that

$$\begin{aligned} w_k^2 &\leq \frac{a_1^2}{a_k^2} n_{1j}^2 + \cdots + \frac{a_{j-1}^2}{a_k^2} n_{j-1,j}^2 + \frac{a_j^2}{a_k^2} \\ &\leq (\alpha^{2(k-1)} + \cdots + \alpha^{2(k-j)})\beta^2 \\ &\leq d\alpha^{2(d-1)}\beta^2. \end{aligned}$$

Thus $|w_k|_\infty \leq \sqrt{d}\,\alpha^{d-1}\beta$.

- **Case II: $R(e_j) < R(v)$ for every $j \leq k$.** Then, since v is an R-extremal vector of $\mathbb{Z}^d$, $R(v) \leq R(v')$ for every v' of the form $v + c_1 e_1 + \cdots + c_k e_k$ with $c_1, \cdots, c_k \in \mathbb{Z}$. Set $w' = nv'$, and choose $c_k, c_{k-1}, \cdots, c_1$ so that $|w'_j| \leq \frac{1}{2}$ for every $j \leq k$. Since $w_i = w'_i$ for $k < i \leq d$, from $R(v) \leq R(v')$ we deduce that

$$\begin{aligned} w_k^2 &\leq \frac{a_1^2}{a_k^2}(w'_1)^2 + \cdots + \frac{a_k^2}{a_k^2}(w'_k)^2 \\ &\leq \frac{1}{4}(\alpha^{2(k-1)} + \cdots + \alpha^2 + 1) \\ &\leq \frac{d}{4}\alpha^{2(d-1)} < d\alpha^{2(d-1)}\beta^2, \end{aligned}$$

so $|w_k|_\infty < \sqrt{d}\alpha^{d-1}\beta$.

Combining both cases we get

$$||w||_\infty \leq \sqrt{d}\alpha^{d-1}\beta.$$

Now it's easy to control the norm of v:

$$\begin{aligned} ||v||_\infty = ||n^{-1}w||_\infty &\leq d||n^{-1}||_\infty ||w||_\infty \\ &\leq d((d-1)!||n||_\infty^{d-1})(\sqrt{d}\alpha^{d-1}\beta) \\ &\leq \sqrt{d} \cdot d!\alpha^{d-1}\beta^d. \end{aligned}$$

This completes the proof. □

We need a slight generalization of Lemma B.2.2.

Lemma B.2.3. *Let R be a positive definite, (α, β)-reduced quadratic form on $\mathbb{R}^d$, where $\alpha, \beta \geq 1$, and let $\Delta \subset \mathbb{Z}^d$ be a lattice of $\mathbb{R}^d$. Any R-extremal vector w of Δ verifies*

$$||w||_\infty \leq W_{1,d}\alpha^{d-1}\beta^d[\mathbb{Z}^d : \Delta]^{2d},$$

where $W_{1,d} = d^{\frac{3}{2}} \cdot d!(d+1)^d$.

To prove Lemma B.2.3 we'll use three easy intermediate results. The first one can be proved easily by induction on ℓ.

Lemma B.2.4. *Let $x_1, \cdots, x_\ell$ be positive integers such that $x_1 \cdots x_\ell = m$. Then*

$$x_1 + \cdots + x_\ell \leq m + \ell - 1,$$

and the equality holds if and only if $x_j = m$ for some j and $x_i = 1$ for $i \neq j$.

For the second result we need a definition: We say that a $d \times d$ matrix b with real coefficients *has big diagonal* if $b_{ii} \geq |b_{ij}|$ for any $1 \leq i, j \leq d$.

Lemma B.2.5. *Let c be a non-singular $d \times d$ matrix with integral coefficients. There is $\gamma \in \Gamma_{d,\infty}$ such that $c\gamma$ is an upper-triangular matrix with big diagonal.*

Proof. Using repeatedly the euclidean algorithm, we transform c into an upper-triangular matrix with big diagonal performing elementary column operations[1], which correspond to multiplying c on the right by some $\gamma \in \Gamma_{d,\infty}$.

