Réseaux des groupes de Lie

(Version préliminaire)

Yves Benoist

Cours de M2 à Paris 6 en 07-08

Introduction

Le but de ce cours est l'interrelation entre la théorie des nombres et la théorie ergodique à travers la théorie des groupes. Les espaces homogènes de volume fini et plus particulièrement la dynamique des actions par translation sur ces espaces seront l'objet central de ce cours.

Un réseau est un sous-groupe discret de covolume fini. Les prototypes de réseaux sont les sous-groupes qui, comme le sous-groupe $SL(d,\mathbb{Z})$ du groupe $SL(d,\mathbb{R})$, sont construits par des méthodes arithmétiques. D'une part, l'existence de ce volume fini permet d'utiliser des méthodes issues des systèmes dynamiques et de la théorie ergodique. D'autre part, la provenance arithmétique de ces groupes est à la source de nombreuses applications. Enfin, l'utilisation de tous les corps locaux permet d'étendre considérablement le champ d'applications.

Sommaire prévu :
- Structure des groupes de Lie semisimples, décomposition de Cartan.
- Exemples de réseaux.
- Mélange. Théorème de Howe-Moore.
- Comptage de points dans les réseaux. Théorème d'Eskin-McMullen.
- Variété drapeau. Théorème de Furstenberg.
- Représentation des réseaux. Théorème de superrigidité de Margulis.
- Corps locaux. Théorème d'arithméticité de Margulis.
- Récurrence. Théorème de Dani-Margulis.
- Théorème ergodique de Birkhoff. Entropie.
- Flots unipotents, mesures invariantes, équidistribution et fermés invariants.
- Théorèmes de Ratner et applications.

Références :
- M. Raghunathan : Discrete subgroups of Lie groups, Springer (1972)
- R. Zimmer : Ergodic theory and semisimple groups,Birkhauser (1984)
- G. Margulis : Discrete subgroups of semisimple Lie groups, Springer (1991)
- D. Witte-Morris : Ratner's theorems on unipotent flows, Chicago LMS(2004)
- Y. Benoist : Five lectures on lattices, SMF (2008).

Table des matières

1 Construction de réseaux

Ce premier chapitre donne un bon aperçu de l'ensemble du cours. On y trouvera déjà la mixture *théorie des nombres + théorie ergodique + théorie des groupes* propre à ce cours. En effet, nous y montrerons, pour les groupes orthogonaux, le théorème de Borel et Harish-Chandra qui affirme que "les groupes arithmétiques sont des réseaux".

D'une part, les motivations de cet énoncé sont arithmétiques : il s'agit d'une impressionante généralisation non commutative du théorème des unités de Dirichlet.

D'autre part la méthode due a Margulis que nous allons utiliser pour le démontrer est issue de la théorie ergodique : nous allons utiliser des propriétés de récurrence de marches aléatoires ainsi que des propriétés de croissance exponentielle des marches aléatoires linéaires. Pour faire fonctionner cette méthode, nous aurons besoin de diverses propriétés de l'espace des réseaux de $\mathbb{R}^d$ dont le critère de compacité de Mahler.

Ceci nous permettra de démontrer le théorème de Borel Harish-Chandra pour les groupes orthogonaux (il est dû a Siegel dans ce cas).

Enfin, c'est grâce à la compréhension de la structure des groupes algébriques que nous démontrerons par les même méthodes dans le chapitre 5 une version générale du théorème de Borel et Harish-Chandra.

1.1 Un exemple : le groupe orthogonal

Nous allons détailler dans cette section notre objectif principal (proposition 1.3). Pour cela, nous devons définir ce qu'est un réseau.

Soit G un groupe localement compact. Rappelons que G admet une mesure (borélienne) positive λ_G invariante par toutes les translations à droite $x \mapsto xg$, que cette mesure est unique à multiplication près par un scalaire positif et qu'elle est appelée la mesure de Haar à droite de G.

Rappelons qu'un sous-groupe Γ de G est dit *discret* si la topologie de G induite sur Γ est discrète. La projection $p : g \mapsto g\Gamma$ de G dans $X := G/\Gamma$ est alors un revêtement. On note alors λ_X la mesure sur X qui coïncide localement via p avec la mesure de Haar λ_G,

Définition 1.1 *Un sous-groupe discret Γ de G est un réseau si $\lambda_X(X) < \infty$.*

Autrement dit, un sous-groupe discret Γ de G est un réseau si il existe une partie mesurable F de G telle que $\lambda_G(F) < \infty$ et $F\Gamma = G$.

Par exemple les sous-groupes discrets *cocompacts*, i.e. ceux pour lesquels le quotient X est compact, sont des réseaux.

Commençons par une simple remarque.

Lemme 1.2 *Un groupe localement compact G qui contient un réseau Γ est unimodulaire*

Autrement dit, la mesure de Haar à droite est aussi invariante à gauche. La mesure λ_X est donc aussi invariante par translation à gauche.

Démonstration La translation à gauche $x \mapsto gx$ par un élément g de G multiplie la mesure de Haar à droite λ_G par un scalaire $\Delta(g)$. Donc la translation à gauche sur X par un élément g de G multiplie aussi la mesure λ_X par $\Delta(g)$. Comme Γ est un réseau, le volume total $\lambda_X(X)$ est fini. Ce volume est préservé par g, on a donc $\Delta(g) = 1$. □

Proposition 1.3 (Siegel) *Soient $d \geq 3$, $Q(x_1, \ldots, x_d) = \sum a_{i,j} x_i x_j$ une forme quadratique non dégénérée à coefficients entiers, $G_{\mathbb{R}}$ le groupe des transformations orthogonales à coefficients réels et $G_{\mathbb{Z}}$ le sous-groupe discret des transformations orthogonales à coefficients entiers :*
$G_{\mathbb{R}} = O(Q, \mathbb{R}) = \{g \in \mathrm{GL}(d, \mathbb{R}) \mid Q \circ g = Q\}$ et $G_{\mathbb{Z}} = G_{\mathbb{R}} \cap \mathrm{GL}(d, \mathbb{Z})$.
Alors $G_{\mathbb{Z}}$ est un réseau dans $G_{\mathbb{R}}$.

Remarques - Nous verrons que cette proposition est un cas particulier d'un énoncé bien plus général valable pour tous les "$\mathbb{Q}$-groupes sans $\mathbb{Q}$-caractère".

- La méthode traditionnelle pour montrer cette proposition consiste à construire explicitement un domaine F dit "domaine de Siegel" et à calculer $\lambda_G(F)$. C'est la "théorie de la réduction", c.f. [6]. Comme annoncé, nous allons suivre une méthode plus rapide mais qui ne donne pas d'estimation sur le domaine fondamental.

- Cet énoncé est encore vrai pour $d = 2$ lorsque la forme quadratique Q est *anisotrope* sur $\mathbb{Q}$ i.e. lorsque l'équation $Q(x) = 0$ n'a pas de solutions entières non nulles. Cela résulte de ce que, pour tout entier $p \geq 2$ non carré, l'équation de Pell-Fermat $n^2 - pm^2 = 1$ a une infinité de solutions entières (n, m).

- Mais cet énoncé est faux pour $d = 2$ lorsque la forme quadratique Q est *isotrope* sur $\mathbb{Q}$ i.e. lorsque l'équation $Q(x) = 0$ n'a pas de solutions entières non nulles.

1.2 Récurrence des marches aléatoires

Nous allons commencer par donner dans le corollaire ci-dessous un critère qui assure que le volume d'une mesure invariante est fini. Ce critère est basé sur des propriétés de récurrence de marches aléatoires.

Soient G un groupe localement compact, X un espace localement compact et $(g, x) \mapsto gx$ une action continue de G sur X. Rappelons qu'une application continue est *propre* si l'image inverse de tout compact est compacte.

On suppose

HC Il existe une fonction propre $f : X \to [0, \infty[$, une probabilité μ sur G et des constantes $a < 1$, $b > 0$ telles que $A_\mu(f) \leq af + b$

où A_μ est l'opérateur de moyennisation donné par, pour tout x dans X,

$$A_\mu(f)(x) = \int_G f(gx) d\mu(g)$$

Cet opérateur A_μ est donc l'opérateur de convolution par la probabilité $\check{\mu}$ image de μ par l'inversion $g \to g^{-1}$.

Remarque Cette hypothèse **HC** signifie que la moyennisation par μ contracte, à une constante près, une fonction propre f sur X .

Lemme 1.4 *Sous l'hypothèse* **HC**, *pour tout $\varepsilon > 0$, il existe un compact $K \subset X$ tel que, pour tout point $x \in X$, il existe $M = M_x$ tel que pour tout $n \geq M$,*

$$A_\mu^n(\mathbf{1}_K)(x) \geq 1 - \varepsilon \ .$$

où $\mathbf{1}_K$ est la fonction caractéristique de K.
En outre, l'entier M_x est uniforme sur les compacts de X.

Ce lemme est un lemme de récurrence pour les marches aléatoires sur X. En effet, il affirme que si on marche au hasard sur X en partant du point x, avec des déplacements donnés par la loi μ, à partir d'un moment, la probabilité d'être hors de K est au plus ε.