□

Lemma B.2.6. *Consider an upper-triangular matrix $b \in M_d(\mathbb{Z})$ with big diagonal. Let $\delta = |\det b|_\infty$ and take $\alpha > 0$ and $\beta \geq 1$. Then $\mathscr{S}_{d,\infty}^{\alpha,\beta} b$ is contained in $\mathscr{S}_{d,\infty}^{\alpha\delta,\beta(\delta+d)}$.*

Proof. Take $a \in A_\alpha$ and $n \in N_\beta$. It suffices to prove that $anb = a'n'$ for some $a' \in A_{\alpha\delta}$ and $n' \in N_{\beta(\delta+d)}$. We set $c = diag(b_{11}, \cdots, b_{dd})$. Then

$$a' = ac = diag(a_{11}b_{11}, \cdots, a_{dd}b_{dd}),$$

and

$$\frac{a_{i+1,i+1}b_{i+1,i+1}}{a_{ii}b_{ii}} \leq \alpha b_{i+1,i+1} \leq \alpha\delta,$$

hence a' is in $A_{\alpha\delta}$. Now, $n' = c^{-1}nb$ so for $i < j$ we have

$$\begin{aligned} |n'_{ij}|_\infty = \frac{1}{b_{ii}} \left| \sum_{k=1}^{j} n_{ik}b_{kj} \right|_\infty &\leq \beta \sum_{k=1}^{j} |b_{kj}|_\infty \\ &\leq \beta \sum_{k=1}^{j} b_{kk} < \beta(\delta + d). \end{aligned}$$

We used Lemma B.2.4 in the last step. This shows that n' is in $N_{\beta(\delta+d)}$. □

We are ready to prove that R-extremal vectors in Δ are small if R is (α, β)-reduced.

Proof of Lemma B.2.3. By Lemma B.2.5, we can write Δ as $b\mathbb{Z}^d$ for some upper-triangular matrix with a big diagonal $b \in M_d(\mathbb{Z})$. Then $[\mathbb{Z}^d : \Delta] = |\det b|_\infty$, which we denote by δ.

[1] These are permuting columns or adding to a column an integral multiple of another.

Consider an R-extremal vector $w = bv$ of Δ. Then v is an $(R \circ b)$-extremal vector of $\mathbb{Z}^d$. The positive definite quadratic form $R \circ b$ is $(\alpha\delta, \beta(\delta + d))$-reduced by Lemma B.2.6, so

$$\begin{aligned} ||v||_\infty &\leq \sqrt{d} \cdot d!(\alpha\delta)^{d-1}(\beta(\delta + d))^d \\ &\leq \sqrt{d} \cdot d!(d+1)^d \alpha^{d-1}\beta^d\delta^{2d-1} \end{aligned}$$

by Lemma B.2.2, and hence

$$\begin{aligned} ||w||_\infty &\leq d||b||_\infty||v||_\infty \\ &\leq d^{\frac{3}{2}} \cdot d!(d+1)^d \alpha^{d-1}\beta^d\delta^{2d}. \end{aligned}$$

□

B.2.2 Succesive minima of lattices

Consider a positive definite quadratic form R on $\mathbb{R}^d$ and a lattice Δ of $\mathbb{R}^d$. The dimensions of $E_r^-(\Delta, R)$ and $E_r^\circ(\Delta, R)$ will be respectively denoted by $d_r^-(\Delta, R)$ and $d_r^\circ(\Delta, R)$. Let i be an integer between 1 and d. The i-th R-minima of Δ is defined as

$$\mathscr{M}_i(\Delta, R) = \inf\{r > 0 \mid d_r^-(\Delta, R) \geq i\}.$$

We say that the vectors $v_1, \cdots, v_d \in \Delta$ realize the R-minima of Δ if

$$R(v_i) = \mathscr{M}_i(\Delta, R),$$

for every $1 \leq i \leq d$. In the proof of Proposition B.2.1 we'll use the next lemma.

Lemma B.2.7. *Let $v_1, \cdots, v_d$ be linearly independent vectors in Δ realizing the R-minima of Δ. Then each v_i is an R-extremal vector of Δ.*

Remark B.2.8. *There are always linearly independent $v_1, \ldots, v_d \in \Delta$ realizing the R-minima of Δ: we choose an R-shortest non-zero $v_1 \in \Delta$. If we already have $v_1, \ldots, v_j$, we choose an R-shortest v_{j+1} in $\Delta - (\mathbb{R}v_1 \oplus \cdots \oplus \mathbb{R}v_j)$. It's possible to do this since any subset of Δ is closed.*

Let's prepare for the proof of Lemma B.2.7. For R and Δ fixed, the subspaces $E_r^-(\Delta, R)$ form a (not necessarily complete) flag of $\mathbb{R}^d$

$$\{0\} = E_0 \subsetneq \cdots \subsetneq E_\ell = \mathbb{R}^d.$$

Let $\mathbf{d}_i$ be the dimension of E_i for $0 \leq i \leq \ell$ and let $\mathbf{r}_i$ be the smallest non-negative real number such that

$$E_i = E_{\mathbf{r}_i}^-(\Delta, R).$$

To lighten the notation we write $\mathscr{M}_j$ instead of $\mathscr{M}_j(\Delta, R)$ in the next lemma.