Démonstration D'après l'hypothèse **HC**, on a, pour tout $n \geq 1$

$$A_\mu^n(f) \leq a^n f + b(1 + \cdots + a^{n-1}) \leq a^n f + B$$

avec $B = \frac{b}{1-a}$. Comme f est propre, on peut prendre pour compact

$$K = \{y \in X \mid f(y) \leq \frac{2B}{\varepsilon}\}$$

de sort que $\mathbf{1}_{K^c} \leq \frac{\varepsilon}{2B} f$. On a alors les majorations

$$A_\mu^n(\mathbf{1}_{K^c})(x) \leq \frac{\varepsilon}{2B} A_\mu^n(f)(x) \leq \frac{\varepsilon a^n}{2B} f(x) + \frac{\varepsilon}{2} \leq \varepsilon$$

dès que n est suffisamment grand pour que $f(x) \leq \frac{B}{a^n}$. □

Rappelons qu'une *mesure de Radon* sur X est une mesure borélienne finie sur les compacts.

Corollaire 1.5 *Sous l'hypothèse* **HC**, *toute mesure de Radon G-invariante ν sur X est finie.*

Remarque Nous allons uniquement utiliser l'égalité, pour toute fonction positive f sur X,

$$\int_G A_\mu(f)d\nu(x) = \int_G f d\nu(x),$$

c'est-à-dire le fait que la mesure ν sur X est *μ-stationnaire*.

Démonstration D'après le lemme 1.4 avec $\varepsilon = \frac{1}{2}$, il existe un compact $K \subset X$ tel que pour tout compact $L \subset X$ et n suffisamment grand on a

$$\nu(L) \leq 2\int_X A_\mu^n(\mathbf{1}_K)(x)d\nu(x) = 2\int_X \mathbf{1}_K(x)d\nu(x) = 2\nu(K).$$

L'hypothèse **HC** assure aussi que X est une réunion dénombrable de compacts, on a donc $\nu(X) = \sup_L \nu(L) \leq 2\nu(K)$. □

1.3 Marches aléatoires linéaires

> Dans cette partie, nous construisons des fonctions φ_i sur lequelles la moyennisation A_μ est une contraction. Cette propriété de contraction est liée à une propriété de croissance exponentielle pour la marche aléatoire linéaire associée à une probabilité μ.

Munissons $\mathbb{R}^d$ d'une norme $\|.\|$ associée à un produit scalaire euclidien $\langle .,. \rangle$ et notons aussi $\|.\|$ la norme euclidienne induite sur l'espace des matrices $M(d,\mathbb{R})$.

Le lemme suivant est un cas particulier élémentaire d'un théorème de Furstenberg sur la croissance exponentielle des marches aléatoires matricielles.

Notons $G = \mathrm{GL}(d,\mathbb{R})$ le groupe linéaire et $S^+ \subset G$ l'ensemble des matrices symétriques définies positives. Soit μ une probabilité sur G. Notons $\mathrm{supp}(\mu)$ le support de μ et Γ_μ le plus petit sous-groupe fermé de G le contenant. On dit que μ est *symétrique* si $\mu = \check{\mu}$.

Lemme 1.6 *On suppose μ symétrique,* $\mathrm{supp}(\mu) \subset S^+$ *et* $\int_G |\log\|g\||d\mu(g) < \infty$. *Alors pour tout $v \in \mathbb{R}^d$ non nul,*

$$\int_G \log(\frac{\|gv\|}{\|v\|})d\mu(g) \geq 0$$

avec égalité ssi Γ_μ stabilise la droite $\mathbb{R}v$.

Démonstration Notons I_v le membre de gauche. On calcule en appliquant tout d'abord l'égalité $\mu = \check{\mu}$ puis l'inégalité de Cauchy-Schwarz et enfin le fait que les matrices g sont μ-presque surement symétriques :

$$\begin{aligned} 2\int_G \log(\|gv\|)d\mu(g) &= \int_G \log(\|gv\|\|g^{-1}v\|)d\mu(g) \\ &\geq \int_G \log(\langle gv, g^{-1}v\rangle)d\mu(g) \\ &= 2\int_G \log(\|v\|)d\mu(g) \end{aligned}$$

Ceci donne la majoration $I_v \geq 0$. Par Cauchy-Schwarz, le cas d'égalité dans cette inégalité n'est atteint que si v est vecteur propre de g^2 pour μ-presque tout g. Comme les matrices g sont μ-presque sûrement définies positives, v est alors aussi vecteur propre de g et la droite engendrée par v est stabilisée par Γ_μ. □

Pour $1 \leq i \leq d$, on note encore $\|.\|$ la norme euclidienne naturelle sur les puissances extérieures $\Lambda^i\mathbb{R}^d$: c'est l'unique norme euclidienne pour laquelle le produit extérieur $v = v_1 \wedge \cdots \wedge v_i$ d'une famille orthonormée est de norme 1. Le groupe $G = \mathrm{GL}(d, \mathbb{R})$ agit naturellement sur $\Lambda^i\mathbb{R}^d$ par l'égalité $gv = gv_1 \wedge \cdots \wedge gv_i$. Il laisse invariant le cône $W_i \subset \Lambda^i\mathbb{R}^d$ des *vecteurs décomposables* non nuls

$$W_i := \{v = v_1 \wedge \cdots \wedge v_i \neq 0 \mid v_j \in \mathbb{R}^d\}.$$

Le quotient $\mathbb{G}_i^d$ de ce cône W_i par les homothéties positives est la Grassmanienne des i-plans de $\mathbb{R}^d$. On note $\varphi_i : W_i \to]0, \infty[$ la fonction sur W_i donnée par

$$\varphi_i(v) = \|v\|^{-1} \text{ pour tout } v \in W_i.$$

Corollaire 1.7 *On suppose μ symétrique,* $\mathrm{supp}(\mu) \subset S^+$, $\mathrm{supp}(\mu)$ *compact et que l'action de Γ_μ dans $\mathbb{R}^d$ est irréductible. Alors il existe $\delta > 0$ et $a_0 < 1$ tels que, pour tout $0 < i < d$, on a $A_\mu(\varphi_i^\delta) \leq a_0\varphi_i^\delta$.*

Remarques - L'hypothèse d'*irréducibilité* signifie que $\mathbb{R}^d$ ne contient pas de sous-espace vectoriel Γ_μ invariant.
- La mesure G-invariante sur W_i est de masse totale infinie... cela ne contredit pas le corollaire 1.5 car la fonction $\varphi_i^\delta : W_i \to [0, \infty[$ n'est pas propre.

Démonstration Le lemme 1.6 assure que pour tout v dans W_i, l'intégrale $I_v = \int_G \log(\frac{\|gv\|}{\|v\|})d\mu(g)$ est non négative : $I_v \geq 0$. Mieux, comme l'hypothèse d'irréducibilité assure que l'action de Γ_μ sur la grassmanienne $\mathbb{G}_i^d$ n'a pas de points fixes, on a $I_v > 0$. Comme la grassmanienne est compacte et que l'application $v \to I_v$ est continue, il existe une constante $C > 0$ telle que $I_v \geq 2C$, pour tout $v \in W_i$.

Posons $M = \sup\{\log(\max(\|g\|^d, \|g\|^{-d})) \mid g \in \mathrm{supp}(\mu)\}$. On remarque que pour tout réel $t \in [-1, 1]$, on a la majoration

$$e^t \leq 1 + t + t^2.$$

On calcule alors, avec $\delta = \min(1/M, C/M^2)$,

$$\begin{aligned}
\frac{A_\mu(\varphi_i^\delta)(v)}{\varphi_i^\delta(v)} &= \int_G e^{-\delta \log(\frac{\|gv\|}{\|v\|})} d\mu(g) \\
&\leq 1 - \delta \int_G \log(\frac{\|gv\|}{\|v\|}) d\mu(g) + \delta^2 \int_G \left(\log(\frac{\|gv\|}{\|v\|})\right)^2 d\mu(g) \\
&\leq 1 - 2C\delta + M^2\delta^2 \leq 1 - C\delta.
\end{aligned}$$

Il suffit de prendre $a_0 = 1 - C\delta$. □

1.4 L'espace des réseaux

Pour construire la fonction f vérifiant **HC**, nous aurons besoin de quelques propriétés de l'espace des réseaux de $\mathbb{R}^d$, que nous démontrons dans cette section. Nous réutiliserons plus tard ces propriétés pour démontrer les théorèmes de Ratner.

Rappelons qu'un réseau de $\mathbb{R}^d$ est un sous-groupe discret de $\mathbb{R}^d$ qui est abélien libre de rang d. L'ensemble X' des réseaux de $\mathbb{R}^d$ est une variété comme espace quotient $X' := \mathrm{GL}(d,\mathbb{R})/SL^{\pm}(d,\mathbb{Z})$. Par définition de la topologie quotient, une suite Δ_n de réseaux de $\mathbb{R}^d$ converge vers un réseau Δ de $\mathbb{R}^d$ ssi il existe une base $f_{n,1},\dots,f_{n,d}$ de Δ_n qui converge vers une base $f_1,\dots,f_d$ de Δ.