Lemma B.2.9. *Let $1 \leq j \leq d$ and $k \geq 0$ be integers such that $\boldsymbol{d}_k < j \leq \boldsymbol{d}_{k+1}$. Then $E_{\mathscr{M}_j}^\circ(\Delta, R) = E_k$.*

Proof. From the definition of $\mathscr{M}_j$ follows that $d^\circ_{\mathscr{M}_j}(\Delta, R) < j$. But $d^\circ_{\mathscr{M}_j}(\Delta, R)$ is one of the $\mathbf{d}_i'$s, hence its value cannot exceed $\mathbf{d}_k$. This means that $E^\circ_{\mathscr{M}_j}(\Delta, R)$ is contained in E_k. Now, $E_k = E^-_{\mathbf{r}_k}(\Delta, R)$ has dimension $\mathbf{d}_k < j$, hence $\mathbf{r}_k < \mathscr{M}_j$. This implies that E_k is contained in $E^\circ_{\mathscr{M}_j}(\Delta, R)$. □

Proof of Lemma B.2.7. Consider any integer $1 \leq j \leq d$ and choose $k \geq 0$ such that

$$\mathbf{d}_k < j \leq \mathbf{d}_{k+1}.$$

Then $E^\circ_{\mathscr{M}_j}(\Delta, R) = E_k$ by Lemma B.2.9. Since $E_k = E^-_{\mathbf{r}_k}(\Delta, R)$ has dimension $\mathbf{d}_k$, then $\mathbf{r}_k \geq \mathscr{M}_{\mathbf{d}_k} = R(v_{\mathbf{d}_k})$. It follows that $v_1, \cdots, v_{\mathbf{d}_k}$ belong to E_k. Since $v_1, \ldots, v_d$ are linearly independent, $(v_1, \cdots, v_{\mathbf{d}_k})$ is a basis of E_k and thus v_j is not in $E_k = E^\circ_{R(v_j)}(\Delta, R)$. In other words, v_j is an R-extremal vector of Δ. □

Corollary B.2.10. *Let R be a positive definite, (α, β)-reduced quadratic form on $\mathbb{R}^d$, where $\alpha, \beta \geq 1$. Consider linearly independent vectors $v_1, \cdots, v_d$ in a lattice $\Delta \subset \mathbb{Z}^d$ realizing the R-minima of Δ. Then*

$$||v_i||_\infty \leq W_{1,d}\alpha^{d-1}\beta^d[\mathbb{Z}^d : \Delta]^{2d},$$

for every $1 \leq i \leq d$, where $W_{1,d} = d^{\frac{3}{2}} \cdot d!(d+1)^d$.

Proof. Lemma B.2.7 tells us that each v_i is an R-extremal vector of Δ, hence the desired bound is given by Lemma B.2.3. □

B.2.3 The main proof

Proof of Proposition B.2.1. Consider linearly independent vectors $v_1, \cdots, v_d \in \mathbb{Z}^d$ realizing the R_2-minima of $\mathbb{Z}^d$, and let $\tau_2 = (v_1, \cdots, v_d) \in M_d(\mathbb{Z})$. By Corollary B.2.10 we know that

$$||\tau_2||_\infty \leq W_{1,d}\alpha_2^{d-1}\beta_2^d.$$

Let Δ be the lattice $b\mathbb{Z}^d$ of $\mathbb{R}^d$ and set $w_i = bv_i$. Since $R_1 \circ b = R_2$, the linearly independent vectors $w_1, \cdots, w_d$ realize the R_1-minima of Δ. Let τ_1 be the $d \times d$ integral matrix $(w_1, \cdots, w_d)$. Using Corollary B.2.10 once more we get

$$||\tau_1||_\infty \leq W_{1,d}\alpha_1^{d-1}\beta_1^d|\det b|_\infty^{2d}.$$

Note that $b\tau_2 = \tau_1$, so

$$\begin{aligned} ||b||_\infty = ||\tau_1\tau_2^{-1}||_\infty &\leq d||\tau_1||_\infty||\tau_2^{-1}||_\infty \\ &\leq d!(W_{1,d}\alpha_1^{d-1}\beta_1^d|\det b|_\infty^{2d})(W_{1,d}\alpha_2^{d-1}\beta_2^d)^{d-1} \\ &= (d^{\frac{3d}{2}}(d!)^{d+1}(d+1)^{d^2})\alpha_1^{d-1}\alpha_2^{(d-1)^2}\beta_1^d\beta_2^{d(d-1)}|\det b|_\infty^{2d}. \end{aligned}$$

This concludes the proof. □

We conclude with a reformulation of Proposition B.2.1 in terms of right translates of Siegel sets by integral matrices.