Soit Δ un réseau de $\mathbb{R}^d$. Un sous-espace vectoriel L de $\mathbb{R}^d$ est dit Δ-rationnel si $\Delta \cap L$ est un réseau de L. On note alors $d(L) = d_\Delta(L) := \|v_1 \wedge \cdots \wedge v_i\|$ où $v_1,\dots,v_i$ est une base de $\Delta \cap L$. Cette quantité ne dépend pas du choix de la base. Le réel $d_\Delta = covol(\Delta) := d_\Delta(\mathbb{R}^d)$ est le *covolume* de Δ. On note X l'ensemble des réseaux de covolume 1.

Pour construire notre fonction propre f, nous aurons besoin d'un critère simple et utile de compacité dans l'espace des réseaux. Le voici.

Proposition 1.8 (Mahler) *Une partie $Y \subset X'$ de l'espace des réseaux de $\mathbb{R}^d$ est relativement compacte ssi il existe $\alpha,\beta > 0$ tels que, pour tout $\Delta \in Y$*

$$d_\Delta \leq \alpha \ \text{ et } \ \inf_{v\in\Delta-0} \|v\| \geq \beta.$$

Autrement dit les parties relativement compactes sont caractérisées par une majoration du covolume et de l'inverse de la *systole* $\alpha_1(\Delta) = (\inf_{v\in\Delta-0} \|v\|)^{-1}$.

Corollaire 1.9 *La fonction $\alpha_1 : X \to [0,\infty[$ est continue et propre.*

Pour montrer le critère de compacité de Mahler, nous utiliserons l'inégalité d'Hermite-Minkowski si utile en théorie des nombres. Notons v_d le volume de la boule euclidienne de rayon 1 dans $\mathbb{R}^d$: $v_1 = 2$, $v_2 = \pi$,...

Lemme 1.10 (Hermite, Minkowski) *Tout réseau Δ de $\mathbb{R}^d$ contient un vecteur non nul de norme $\|v\| \leq 2(d_\Delta/v_d)^{\frac{1}{d}}$.*

Démonstration du lemme 1.10 Notons p la projection de $\mathbb{R}^d$ sur le quotient $\mathbb{T}^d = \mathbb{R}^d/\Delta$ et introduisons le plus grand rayon R tel que cette projection p est injective sur la boule ouverte de rayon R. La comparaison des volumes donne la majoration $v_d R^d \leq d_\Delta$. D'autre part, la maximalité de R assure que, pour tout $\varepsilon > 0$, il existe deux vecteurs u_1, u_2 de norme au plus $R+\varepsilon$ qui ont même image dans $\mathbb{T}^d$. Le vecteur non nul $v_\varepsilon = u_1 - u_2$ est dans Δ et de norme au plus $2R+2\varepsilon$. Le groupe discret Δ contient donc un vecteur v non nul de norme au plus $2R$. $\square$

Démonstration de la proposition 1.8 et du corollaire 1.9 Les fonctions $g \to |det(g)|$ et $g \to \alpha_1(g\mathbb{Z}^d)$ sont continues sur $\mathrm{GL}(d,\mathbb{R})$. Donc les fonctions $\Delta \to d_\Delta$ et $\Delta \to \alpha_1(\Delta)$ sont des fonctions continues sur X'. Si Y est une partie relativement compacte, ces deux fonctions sont donc bornées sur Y.

Réciproquement, montrons que toute partie Y de X' sur laquelle ces deux fonctions sont bornées est relativement compacte. On veut donc montrer que toute suite Δ_n dans Y sous-converge dans X'. On raisonne par récurrence sur d. C'est clair pour $d = 1$. Choisissons un vecteur non nul $v_n \in \Delta_n$ de norme minimum. Comme $\alpha_1(\Delta_n)$ est majoré, les normes $\|v_n\|$ sont positivement minorées. En outre par l'inégalité d'Hermite-Minkowski et la majoration du covolume de Δ_n, les normes $\|v_n\|$ sont majorées. La suite v_n sous-converge donc vers un vecteur non nul $v_\infty \in \mathbb{R}^d$ que l'on peut supposer de norme $\|v_\infty\| = 1$. Quitte à modifier chacun des Δ_n par une petite similitude, on peut aussi supposer que $v_n = v_\infty$. Les images Δ'_n de Δ_n dans l'orthogonal $(\mathbb{R}v_\infty)^\perp$ sont des réseaux dont le volume est majoré par α et dont la systole est minoré par $\frac{\sqrt{3}}{2}\beta$. Par hypothèse de récurrence, ces réseaux Δ'_n sous-convergent vers un réseau de $(\mathbb{R}v_\infty)^\perp$. La suite Δ_n sous-converge alors vers un réseau de $\mathbb{R}^d$. □

Dans la partie suivante nous aurons aussi besoin des lemmes techniques suivants.

Lemme 1.11 *Soient Δ un réseau de $\mathbb{R}^d$ et L, M deux sous-espaces Δ-rationnels de $\mathbb{R}^d$. Alors les sous-espaces $L + M$ et $L \cap M$ sont Δ-rationnels et on a la majoration*

$$d(L \cap M)d(L + M) \leq d(L)d(M).$$

Remarque Par convention, on a posé $d(0) = 1$ pour le sous-espace nul.

Démonstration On peut supposer que $\Delta = \mathbb{Z}^d$. On remarque alors qu'un sous-espace est Δ-rationnel ssi il est engendré par des vecteurs à coefficients rationnels. Ceci prouve que $L + M$ est Δ-rationnel.

On remarque aussi qu'un sous-espace est Δ-rationnel ssi il est défini par des équations linéaires à coefficients rationnels. Ceci prouve que $L \cap M$ est Δ-rationnel.

Pour montrer la majoration, on part d'une base $u_1, \ldots, u_k$ de $\Delta \cap L \cap M$ que l'on complète en une base $u_1, \ldots, u_k, v_1, \ldots, v_\ell$ de $\Delta \cap L$ et en une base $u_1, \ldots, u_k, w_1, \ldots, w_m$ de $\Delta \cap M$. La famille $u_1, \ldots, u_k, v_1, \ldots, v_\ell, w_1, \ldots, w_m$ est alors libre et engendre un sous-groupe d'indice fini de $\Delta \cap (L + M)$. On note $u = u_1 \wedge \cdots \wedge u_k$, $v = v_1 \wedge \cdots \wedge v_\ell$ et $w = w_1 \wedge \cdots \wedge w_m$. Notre assertion résulte alors de la majoration

$$\|u\|\|u \wedge v \wedge w\| \leq \|u \wedge v\|\|u \wedge w\|.$$

Cette dernière inégalité se montre en remplaçant, à l'aide du procédé d'orthogonalisation de Gramm-Schmidt, la famille $u_1, \ldots, u_k, v_1, \ldots, v_\ell, w_1, \ldots, w_m$ par

une famille $u'_1, \dots, u'_k, v'_1, \dots, v'_\ell, w'_1, \dots, w'_m$ telle que les deux familles $u'_1, \dots, u'_k, v'_1, \dots, v'_\ell$ et $u'_1, \dots, u'_k, w'_1, \dots, w'_m$ sont orthogonales et telle que $u = u'_1 \wedge \cdots \wedge u'_k$, $u \wedge v = u \wedge v'_1 \wedge \cdots \wedge v'_\ell$ et $u \wedge w = u \wedge w'_1 \wedge \cdots \wedge w'_m$.

Lemme 1.12 *Notons* $S_i(\Delta) := \{$*sous-espaces* Δ*-rationnels de dimension* $i\}$.
a) Pour tout $C > 0$, *on a* $\#\{L \in S_i(\Delta) \mid d_\Delta(L) \leq C\} < \infty$.
b) Les application $X \to]0, \infty[\ ;\ \Delta \mapsto \min_{L \in S_i(\Delta)} d_\Delta(L)$ *sont continues.*

Démonstration a) On peut supposer $\Delta = \mathbb{Z}^d$. Si $e_1, \dots, e_i$ est une base de $L \cap \mathbb{Z}^d$, l'élément $e_1 \wedge \cdots \wedge e_i$ est dans $\Lambda^i(\mathbb{Z})$ et de norme bornée par C. Cela ne laisse qu'un nombre fini de possibilités.

b) Cela résulte des inégalités $\|g^{-1}\|^{-d} d_\Delta(L) \leq d_{g\Delta}(gL) \leq \|g\|^d d_\Delta(L)$. □

1.5 Construction d'une fonction f

En combinant les résultats des deux dernières sections, nous allons maintenant construire explicitement la fonction f vérifiant **HC** dont nous avons besoin pour montrer la proposition 1.3.

Pour $0 < i \leq d$, définissons une fonction α_i de l'espace des réseaux X' dans $[0, \infty[$. Pour tout réseau Δ de $\mathbb{R}^d$,

$$\alpha_i(\Delta) := \sup\{d_\Delta(L)^{-1} \mid L \subset \mathbb{R}^d \ \ \Delta\text{-rationnel, } \dim L = i\}.$$

On notera $\alpha_0 = 1$. La fonction α_1 coïncide avec celle introduite dans la partie précédente. On a vu que α_i est continue.