Corollary B.2.11. *Let b be a $d \times d$ integral matrix. If $\mathscr{S}^{2,1}_{d,\infty} b$ meets $\mathscr{S}^{2,1}_{d,\infty}$, then*

$$||b||_\infty \leq W_{3,d} |\det b|^{2d}_\infty,$$

where $W_{3,d} = 2^{d(d-1)} d^{\frac{3d}{2}} (d!)^{d+1} (d+1)^{d^2}$.

Proof. Take $s_1, s_2 \in \mathscr{S}^{2,1}_{d,\infty}$ such that $s_1 b = s_2$. The positive definite quadratic form $R_i = Q_{d,0} \circ s_i$ is $(2,1)$ reduced and b takes R_1 to R_2, so Proposition B.2.1 implies

$$\begin{aligned} ||b||_\infty &\leq W_d 2^{(d-1)^2+d-1} |\det b|^{2d}_\infty \\ &= 2^{d(d-1)} d^{\frac{3d}{2}} (d!)^{d+1} (d+1)^{d^2} |\det b|^{2d}_\infty. \end{aligned}$$

□

B.3 Reduced integral quadratic forms

The goal of this section is to establish the bound in Proposition B.3.1 of the norm of an (α, β)-reduced integral quadratic form Q on $\mathbb{R}^d$—we are not assuming Q positive definite—in terms of α, β and δ_Q[2]. It is a slight improvement of [Cas78, Lemma 12.3, p. 325] and [LM16, Corollary 3, p. 902]. From it we recover in Corollary B.3.3 the main finiteness lemma of the reduction theory of integral quadratic forms—see [Bor69, Lemme 5.7, p. 38].

Proposition B.3.1. *Let Q be an integral, (α, β)-reduced quadratic form on $\mathbb{R}^d$ for some $\alpha, \beta \geq 1$. Then*

$$||Q||_\infty \leq W_{2,d} \alpha^{d^2} \beta^{2d^2} |\delta_Q|^{2d}_\infty,$$

where $W_{2,d} = d^{\frac{d}{2}} (d+1)^{d^2} (d!)^{2d+1}$.

The proof of Proposition B.3.1 is based on Proposition B.2.1 and the next lemma. We denote by $J = (J_{ij})$ the $d \times d$ matrix with entries $J_{ij} = \delta_{i+j,d+1}$.

Lemma B.3.2. *Consider real numbers $\alpha > 0$ and $\beta \geq 1$. If s belongs to the Siegel set $\mathscr{S}^{\alpha,\beta}_{d,\infty}$, then ${}^t s^{-1} J$ is in $\mathscr{S}^{\alpha,(d-1)!\beta^{d-1}}_{d,\infty}$.*

Proof. Write $s = kan$ with $k \in K, a = diag(a_1, \cdots, a_d) \in A_\alpha$, and $n \in N_\beta$. Then ${}^t s^{-1} J = (kJ)(Ja^{-1}J)(J\,{}^t n^{-1} J)$. Note that kJ is in K,

$$Ja^{-1}J = diag(a_d^{-1}, \cdots, a_1^{-1})$$

is in A_α, and $J\,{}^t n^{-1} J$ is in $N_{(d-1)!\beta}$ because it is unipotent, upper triangular and

$$||J\,{}^t n^{-1} J||_\infty = ||n^{-1}||_\infty \leq (d-1)! ||n||^{d-1}_\infty \leq (d-1)! \beta^{d-1}.$$

□

[2]Recall that b_Q is the matrix of Q in the canonical basis of $\mathbb{R}^d$, and that $||b_Q||_\infty$ and $\det b_Q$ are denoted by $||Q||_\infty$ and δ_Q, respectively.