Reprenons les notation du corollaire 1.7. On a donc une probabilité μ sur $G = \mathrm{GL}(d, \mathbb{R})$ telle que

HI μ est symétrique, le support de μ est compact et inclus dans S^+, et l'action du groupe Γ_μ dans $\mathbb{R}^d$ est irréductible.

Le lemme suivant permettra de construire la fonction f que nous cherchons.

Lemme 1.13 *Soit* μ *une probabilité sur* $\mathrm{GL}(d, \mathbb{R})$ *qui vérifie* [**HI**]. *Alors il existe* $a_0 < 1$ *et* $b_0 > 0$ *tels que, pour tout* $0 < i < d$, *on a*

$$A_\mu(\alpha_i^\delta) \leq a_0 \alpha_i^\delta + b_0 \max_{j>0} (\alpha_{i-j}^\delta \alpha_{i+j}^\delta)^{\frac{1}{2}}.$$

où le max *est pris sur les entiers* j *avec* $0 < j \leq \min(i, d-i)$.

Démonstration On veut majorer, pour $\Delta \in X$, l'intégrale $A_\mu(\alpha_i^\delta)(\Delta)$.

Choisissons $a_0 < 1$ et $\delta > 0$ comme dans le corollaire 1.7 et posons cette fois, $r = \sup\{\max(\|g\|^d, \|g^{-1}\|^d) \mid g \in \mathrm{supp}(\mu)\}$ de sorte que, pour tout sous-espace Δ-rationnel $L \subset \mathbb{R}^d$, on ait, pour μ-presque tout g,

$$r^{-1} d_\Delta(L) \leq d_{g\Delta}(gL) \leq r d_\Delta(L).$$

Choisissons un sous-espace Δ-rationnel $L_i \subset \mathbb{R}^d$ de dimension i tel que

$$d_\Delta(L_i) = \alpha_i(\Delta)^{-1}$$

et introduisons l'ensemble (fini)

$$\Psi_i := \{L \subset \mathbb{R}^d \mid \Delta\text{-rationnel, } \dim L = i,\ d_\Delta(L) \leq r^2 d_\Delta(L_i)\}.$$

On va distinguer deux cas.

1er cas : Ψ_i contient un seul élément L_i. Alors, pour tout sous-espace Δ-rationnel L de dimension i, et μ-presque tout g, on a

$$d_{g\Delta}(gL) \geq d_{g\Delta}(gL_i)$$

d'où, par le corollaire 1.7,

$$A_\mu(\alpha_i^\delta)(\Delta) = \int_G \frac{1}{d_{g\Delta}(gL_i)^\delta} d\mu(g) \leq a_0 \frac{1}{d_\Delta(L_i)^\delta} = a_0 \alpha_i^\delta(\Delta).$$

2ème cas : Ψ_i contient un autre élément L_i'. Notons $j := \dim(L_i + L_i') - i$. On a alors, grâce au lemme 1.11, pour μ-presque tout g,

$$\begin{aligned} \alpha_i(g\Delta) &\leq r\alpha_i(\Delta) = r d_\Delta(L_i)^{-1} \\ &\leq r^2 (d_\Delta(L_i) d_\Delta(L_i'))^{-\frac{1}{2}} \\ &\leq r^2 (d_\Delta(L_i \cap L_i') d_\Delta(L_i + L_i'))^{-\frac{1}{2}} \\ &\leq r^2 (\alpha_{i-j}(\Delta)\alpha_{i+j}(\Delta))^{\frac{1}{2}}. \end{aligned}$$

et donc, avec $b_0 = r^{2\delta}$,

$$A_\mu(\alpha_i^\delta)(\Delta) \leq b_0 \max_{j>0} (\alpha_{i-j}^\delta(\Delta)\alpha_{i+j}^\delta(\Delta))^{\frac{1}{2}}.$$

On obtient la majoration annoncée en combinant ces deux cas. □

Voici enfin la construction de la fonction f cherchée.

Corollaire 1.14 *Soit μ une probabilité sur $\mathrm{SL}(d,\mathbb{R})$ qui vérifie* **[HI]**. *Alors il existe $\delta > 0$ et $\varepsilon > 0$ tels que la fonction $f : X \to [0, \infty[$*

$$f := \textstyle\sum_{0<i<d} \varepsilon^{(d-i)i} \alpha_i^\delta$$

vérifie **[HC]** *: elle est propre et il existe $a < 1$, $b > 0$, tels que $A_\mu(f) \leq af + b$.*

Démonstration La propreté de f résulte du corollaire 1.9.

Notons $\beta_i = \varepsilon^{(d-i)i} \alpha_i^\delta$ de sorte que $f = \sum_{0<i<d} \beta_i$. Appliquons le lemme 1.13, l'égalité

$$2(d-i)i = (d-i-j)(i+j) + (d-i+j)(i-j) + 2j^2.$$

et la majoration $2(st)^{\frac{1}{2}} \leq s + t$, pour tout $s, t \geq 0$.

On obtient alors avec $a_0 < 1$ et $b_0 > 0$,

$$A_\mu f \leq a_0 \textstyle\sum_{0<i<d} \beta_i + b_0 \max_{j>0} \varepsilon^{j^2} (\beta_{i-j}\beta_{i+j})^{\frac{1}{2}} \leq (a_0 + b_0 \varepsilon d) \sum_{0<i<d} \beta_i + b_0 \varepsilon d$$

et donc $A_\mu f \leq af + b$ avec $a = a_0 + b_0 \varepsilon d$ et $b = b_0 \varepsilon d$. On a bien $a < 1$ si ε est choisi suffisamment petit. □

1.6 Application au groupe orthogonal

Terminons cette partie en montrant comment les idées ci-dessus s'organisent pour montrer que le groupe $G_{\mathbb{Z}} = O(Q, \mathbb{Z})$ est un réseau du groupe $G_{\mathbb{R}} = O(Q, \mathbb{R})$.

Nous reprendrons ces idées plus en détail dans un cadre général dans le chapitre 5

Démonstration de la proposition 1.3 Ce groupe $G_{\mathbb{R}}$ est unimodulaire (parce qu'il est engendré par des éléments d'ordre 2 : les réflexions hyperplanes). La mesure ν sur le quotient $G_{\mathbb{R}}/G_{\mathbb{Z}}$ induite par la mesure de Haar est donc $G_{\mathbb{R}}$-invariante. On veut montrer que cette mesure ν est finie.

Notons $H_{\mathbb{R}} = \mathrm{SL}^{\pm}(d, \mathbb{R})$ et $H_{\mathbb{Z}} = \mathrm{SL}^{\pm}(d, \mathbb{Z})$. On remarque tout d'abord que

$$\textit{l'injection } i : G_{\mathbb{R}}/G_{\mathbb{Z}} \hookrightarrow H_{\mathbb{R}}/H_{\mathbb{Z}} \textit{ est propre.}$$

Pour vérifier cela, on doit montrer que si une suite $g_n H_{\mathbb{Z}}$ avec $g_n \in G_{\mathbb{R}}$ converge dans $H_{\mathbb{R}}/H_{\mathbb{Z}}$, alors la suite $g_n G_{\mathbb{Z}}$ converge dans $G_{\mathbb{R}}/G_{\mathbb{Z}}$. Notons h_n une suite de $H_{\mathbb{Z}}$ telle que $g_n h_n$ converge dans $H_{\mathbb{R}}$. Comme l'injection $G_{\mathbb{Z}} \backslash H_{\mathbb{Z}} \hookrightarrow G_{\mathbb{R}} \backslash H_{\mathbb{R}}$ est d'image discrète (elle s'identifie à un ensemble de formes quadratiques à coefficients entiers), on peut écrire, pour n grand $h_n = \gamma_n h$ avec $\gamma_n \in G_{\mathbb{Z}}$ et $h \in H_{\mathbb{Z}}$. La suite $g_n \gamma_n$ est donc convergente et l'injection i est propre.

La mesure ν peut donc être vue comme une mesure de Radon sur l'espace $H_{\mathbb{R}}/H_{\mathbb{Z}}$ des réseaux de covolume 1. On veut bien sûr appliquer une combinaison des corollaires 1.5 et 1.14. Pour cela, il suffit de construire une probabilité μ portée par $G_{\mathbb{R}}$ vérifiant la condition [**HI**]. Remarquons que cette condition ne fait plus intervenir le groupe $G_{\mathbb{Z}}$. Notons (p, q) la signature de Q. On peut choisir un produit scalaire euclidien de $\mathbb{R}^d$ et une base orthonormée de $\mathbb{R}^d$ tels que, $Q(x_1, \ldots, x_{p+q}) = x_1^2 + \cdots x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$. On décompose l'algèbre de Lie $\mathfrak{g}$ de $G_{\mathbb{R}}$ en une somme directe $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{q}$, où

$$\begin{aligned} \mathfrak{k} = \{M \in \mathfrak{g} \mid M = -{}^t M\} &= \{\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \mid A = -{}^t A \ , \ D = -{}^t D\}, \\ \mathfrak{q} = \{M \in \mathfrak{g} \mid M = {}^t M\} &= \{\begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix} \mid C = {}^t B\}. \end{aligned}$$

On prend pour μ la mesure sur $G_{\mathbb{R}}$ image par l'application exponentielle d'une probabilité symétrique μ_0 sur $\mathfrak{q}$ dont le support est une boule centrée en 0. On vérifie facilement l'égalité $\mathfrak{k} = [\mathfrak{q}, \mathfrak{q}]$. Le groupe Γ_μ est donc la composante connexe du groupe $G_{\mathbb{R}}$.

Comme $d \geq 3$, l'action de la composante connexe de $G_{\mathbb{R}}$ sur $\mathbb{R}^d$ est irréductible. Cette probabilité μ vérifie bien la condition [**HI**]. □

La même démonstration permet de retrouver le

Corollaire 1.15 *Pour $d \geq 2$, le groupe $\mathrm{SL}(d, \mathbb{Z})$ est un réseau de $\mathrm{SL}(d, \mathbb{R})$.*

2 Algèbres de Lie semisimples

Ce chapitre est constitué de quelques rappels sur les algèbres de Lie semisimples

2.1 Algèbres de Lie nilpotentes et résolubles

Commençons par étudier les algèbres de Lie résolubles c'est-à-dire celles obtenues par extensions successives d'algèbres abéliennes.

Toutes nos algèbres de Lie sont de dimension finie sur un corps k de caractéristique nulle.

Définition 2.1 *Une algèbre de Lie est un k-espace vectoriel $\mathfrak{g}$ muni d'une application bilinéaire antisymétrique à valeurs dans $\mathfrak{g}$ notée $[.,.]$ vérifiant l'identité de Jacobi : pour tout $X, Y, Z \in \mathfrak{g}$,*

$$[X,[Y,Z]] = [[X,Y],Z] + [Y,[X,Z]]$$

Exemples fondamentaux - L'algèbre de Lie d'un groupe de Lie G, c'est-à-dire l'espace des champs de vecteurs invariants par translation à gauche, est une $\mathbb{R}$-algèbre de Lie. Rappelons que toute $\mathbb{R}$-algèbre de Lie $\mathfrak{g}$ est l'algèbre de Lie d'un groupe de Lie connexe et simplement connexe. Celui-ci est uniquement déterminé par $\mathfrak{g}$.

- L'algèbre de Lie $\mathrm{End}(k^d)$ avec le crochet $[A,B] = AB - BA$. Remarquons que, même si nous n'utiliserons pas ce fait, toute algèbre de Lie s'identifie à une sous-algèbre de Lie de $\mathrm{End}(V)$, par le théorème d'Ado.

- Un endomorphisme $D \in \mathrm{End}(\mathfrak{g})$ d'une algèbre de Lie $\mathfrak{g}$ est une *dérivation* si

$$D([Y,Z]) = [DY,Z] + [Y,DZ], \quad \text{pour tout } Y, Z \in \mathfrak{g}.$$

L'ensemble $\mathrm{Der}(\mathfrak{g})$ des dérivations de $\mathfrak{g}$ est une sous-algèbre de Lie de $\mathrm{End}(\mathfrak{g})$. Pour tout X dans $\mathfrak{g}$, on note $\mathrm{ad}X$ la *dérivation intérieure* donnée par $\mathrm{ad}X(Y) = [X,Y]$, pour tout $Y \in \mathfrak{g}$. L'application $\mathrm{ad} : \mathfrak{g} \to \mathrm{Der}\mathfrak{g}$ est un morphisme d'algèbres de Lie, i.e. $\mathrm{ad}[X,Y] = [\mathrm{ad}X, \mathrm{ad}Y]$, pour tout $X, Y \in \mathfrak{g}$. Ce morphisme est appelé le morphisme *adjoint*, son noyau est le centre $\mathfrak{z}$ de $\mathfrak{g}$, $\mathfrak{z} := \{X \in \mathfrak{g} \mid [X,\mathfrak{g}] = 0\}$. Historiquement, le mot *dérivation* est un raccourci pour l'expression "dérivation d'un groupe à un paramètre d'automorphismes".

Définition 2.2 *Un idéal de $\mathfrak{g}$ est un sous-espace $\mathfrak{h}$ tel que $[\mathfrak{g},\mathfrak{h}] \subset \mathfrak{h}$.*

Une algèbre de Lie $\mathfrak{g}$ est abélienne si $[\mathfrak{g},\mathfrak{g}] = 0$. Elle est nilpotente (resp. résoluble) si il existe un drapeau d'idéaux $0 = \mathfrak{g}_0 \subset \cdots \subset \mathfrak{g}_i \subset \cdots \subset \mathfrak{g}_p = \mathfrak{g}$ tels que $[\mathfrak{g},\mathfrak{g}_i] \subset \mathfrak{g}_{i-1}$ (resp. $\mathfrak{g}_i/\mathfrak{g}_{i-1}$ est abélienne), pour tout $i = 1, \ldots, p$.

Exemples fondamentaux - L'algèbre de Lie $\mathfrak{a}_d \subset \mathrm{End}(k^d)$ des matrices diagonales est abélienne.

- L'algèbre de Lie $= \mathfrak{u}_d^+ \subset \mathrm{End}(k^d)$ des matrices strictement triangulaires supérieures est nilpotente.

- L'algèbre de Lie $\mathfrak{p}_d^+ = \mathfrak{a}_d \oplus \mathfrak{u}_d^+$ des matrices triangulaires supérieures est résoluble.

Les deux théorèmes suivants expliquent en quoi ces exemples sont fondamentaux.

Théorème 2.3 (Engel) *Soit V un k-espace vectoriel de dimension d et $\mathfrak{g} \subset \mathrm{End}(V)$ une sous-algèbre de Lie dont tout élément est nilpotent. Alors il existe une base de V telle que $\mathfrak{g} \subset \mathfrak{u}_d^+$.*

Remarque L'algèbre de Lie $\mathfrak{g} = \mathbb{C}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est nilpotente, car abélienne, mais ses éléments ne sont pas nilpotents.

Démonstration On procède par récurrence sur $\dim \mathfrak{g}$. Il suffit de trouver un vecteur v dans V annulé par $\mathfrak{g}$.

On remarque tout d'abord que, pour $X \in \mathfrak{g}$, $\mathrm{ad}X$ est nilpotent. En effet, pour tout $Y \in \mathrm{End}V$,

$$(\mathrm{ad}X)^n(Y) = \textstyle\sum_{0 \leq r \leq n} (-1)^r C_n^r X^{n-r} Y X^r$$

est nul pour $n \geq 2 \dim V$.

Soit $\mathfrak{h} \subsetneq \mathfrak{g}$ une sous-algèbre de Lie maximale. L'hypothèse de récurrence appliquée à l'action adjointe de $\mathfrak{h}$ dans $\mathfrak{g}/\mathfrak{h}$ prouve qu'il existe un sous-espace $\mathfrak{h}' = kX \oplus \mathfrak{h}$ de $\mathfrak{g}$ tel que $[\mathfrak{h}, \mathfrak{h}'] \subset \mathfrak{h}$. Comme $[X, X] = 0$, $\mathfrak{h}'$ est une sous-algèbre de Lie de $\mathfrak{g}$. Par maximalité de $\mathfrak{h}$, on a $\mathfrak{h}' = \mathfrak{g}$ et $\mathfrak{h}$ est un idéal de codimension 1 dans $\mathfrak{g}$.

Posons alors $W = \{w \in V \mid \mathfrak{h}w = 0\}$. C'est un sous-espace $\mathfrak{g}$-invariant de V. Il suffit de prendre v dans le noyau de la restriction de X à W. □

Théorème 2.4 (Lie) *Soient K un corps algébriquement clos, V un K-espace vectoriel de dimension d et $\mathfrak{g} \subset \mathrm{End}(V)$ une sous-algèbre de Lie résoluble. Alors il existe une base de V telle que $\mathfrak{g} \subset \mathfrak{p}_d^+$.*

Remarque L'algèbre de Lie $\mathfrak{g} = \mathbb{R}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est résoluble, car abélienne, mais elle ne stabilise pas de droite dans $\mathbb{R}^2$.

Démonstration En procédant par récurrence sur $\dim V$, il suffit de trouver dans V une droite $\mathfrak{g}$-invariante. Soient $\mathfrak{h}$ un idéal de codimension 1 de $\mathfrak{g}$ et $X \in \mathfrak{g} \smallsetminus \mathfrak{h}$. En raisonnant par récurrence sur $\dim \mathfrak{g}$, on peut supposer qu'il existe un vecteur

$v_0 \in V$ et une forme linéaire $\lambda \in \mathfrak{h}^*$ tels que, pour tout $H \in \mathfrak{h}$, on a $Hv_0 = \lambda(H)v_0$. Posons $v_i = X^i v_0$ et notons W l'espace vectoriel engendré par tous les v_i. On vérifie par récurrence sur i que $Hv_i - \lambda(H)v_i$ est combinaison linéaire de $v_0, \ldots, v_{i-1}$. En particulier, W est $\mathfrak{h}$-invariant. On en déduit que $\lambda([H,X]) = \frac{1}{\dim W} tr_W([H,X]) = 0$. On peut alors préciser le calcul précédent par récurrence sur i et obtenir $Hv_i = \lambda(H)v_i$, pour tout $H \in \mathfrak{h}$. Il suffit alors de prendre pour v un vecteur propre de X dans W. Un tel vecteur existe car K est algébriquement clos. □

2.2 Algèbres de Lie semisimples

Comme pour les algèbres associatives de dimension finie, ce sont les algèbres de Lie semisimples qui sont à la fois les plus utiles, les plus subtiles et les mieux comprises.