Proof of Proposition B.3.1. Consider $s_2 \in \mathscr{S}_{d,\infty}^{\alpha,\beta}$ such that $Q = Q_{p,q} \circ s_2$ and define

$$s_1 = I_{p,q}\, {}^t s_2^{-1} J,$$

where $I_{p,q}$ is the matrix of $Q_{p,q}$ in the canonical basis of $\mathbb{R}^d$. Notice that s_1 is in $\mathscr{S}_{d,\infty}^{\alpha,(d-1)!\beta^{d-1}}$ by Lemma B.3.2. Then, the positive definite quadratic forms $R_1 = Q_{d,0} \circ s_1$ and $R_2 = Q_{d,0} \circ s_2$ are respectively $(\alpha, (d-1)!\beta^{d-1})$ and (α, β)-reduced. One easily checks that $s_2 = s_1 J b_Q$, hence $R_1 \circ (J b_Q) = R_2$. Proposition B.2.1 gives

$$\begin{aligned} ||Q||_\infty = ||Jb_Q||_\infty &\leq W_d \alpha^{d-1} \alpha^{(d-1)^2} ((d-1)!\beta^{(d-1)})^d \beta^{d(d-1)} |\det Jb_Q|_\infty^{2d} \\ &\leq d^{\frac{3d}{2}} (d!)^{d+1} ((d-1)!)^d (d+1)^{d^2} \alpha^{d^2} \beta^{2d^2} |\delta_Q|_\infty^{2d}. \end{aligned}$$

□

Now we easily obtain the next classical result.

Corollary B.3.3. *Let m be a non-zero integer. There are finitely many $\mathbb{Z}$-equivalence classes of integral quadratic forms Q in d variables with $\delta_Q = m$.*

Proof. Any such class has a $\left(\frac{2}{\sqrt{3}}, \frac{1}{2}\right)$-reduced representative Q by Proposition 9.3.1, and there are finitely many $\left(\frac{2}{\sqrt{3}}, \frac{1}{2}\right)$-reduced integral quadratic forms on $\mathbb{R}^d$ by Proposition B.3.1. □

Appendix C

Constants

C.1 Chapter 4

- $\mathcal{D}_1$ (not explicit)—Corollary 4.3.2

C.2 Chapter 5

- $\mathcal{C}_{i,d} = d^{3d^2(d-1)+13d+1} \cdot d!^{2d^2+1} C_d (C_d^{(2)})^6$—Theorem 5.1.1
- $\mathcal{C}_{a,d} = (d!)^7 d^{2d^2(d-1)} F_d (C_d^{(2)})^4$—Theorem 5.1.2

C.3 Chapter 6

- $C_d = 12 \cdot 2^{3d^2(d-1)} \mathcal{D}^6 \mathcal{N}_d^{12} d^2$—Proposition 6.0.1
- $\mathcal{D} = 5\sqrt{\mathcal{D}_1}$—Proposition 6.2.1
- $\mathcal{N}_d = 3(3d^2 \cdot d!)^{\frac{1}{4}d(d-1)+1} \mathcal{M}_d$—Lemma 6.3.3

C.4 Chapter 7

- $F_d = (10\mathcal{F}_d)^4 \cdot 2^{d^2(d-1)}$—Proposition 7.0.1
- $\mathcal{F}_d = \mathtt{R}_d{}^{-1}(3d^2 \cdot d!)^{\frac{1}{2}d(d-1)}$—proof of Proposition 7.0.1

C.5 Chapter 8

- $C_d^{(2)} = (3^{2d^4} d^{6d^3+1})^{c_d} \mathcal{V}_{d,\infty}$—Proposition 8.0.1
- $\mathcal{E}_d = 2^{d^3} \cdot 3^{2d^4} d^{3d^3}$—Section 8.1
- $A_d = \left(\frac{4}{d(d-1)}\right)^{c_d} \mathcal{V}_{d,\infty}$—Lemma 8.1.3

- $C_d^{(4)} = \frac{2^3 \mathcal{V}_{d,\infty}{}^{\frac{1}{c_d}}}{d(d-1)}$—Lemma 8.1.3
- $\varepsilon_{\infty,d} = \frac{1}{2} \cdot \left(\frac{1}{2 \cdot 3^{2d} d^3 2^{d+2}}\right)^{(d-1)^2}$—Subsection 8.3.2
- $\varepsilon_{p,d} = \frac{1}{2} \cdot \left(\frac{1}{2 \cdot 3^{2d} d^3 p^{2d+1}}\right)^{(d-1)^2}$—Subsection 8.3.2
- $\varepsilon_{d,S} = \min_{\nu \in S} \varepsilon_{d,\nu}$—Subsection 8.3.2
- $C_{\infty,d} = 3^{2d} d^3 2^{d+2}$—Proposition 8.3.10
- $C_{p,d} = 3^{2d} d^3 p^{2d+1}$—Proposition 8.3.10
- $\vartheta_d = \frac{1}{(d-1)^2}$—Proposition 8.3.10
- $B_d = \frac{2\mathcal{V}_{d,\infty}{}^{\frac{1}{c_d}}}{d(d-1)}$—Lemma 8.4.7