Définition 2.5 *La forme de Killing $B = B_{\mathfrak{g}}$ d'une algèbre de Lie $\mathfrak{g}$ est la forme bilinéaire symétrique sur $\mathfrak{g}$ donnée par $B(X,Y) = tr_{\mathfrak{g}}(\mathrm{ad}X \mathrm{ad}Y)$.*

Le radical $\mathfrak{r}$ de $\mathfrak{g}$ est le plus grand idéal résoluble de $\mathfrak{g}$.

Remarques - Le radical $\mathfrak{r}$ existe. En effet, la somme de deux idéaux résolubles de $\mathfrak{g}$ est encore un idéal résoluble.

- Le radical $\mathfrak{r}$ est invariant par toute dérivation D de $\mathfrak{g}$. En effet, on peut pour le vérifier, supposer $k = \mathbb{C}$. Mais $\mathfrak{r}$ est invariant par tous les automorphismes de $\mathfrak{g}$ et en particulier par les automorphismes e^{tD}, pour tout $t \in k$.

Définition 2.6 *Une algèbre de Lie $\mathfrak{g}$ est semisimple si tout idéal abélien de $\mathfrak{g}$ est nul.*

Une algèbre de Lie $\mathfrak{g}$ est simple si 0 et $\mathfrak{g}$ sont les seuls idéaux de $\mathfrak{g}$ et si $\dim \mathfrak{g} > 1$.

Voici d'autres définitions équivalentes pour les algèbres de Lie semisimples

Théorème 2.7 *Les quatre affirmations suivantes sont équivalentes*
i) Tout idéal abélien de $\mathfrak{g}$ est nul.
ii) Le radical $\mathfrak{r}$ est nul.
iii) $\mathfrak{g}$ est une somme directe d'idéaux simples $\mathfrak{g} = \oplus_i \mathfrak{g}_i$.
iv) La forme de Killing $B_{\mathfrak{g}}$ est non dégénérée.

Remarques - Comme corollaire, *la semisimplicité est invariante par changement de corps de base* : pour toute extension de corps $k \subset K$, une k-algèbre de Lie $\mathfrak{g}$ est semisimple ssi son extension $\mathfrak{g} \otimes_k K$ est une K-algèbre de Lie semisimple.

- Comme autre corollaire, *une algèbre de Lie semi-simple $\mathfrak{g}$ n'a qu'un nombre fini d'idéaux simples* : ce sont les $\mathfrak{g}_i$. En effet, si $\mathfrak{a}$ est un idéal simple différent de tous les $\mathfrak{g}_i$, on a $[\mathfrak{a}, \mathfrak{g}_i] \subset \mathfrak{a} \cap \mathfrak{g}_i = 0$ et donc $\mathfrak{a}$ est dans le centre de $\mathfrak{g}$. Contradiction.

Lemme 2.8 *Soit $\mathfrak{a}$ un idéal d'une algèbre de Lie $\mathfrak{g}$.*
a) L'orthogonal $\mathfrak{a}^\perp := \{X \in \mathfrak{g} \mid B(X, \mathfrak{a}) = 0\}$ est un idéal de $\mathfrak{g}$.
b) La forme de Killing de $\mathfrak{a}$ est la restriction de celle de $\mathfrak{g}$.

Démonstration du lemme 2.8
a) Cela résulte de l'égalité $B([X,Y],Z) + B(Y,[X,Z]) = 0$, pour $X, Y, Z \in \mathfrak{g}$.
b) Cela résulte de l'inclusion $\mathrm{ad}X\mathrm{ad}Y(\mathfrak{g}) \subset \mathfrak{a}$, pour $X, Y \in \mathfrak{a}$. □

Démonstration du théorème 2.7
i) $\Rightarrow$ *ii)* Si $\mathfrak{r} \neq 0$, on pose $D^0\mathfrak{r} = \mathfrak{r}$, $D^{j+1}\mathfrak{r} = [D^j\mathfrak{r}, D^j\mathfrak{r}]$. Le dernier *idéal dérivé* non nul $D^j\mathfrak{r}$ est un idéal abélien de $\mathfrak{g}$.

iii) $\Rightarrow$ *iv)* Comme $[\mathfrak{g}_i, \mathfrak{g}_j] = 0$ et, par suite, $B(\mathfrak{g}_i, \mathfrak{g}_j) = 0$ pour $i \neq j$, on peut supposer $\mathfrak{g}$ simple. Remarquons qu'on a $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$ car, comme $\dim \mathfrak{g} > 1$, $\mathfrak{g}$ ne peut pas être abélienne. Le noyau de la forme de Killing B est un idéal de $\mathfrak{g}$. Il est soit nul, soit égal à $\mathfrak{g}$.

Il suffit de montrer que B est non nul. C'est le point le plus délicat de la démonstration. Supposons par l'absurde que B est nul. On note $A = \mathrm{ad}\mathfrak{g}$ et $M := \{\varphi \in \mathrm{End}\mathfrak{g} \mid [\varphi, A] \subset A\}$.

Montrons que, pour $a \in A$ et $\varphi \in M$, on a $tr(\varphi a) = 0$. On peut pour cela supposer que $a = [b, c]$ avec $b, c \in A$, car on a $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$ et donc $A = [A, A]$. On a alors $tr(\varphi a) = tr([\varphi, b]c) = 0$ car la forme de Killing est nulle.

Comme A est inclus dans M, le lemme ci-dessous prouve que tout élément de A est nilpotent, donc par le théorème de Engel, l'algèbre de Lie A est nilpotente. Contradiction.

iv) $\Rightarrow$ *i)* Soit $\mathfrak{a}$ un idéal abélien de $\mathfrak{g}$. On a $B(\mathfrak{a}, \mathfrak{g}) = 0$, donc $\mathfrak{a} = 0$.

ii) $\Rightarrow$ *iii)* Par récurrence sur $\dim \mathfrak{g}$. Soit $\mathfrak{a}$ un idéal non nul minimal de $\mathfrak{g}$. D'après les remarques suivant la définition 2.5, le radical résoluble de $\mathfrak{a}$ est un idéal de $\mathfrak{g}$. Il est donc nul. Par l'implication *iii)* $\Rightarrow$ *iv)*, la forme de Killing de $\mathfrak{a}$ est non dégénérée. On en déduit que $\mathfrak{g} = \mathfrak{a} \oplus \mathfrak{a}^\perp$ et que la forme de Killing de l'idéal $\mathfrak{a}^\perp$ est non dégénérée. Par récurrence, $\mathfrak{a}^\perp$ est une somme directe d'idéaux simples et $\mathfrak{g}$ aussi. □

On a utilisé le

Lemme 2.9 *Soit $V = k^d$, A un k-sous-espace vectoriel de* End$V$ *et $M = \{\varphi \in$ End$V \mid [\varphi, A] \subset A\}$. Soit $\psi \in M$ tel que, pour tout $\varphi \in M$, on a $tr(\varphi\psi) = 0$. Alors ψ est nilpotent.*

Démonstration On peut supposer que $k = \mathbb{C}$. Ecrivons $\psi = \psi_s + \psi_n$ la décomposition de Jordan de ψ. On peut supposer ψ_s diagonale et ψ_n strictement triangulaire supérieure. L'égalité $\mathrm{ad}(\psi) = \mathrm{ad}(\psi_s) + \mathrm{ad}(\psi_n)$ est aussi la décomposition de Jordan de $\mathrm{ad}(\psi)$. La partie semisimple ψ_s est donc aussi dans M. Son conjugué $\varphi = \overline{\psi_s}$ est aussi dans M. On a alors, en notant λ_i les valeurs propres de ψ, $\sum_i |\lambda_i|^2 = tr(\varphi\psi) = 0$. Donc $\psi_s = 0$. □

Proposition 2.10 *Toute dérivation d'une algèbre de Lie semisimple* $\mathfrak{g}$ *est intérieure.*

Démonstration L'algèbre de Lie $\mathfrak{a} := \mathrm{ad}\mathfrak{g}$ est un idéal de l'algèbre de Lie $\mathfrak{d} := \mathrm{Der}\mathfrak{g}$ car on a l'égalité $[D, \mathrm{ad}X] = \mathrm{ad}(DX)$, pour tout $D \in \mathfrak{d}$ et $X \in \mathfrak{g}$. Notons $\mathfrak{a}^\perp$ l'orthogonal dans $\mathfrak{d}$ de $\mathfrak{a}$ pour la forme de Killing de $\mathfrak{d}$. Comme la forme de Killing de $\mathfrak{a}$ est non dégénérée, on a l'égalité $\mathfrak{d} = \mathfrak{a} \oplus \mathfrak{a}^\perp$.

Il suffit pour conclure de montrer que tout élément $D \in \mathfrak{a}^\perp$ est nul. Cela résulte de l'égalité, $\mathrm{ad}(DX) = [D, \mathrm{ad}X] \in \mathfrak{a} \cap \mathfrak{a}^\perp = 0$, pour tout $X \in \mathfrak{g}$ et de l'injectivité de l'application adjointe. □

Comme l'application adjointe $\mathrm{ad} : \mathfrak{g} \to \mathrm{Der}\mathfrak{g}$ est injective, cette proposition permet d'identifier $\mathfrak{g}$ avec l'algèbre de Lie $\mathrm{Der}\mathfrak{g}$ des dérivations de $\mathfrak{g}$. C'est très utile car cela permet de voir toute algèbre de Lie semisimple comme l'algèbre de Lie d'un groupe *algébrique* : le groupe de ses automorphismes. Voici une application utile de ce fait.

Définition 2.11 *Un élément* X *d'une algèbre de Lie semisimple est dit nilpotent si l'endomorphisme* $\mathrm{ad}X$ *est nilpotent. Un élément* X *est dit semisimple si* $\mathrm{ad}X$ *est semisimple.*

Proposition 2.12 (décomposition de Jordan) *Soit* $\mathfrak{g}$ *une algèbre de Lie semisimple. Tout élément* X *de* $\mathfrak{g}$ *admet une décomposition unique* $X = X_s + X_n$ *avec* X_s *semisimple,* X_n *nilpotent et* $[X_s, X_n] = 0$.

Démonstration

Unicité La décomposition de Jordan de $\mathrm{ad}X$ est $\mathrm{ad}(X_s) + \mathrm{ad}(X_n)$.

Existence Il suffit de voir que la partie semisimple $(\mathrm{ad}X)_s$ de $\mathrm{ad}X$ est une dérivation car la proposition 2.10 prouvera qu'il existe X_s dans $\mathfrak{g}$ tel que $\mathrm{ad}(X_s) = (\mathrm{ad}X)_s$.

On peut supposer $k = \mathbb{C}$. Soit $\mathfrak{g}_\lambda = \bigcup_{p\geq 1} \mathrm{Ker}((\mathrm{ad}X - \lambda)^p)$ de sorte que $\mathfrak{g} = \oplus_{\lambda\in\mathbb{C}}\mathfrak{g}_\lambda$. L'élément $(\mathrm{ad}X)_s$ agit sur $\mathfrak{g}_\lambda$ par multiplication par λ. Il suffit donc de vérifier que $[\mathfrak{g}_\lambda, \mathfrak{g}_\mu] \subset \mathfrak{g}_{\lambda+\mu}$. Ce qui résulte de la formule suivante que l'on démontre par récurrence sur p :

$$(\mathrm{ad}X - \lambda - \mu)^p[Y, Z] = \textstyle\sum_{0\leq r\leq p} C_p^r[(\mathrm{ad}X - \lambda)^r Y, (\mathrm{ad}X - \mu)^{p-r} Z]$$

pour tout $X, Y, Z \in \mathfrak{g}$. □

Remarque Lorsque $k = \mathbb{R}$, Un élément X de $\mathfrak{g}$ est dit *elliptique* (resp. *hyperbolique*) si $\mathrm{ad}X$ est semisimple à valeurs propres imaginaires pures (resp. réelles). On a encore une écriture unique $X = X_e + X_h + X_n$ avec X_e elliptique, X_h hyperbolique et X_n nilpotent qui commutent deux à deux.

2.3 Représentations de $\mathfrak{sl}_2$

L'algèbre de Lie $\mathfrak{s} = \mathfrak{sl}(2,k)$ est une algèbre de Lie simple de dimension minimale. Son étude est fondamentale car, sur un corps algébriquement clos, toute algèbre de Lie semisimple contient de nombreuses copies de $\mathfrak{s}$.

Définition 2.13 *Une représentation d'une k-algèbre de Lie $\mathfrak{g}$ dans un k-espace vectoriel V est un morphisme de $\mathfrak{g}$ dans* End$V$. *On dit aussi que V est un $\mathfrak{g}$-module.*

Elle est dite simple ou irréductible si les seuls sous-espaces $\mathfrak{g}$-invariants sont 0 *ou V.*

Exemples fondamentaux - La représentation adjointe ad.

- L'algèbre de Lie $\mathfrak{s} = \mathfrak{sl}(2,k)$ admet, pour tout $d \geq 0$, une représentation dans le k-espace vectoriel V_d de dimension $d+1$ des polynômes homogènes de degré d sur k^2. Décrivons plus précisément ces représentations. Une base de l'algèbre de Lie $\mathfrak{s} = \mathfrak{sl}(2,k)$ est X, H, Y avec

$$X := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \; H := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \; Y := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

qui vérifient les relations

$$[H,X] = 2X \;, \;\; [H,Y] = -2Y \;\text{ et }\; [X,Y] = H.$$

L'action de cette base dans V_d est donnée par $X \to x\frac{\partial}{\partial y}$, $H \to x\frac{\partial}{\partial x} - y\frac{\partial}{\partial y}$ et $Y \to y\frac{\partial}{\partial x}$. Cette représentation de $\mathfrak{s}$ dans V_d est appelée la *représentation de plus haut poids* d car d y est la plus grande valeur propre de H.

Proposition 2.14 *Soit V un $\mathfrak{sl}(2,k)$-module de dimension finie.*
a) V est somme directe de représentations simples.
b) Si V est simple alors V est isomorphe à une des représentations V_d de plus haut poids d.

On représente parfois V_d par un diagramme "ficelles" formé de $d+1$ noeuds labellés par les valeurs propres $-d, -d+2, \ldots, d-2, d$ de H, les ficelles symbolisant l'action de X et Y sur les vecteurs propres de H correspondant.

Démonstration a) Nous allons utiliser un argument transcendant appelé *l'astuce unitaire* de Weyl. Il suffit de montrer que tout sous-espace $\mathfrak{s}$-invariant $V' \subset V$ admet un supplémentaire V'' $\mathfrak{s}$-invariant. Notons $p : V \to V/V'$ la projection naturelle. On peut supposer que le corps de base est $\mathbb{C}$ car l'ensemble

$$\{\sigma \in \mathrm{Hom}_{\mathfrak{s}}(V/V', V) \mid p \circ \sigma = Id\}$$

est un espace affine défini sur k : s'il a un point à coefficients dans une extension de k il en a aussi un à coefficients dans k. En effet, tout système d'équations

affines à coefficients dans k qui a des solutions dans une extension de k en a aussi dans k.

Notons alors $K = \mathrm{SU}(2)$ le groupe spécial unitaire

$$K := \{\begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \mid a, b \in \mathbb{C}\ ,\ \ |a|^2 + |b|^2 = 1\}$$

Son algèbre de Lie $\mathfrak{k} = \{\text{matrices antihermitiennes de trace nulle}\}$ est une forme réelle de $\mathfrak{s}$ i.e. $\mathfrak{s} \simeq \mathfrak{k} \otimes_{\mathbb{R}} \mathbb{C}$. Comme K est simplement connexe, toute représentation de $\mathfrak{s}$ s'intègre donc en une représentation de K. Munissons V, grâce à la mesure de Haar de K, d'un produit scalaire hermitien K-invariant. Il suffit de prendre pour V'' l'orthogonal de V'. Ce sous-espace est K-invariant. Il est donc aussi $\mathfrak{s}$-invariant.

b) Décomposons V en somme directe $V = \oplus_{\mu \in \mathbb{C}} V_\mu$ de sous-espaces caractéristiques de H pour la valeur propre μ. On a

$$X(V_\mu) \subset V_{\mu+2} \ \text{ et } \ Y(V_\mu) \subset V_{\mu-2}$$

car on a les formules dans $\mathrm{End}V$, pour tout $j \geq 1$,

$$(H - \mu - 2)^j X = X(H - \mu)^j \ \text{ et } \ (H - \mu + 2)^j Y = Y(H - \mu)^j.$$

Soit v_0 un vecteur propre de H pour une valeur propre λ de partie réelle maximum. On a $Hv_0 = \lambda v_0$ et $Xv_0 = 0$.

Soit $n \geq 0$ tel que $Y^n v_0 \neq 0$ et $Y^{n+1} v_0 = 0$. et posons $v_i = Y^i v_0$, pour $i \geq 0$.

Par récurrence, on a la formule dans $\mathrm{End}V$,

$$[X, Y^{j+1}] = (j+1) Y^j (H - j).$$

Donc, on a $0 = XY^{n+1} v_0 = (n+1)(\lambda - n) v_n$. On a donc $\lambda = n$. Cette même formule permet de calculer, pour $0 \leq i \leq n$,

$$Yv_i = v_{i+1}\ \ , \quad Hv_i = (n - 2i)v_i\ \ , \quad Xv_i = (n - i + 1) i v_{i-1}.$$

Comme Vest simple, $v_0, \ldots, v_n$ est une base de V. On reconnait le $\mathfrak{s}$-module V_n à l'aide de l'identification $v_i \mapsto n(n-1)\cdots(n-i+1) x^{n-i} y^i$.