C.6 Chapter 9

- $\mathcal{K}_d = d \cdot d! \mathcal{G}_d{}^d W_{3,d}$—Theorem 9.0.2
- $\mathcal{F}_{1,d} = \mathcal{H}_{1,d}{}^d$—Theorem 9.0.3
- $\mathcal{F}_{2,d} = d \cdot d! \mathcal{H}_{2,d}{}^d W_{3,d}$—Theorem 9.0.3
- $\mathcal{G}_d = 2^{d^5} \mathcal{C}_{i,d} W_{2,d}{}^{d^3}$—Lemma 9.4.1
- $\mathcal{H}_{1,d} = 2^{d^5} \mathcal{C}_{a,d} W_{2,d}{}^{\frac{1}{2}d^2(d-1)}$—Lemma 9.4.2
- $\mathcal{H}_{2,d} = 2^{d^3} d^{d+1} \cdot d! W_{2,d}{}^{\frac{d-1}{2}}$—Lemma 9.4.2

C.7 Appendix A

- $\mathtt{R}_d = \left(\frac{1}{3d}\right)^{\frac{d(d-1)}{2}}$—Lemma A.2.1
- $\mathtt{S}_d = \left(\frac{20d}{3}\right)^{\frac{d(d-1)}{2}}$—Lemma A.2.1
- $n_d = \frac{d(d-2)}{2}$ if d is even or $\frac{(d-1)^2}{2}$ if d is odd—Lemma A.2.7
- $c_d = \frac{d(d+1)}{2} - 1$—Lemma A.3.1, Lemma 8.4.2 Lemma 8.4.4 Lemma 8.4.6
- $V_d^- = \frac{2^{d-1}}{d^{2c_d}}$—Lemma A.3.1, Lemma 8.4.2, Lemma 8.4.6
- $V_d^+ = 2^{d^2-1}$—Lemma A.3.1, Lemma 8.4.6
- $\mathcal{M}_d = 10^{d^2} d^{\frac{1}{4}(d+2)^2}$—Lemma A.2.18

- $\mathcal{M}_{d,1} = 5d^3(20d)^{\frac{1}{4}d(d-1)+1}$—Lemma A.2.22
- $\mathcal{V}_{d,\infty} = \beta_{d,\infty}(X^1_{d,\infty})$—Lemma A.4.1

C.8 Appendix B

- $W_d = d^{\frac{3d}{2}}(d!)^{d+1}(d+1)^{d^2}$—Proposition B.2.1
- $W_{1,d} = d^{\frac{3}{2}} \cdot d!(d+1)^d$—Lemma B.2.3
- $W_{3,d} = 2^{d(d-1)}d^{\frac{3d}{2}}(d!)^{d+1}(d+1)^{d^2}$—Corollary B.2.11
- $W_{2,d} = d^{\frac{d}{2}}(d+1)^{d^2}(d!)^{2d+1}$—Proposition B.3.1

Bibliography

[BdlHV08] Bachir Bekka, Pierre de la Harpe, and Alain Valette. *Kazhdan's property (T)*, volume 11 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2008.

[Ben09] Yves Benoist. Five lectures on lattices in semisimple Lie groups. In *Géométries à courbure négative ou nulle, groupes discrets et rigidités*, volume 18 of *Sémin. Congr.*, pages 117–176. Soc. Math. France, Paris, 2009.

[Ben20] Yves Benoist. Arithmeticity of discrete subgroups. *Ergodic Theory and Dynamical Systems*, pages 1–30, September 2020.

[BH62] Armand Borel and Harish-Chandra. Arithmetic subgroups of algebraic groups. *Annals of Mathematics. Second Series*, 75:485–535, 1962.

[BO07] Yves Benoist and Hee Oh. Polar decomposition for p-adic symmetric spaces. *International Mathematics Research Notices. IMRN*, (24):Art. ID rnm121, 2007.

[Bor63] Armand Borel. Some finiteness properties of adele groups over number fields. *Institut des Hautes Études Scientifiques. Publications Mathématiques*, (16):5–30, 1963.

[Bor69] 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.

[BS91] M. Burger and P. Sarnak. Ramanujan duals II. *Inventiones Mathematicae*, 106(1):1–11, December 1991.

[Cas78] J. W. S. Cassels. *Rational quadratic forms*, volume 13 of *London Mathematical Society Monographs*. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.

[CHH88] M. Cowling, U. Haagerup, and R. Howe. Almost L^2 matrix coefficients. *Journal für die Reine und Angewandte Mathematik. [Crelle's Journal]*, 387:97–110, 1988.

[CS99] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, third edition, 1999.

[CS14] Ted Chinburg and Matthew Stover. Small generators for S-unit groups of division algebras. *New York Journal of Mathematics*, 20:1175–1202, 2014.

[CU04] Laurent Clozel and Emmanuel Ullmo. Équidistribution des points de Hecke. In *Contributions to automorphic forms, geometry, and number theory*, pages 193–254. Johns Hopkins Univ. Press, Baltimore, MD, 2004.

[Dan86] S. G. Dani. On orbits of unipotent flows on homogeneous spaces, II. *Ergodic Theory and Dynamical Systems*, 6(2):167–182, June 1986.

[Die03] Rainer Dietmann. Small solutions of quadratic Diophantine equations. *Proceedings of the London Mathematical Society. Third Series*, 86(3):545–582, 2003.

[Die07] Rainer Dietmann. Polynomial bounds for equivalence of quadratic forms with cube-free determinant. *Mathematical Proceedings of the Cambridge Philosophical Society*, 143(3):521–532, November 2007.

[Gau65] Johann Carl Friedrich Gauss. *Disquisitiones arithmeticae*. Yale University Press, New Haven London, 1965.

[Gel75] Stephen S. Gelbart. *Automorphic forms on adèle groups*. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1975.

[GGPS69] I. M. Gelfand, M. I. Graev, and I. I. Pyatetskii-Shapiro. *Representation theory and automorphic functions*. Translated from the Russian by K. A. Hirsch. W. B. Saunders Co., Philadelphia, Pa.-London-Toronto, Ont., 1969.

[God17] Roger Godement. *Introduction to the theory of Lie groups*. Universitext. Springer, Cham, 2017.

[GS80] Fritz Grunewald and Daniel Segal. Some General Algorithms. I: Arithmetic Groups. *The Annals of Mathematics*, 112(3):531, November 1980.

[GS85] Fritz Grunewald and Daniel Segal. Decision problems concerning s-arithmetic groups. *The Journal of Symbolic Logic*, 50(3):743–772, 1985.

[HT92] Roger Howe and Eng-Chye Tan. *Nonabelian harmonic analysis*. Universitext. Springer-Verlag, New York, 1992.

[Kim03] Henry H. Kim. Functoriality for the exterior square of $\mathbf{GL}_4$ and the symmetric fourth of $\mathbf{GL}_2$. *Journal of the American Mathematical Society*, 16(1):139–183, 2003.

[KM98] D. Y. Kleinbock and G. A. Margulis. Flows on Homogeneous Spaces and Diophantine Approximation on Manifolds. *The Annals of Mathematics*, 148(1):339, July 1998.

[Kob84] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984.

[KT07] Dmitry Kleinbock and George Tomanov. Flows on S-arithmetic homogeneous spaces and applications to metric Diophantine approximation. *Commentarii Mathematici Helvetici*, pages 519–581, 2007.

[Lag80] J. C. Lagarias. On the computational complexity of determining the solvability or unsolvability of the equation $x^2 - dy^2 = -1$. *Transactions of the American Mathematical Society*, 260(2):485–508, 1980.

[Lan85] Serge Lang. $SL_2(\mathbb{R})$, volume 105 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1985.

[LM16] Han Li and Gregory A. Margulis. Effective Estimates on Integral Quadratic Forms: Masser's Conjecture, Generators of Orthogonal Groups, and Bounds in Reduction Theory. *Geometric and Functional Analysis*, 26(3):874–908, June 2016.

[Lub94] Alex Lubotzky. *Discrete Groups, Expanding Graphs and Invariant Measures*. Progress in Mathematics. Birkhäuser Basel, 1994.

[Mar75] G. A. Margulis. On the action of unipotent groups in the space of lattices. In *Lie groups and their representations (Proc. Summer School, Bolyai, János Math. Soc., Budapest, 1971)*, pages 365–370. 1975.

[Mar91] Gregori A. Margulis. *Discrete Subgroups of Semisimple Lie Groups*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics. Springer-Verlag, Berlin Heidelberg, 1991.

[Mas02] D. W. Masser. Search bounds for Diophantine equations. In *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, pages 247–259. Cambridge Univ. Press, Cambridge, 2002.

[Mat95] Pertti Mattila. *Geometry of Sets and Measures in Euclidean Spaces: Fractals and Rectifiability*. Cambridge University Press, 1 edition, April 1995.

[Moo80] Calvin C. Moore. The Mautner phenomenon for general unitary representations. *Pacific Journal of Mathematics*, 86(1):155–169, 1980.

[MT62] G. D. Mostow and T. Tamagawa. On the compactness of arithmetically defined homogeneous spaces. *Annals of Mathematics. Second Series*, 76:446–463, 1962.

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

[Sch85] Winfried Scharlau. *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1985.

[Ser92] Jean-Pierre Serre. *Lie Algebras and Lie Groups*, volume 1500 of *Lecture Notes in Mathematics*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1992.

[Ser95] Jean-Pierre Serre. *Cours d'arithmétique*. Le mathématicien. Presses Universitaires de France, Paris, 4e édition. edition, 1995.

[Sha00] Yehuda Shalom. Rigidity, Unitary Representations of Semisimple Groups, and Fundamental Groups of Manifolds with Rank One Transformation Group. *The Annals of Mathematics*, 152(1):113, July 2000.

[Sie39] Carl Ludwig Siegel. Einheiten quadratischer Formen. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 13(1):209–239, December 1939.

[Sie72] Carl Ludwig Siegel. Zur Theorie der quadratischen Formen. *Nachrichten der Akademie der Wissenschaften zu Göttingen. II. Mathematisch-Physikalische Klasse*, pages 21–46, 1972.

[Str99] Straumann, S. *Das Äquivalenzproblem ganzer quadratischer Formen: Einige explizite Resultate*. Diplomarbeit, Universität Basel, 1999.

[Tem92] Arkady Tempelman. *Ergodic Theorems for Group Actions*. Springer Netherlands, Dordrecht, 1992.

[Wei40] André Weil. *L'intégration dans les groupes topologiques et ses applications*. Actual. Sci. Ind., no. 869. Hermann et Cie., Paris, 1940.

[Zim84] R. J. Zimmer. *Ergodic Theory and Semisimple Groups*. Monographs in Mathematics. Birkhäuser Basel, 1984.

université PARIS-SACLAY

ÉCOLE DOCTORALE
de mathématiques
Hadamard (EDMH)

Titre: Dynamique homogène et formes quadratiques S-adiques

Mots clés: Formes quadratiques entières, dynamique homogène, groupes de Lie S-adiques

Résumé: Soient $S = \{\infty\} \cup S_f$ un ensemble fini de valuations de $\mathbb{Q}$ et $\mathbb{Z}_S$ l'anneau des S-entiers. Le thème de cette thèse est une approche pratique de la classification des formes quadratiques entières à $\mathbb{Z}_S$-équivalence près : On obtient un critère effectif pour décider si deux formes quadratiques entières en $d \geq 3$ variables données Q_1 et Q_2 sont $\mathbb{Z}_S$-équivalentes. Ceci généralise un résultat de H. Li et G. Margulis pour le cas $S = \{\infty\}$. La preuve se base sur la traduction du problème arithmétique en un problème dynamique, en termes d'une action transitive et qui préserve la mesure, d'un groupe orthogonal S-adique H_S sur un espace (Y, μ) de volume fini. Cette traduction nous permet de traiter le problème avec de puissants outils de dynamique homogène et de la théorie des représentations automorphes. Comme application de notre critère de $\mathbb{Z}_S$-équivalence, on donne une partie génératrice du groupe orthogonal S-entier $O(Q_1, \mathbb{Z}_S)$ définie par des inégalités simples en termes des ν-normes de Q_1 pour $\nu \in S$.

Title: Homogeneous dynamics and S-adic quadratic forms

Keywords: Integral quadratic forms, homogeneous dynamics, S-adic Lie groups

Abstract: Let $S = \{\infty\} \cup S_f$ be a finite set of valuations of $\mathbb{Q}$ and let $\mathbb{Z}_S$ be the ring of S-integers. The topic of this thesis is a practical approach to the classification of integral quadratic forms up to $\mathbb{Z}_S$-equivalence: We obtain an effective criterion to decide if two given integral quadratic forms Q_1 and Q_2 in $d \geq 3$ variables are $\mathbb{Z}_S$-equivalent. This generalizes a result of H. Li and G. Margulis for the case $S = \{\infty\}$. The proof is based on a translation of the arithmetic problem into a dynamical one, in terms of a transitive, measure-preserving action of an S-adic orthogonal group H_S on a finite-volume space (Y, μ). This allows us to address the problem using powerful tools from homogeneous dynamics and automorphic representations. As an application of our criterion of $\mathbb{Z}_S$-equivalence, we give a finite generating set of the S-integral orthogonal group $O(Q_1, \mathbb{Z}_S)$ by means of simple inequalities involving the ν-norms of Q_1 for $\nu \in S$.

Université Paris-Saclay
Espace Technologique / Immeuble Discovery
Route de l'Orme aux Merisiers RD 128 / 91190 Saint-Aubin, France