Réciproquement, il est facile de vérifier que V_n est un $\mathfrak{s}$-module simple. □

2.4 Eléments nilpotents et $\mathfrak{sl}_2$-triplets

> Une des raisons qui rend très utile la classification des représentations de $\mathfrak{sl}_2$ est la théorie des $\mathfrak{sl}_2$-triplets.

Un triplet (x, h, y) dans une algèbre de Lie qui vérifie les relations de commutation $[h, x] = 2x\ ,\ \ [h, y] = -2y$ et $[x, y] = h$ est appelé un $\mathfrak{sl}_2$-triplet.

Théorème 2.15 (Jacobson, Morozov) *Tout élément nilpotent x d'une algèbre de Lie semisimple $\mathfrak{g}$ fait partie d'un $\mathfrak{sl}_2$-triplet (x, h, y).*

Commençons par un lemme.

Lemme 2.16 *Soient X et Z deux éléments de* $\mathrm{End}(k^d)$ *tels que X est nilpotent et $[X,[X,Z]]=0$. Alors le produit XZ est nilpotent.*

Démonstration du lemme 2.16 On peut supposer le corps k algébriquement clos. Soit $W := [X,Z]$. Comme X et W commutent, on a, pour tout $p \geq 1$, $W^p = [X, ZW^{p-1}]$ et donc $tr(W^p) = 0$. Par suite, W est nilpotent.

Remarquons que $[X^p, Z] = pWX^{p-1}$. Soit v un vecteur propre de XZ pour la valeur propre λ et p le plus petit entier tel que $X^p v = 0$. Cet entier existe car X est nilpotent. On a $\lambda X^{p-1}v = X^pZv = pWX^{p-1}v$. Donc λ/p est une valeur propre de W qui est nilpotent. Donc $\lambda = 0$ et XZ est nilpotent. □

Démonstration du théorème 2.15

Construction de h L'endomorphisme $(\mathrm{ad}x)^2$ est autoadjoint pour la forme de Killing de $\mathfrak{g}$, c'est-à-dire que, pour $y, z \in \mathfrak{g}$, on a

$$B((\mathrm{ad}x)^2 y, z) = B(y, (\mathrm{ad}x)^2 z).$$

D'autre part, d'après le lemme 2.16, pour tout z dans le noyau N_2 de $(\mathrm{ad}x)^2$, le produit $\mathrm{ad}x\,\mathrm{ad}z$ est nilpotent et donc $B(x,z) = 0$. C'est-à-dire que x est dans l'orthogonal $N_2^\perp$ de N_2 pour la forme de Killing. Comme B est non dégénérée, $N_2^\perp$ est aussi l'image de $(\mathrm{ad}x)^2$. Il existe donc $y' \in \mathfrak{g}$ tel que, en notant $h = [x, y']$, on a $[h, x] = 2x$.

Construction de y Notons $u := [h, y'] + 2y'$. On aimerait que u soit nul. Par Jacobi, on a $[x, u] = 0$. On cherche donc un élément $z := y' - y$ de $\mathfrak{g}$ tel que $[x, z] = 0$ et $[h, z] + 2z = u$. Remarquons que le noyau N_1 de $\mathrm{ad}x$ est invariant par $\mathrm{ad}h$ car $[h, x] = 2x$. Il suffit donc de voir que -2 n'est pas valeur propre de $\mathrm{ad}h$ dans N_1. Cela résulte du lemme suivant. □

Lemme 2.17 *Soient $X, H, Y' \in \mathrm{End}(k^d)$ trois matrices telles que $[X, Y'] = H$ et $[H, X] = 2X$. Alors les valeurs propres de H dans le noyau* $\mathrm{Ker}X$ *sont des entiers positifs.*

Démonstration On peut supposer k algébriquement clos. On reprend la partie de la démonstration de la classification des $\mathfrak{sl}(2,k)$-modules simples qui est encore valable pour (X, H, Y') :

On montre par récurrence sur $p \geq 0$ que $[Y', X^{p+1}] = (p+1)X^p(H - p)$. Soit v un vecteur non nul du noyau de X qui est vecteur propre de H pour la valeur propre λ. Comme v est dans le noyau de X, il existe un plus grand entier $p \geq 0$ tel que v soit dans l'image de X^p. Notons u un vecteur tel que $X^p u = v$. On a l'égalité $(p+1)(\lambda - p)v = X^{p+1}(Y'u)$. Donc on a $\lambda = p$. □

2.5 Systèmes de racines

Dans cette section $\mathfrak{g}$ est une algèbre de Lie semisimple complexe. Nous rappelons maintenant la structure de $\mathfrak{g}$. Les deux outils clefs sont la construction de $\mathfrak{sl}_2$-triplets à l'aide de la forme de Killing et la classification des représentations de $\mathfrak{sl}(2)$.

Définition 2.18 *Une sous-algèbre de Cartan $\mathfrak{h}$ de $\mathfrak{g}$ est une sous-algèbre commutative formée d'éléments semisimples et qui est maximale pour ces propriétés.*

L'intérêt de cette notion, est qu'on peut diagonaliser simultanément $\mathfrak{g}$ sous l'action adjointe des éléments de $\mathfrak{h}$: pour $\alpha \in \mathfrak{h}^*$, on pose

$$\mathfrak{g}_\alpha = \{X \in \mathfrak{g} \mid [H, X] = \alpha(H)X \text{ pour tout } H \in \mathfrak{h}\}.$$

L'ensemble

$$\Delta = \{\alpha \in \mathfrak{h}^* \mid \mathfrak{g}_\alpha \neq 0 \text{ et } \alpha \neq 0\}$$

est appelé le *système de racines* de $\mathfrak{g}$. L'espace $\mathfrak{g}_\alpha$ associé à une racine $\alpha \in \Delta$ est appelé l'espace *radiciel*. On a la décomposition

$$\mathfrak{g} = \mathfrak{g}_0 \oplus (\oplus_{\alpha\in\Delta}\, \mathfrak{g}_\alpha)\,.$$

Définition 2.19 *Soit E un espace vectoriel réel muni d'un produit scalaire euclidien $\langle .,. \rangle$. Pour $\alpha \in E$, $\alpha \neq 0$ on note s_α la symétrie orthogonale $s_\alpha : E \to E; \beta \mapsto \beta - 2\frac{\langle \alpha,\beta\rangle}{\langle \alpha,\alpha\rangle}\alpha$. On appelle "système de racines abstrait" une partie Δ telle que, pour tout $\alpha, \beta \in \Delta$, on a $2\frac{\langle \alpha,\beta\rangle}{\langle \alpha,\alpha\rangle} \in \mathbb{Z}$ et $s_\alpha(\beta) \in \Delta$.*

Le système de racines abstrait Δ est dit "réduit" si $\alpha \in \Delta \Rightarrow 2\alpha \notin \Delta$.

Le théorème suivant affirme en particulier que le système de racines de $\mathfrak{g}$ est un système de racines abstrait.

Théorème 2.20 *Soit $\mathfrak{g}$ une algèbre de Lie semisimple complexe.*
a) On a $\mathfrak{g}_0 = \mathfrak{h}$. En particulier, $\mathfrak{h}$ est commutative maximale.
b) $\Delta = -\Delta$ et la forme de Killing B restreinte à $\mathfrak{h}$ est non dégénérée.
c) Pour $\lambda \in \mathfrak{h}^*$, on note $H_\lambda \in \mathfrak{h}$ l'élément tel que $B(H_\lambda, H) = \lambda(H)$ pour tout $H \in \mathfrak{h}$. Alors, pour tout $X_{\pm\alpha} \in \mathfrak{g}_{\pm\alpha}$, on a $[X_{-\alpha}, X_\alpha] = B(X_{-\alpha}, X_\alpha)H_\alpha$.
d) Pour tout $\alpha \in \Delta$, on a $\alpha(H_\alpha) \neq 0$. Notons $H'_\alpha := \frac{2H_\alpha}{\alpha(H_\alpha)}$ et choisissons $X'_\alpha \in \mathfrak{g}_\alpha$ tels que $B(X'_\alpha, X'_{-\alpha}) = \frac{2}{\alpha(H_\alpha)}$. Alors $(X'_\alpha, H_\alpha, X'_{-\alpha})$ est un $\mathfrak{sl}_2$-triplet.
e) i) $\dim \mathfrak{g}_\alpha = 1$ *pour tout $\alpha \in \Delta$.*
ii) $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] = \mathfrak{g}_{\alpha+\beta}$ pour tout $\alpha, \beta \in \Delta$.
iii) α et $-\alpha$ sont les seules racines proportionnelles à α.
f) La forme B est définie positive sur $\mathfrak{h}_\mathbb{R} := \sum_{\alpha\in\Delta} \mathbb{R}H_\alpha$ et on a $\mathfrak{h} = \mathfrak{h}_\mathbb{R} \oplus i\mathfrak{h}_\mathbb{R}$.
g) Δ est un système de racines abstrait réduit de l'espace euclidien dual $E = \mathfrak{h}^*_\mathbb{R}$.

Remarques - On a $E = \sum_{\alpha\in\Delta} \mathbb{R}\alpha$ et le produit scalaire sur E est donné par $\langle\alpha,\beta\rangle = B(H_\alpha, H_\beta)$, pour tout $\alpha,\beta \in E$.

- Nous verrons que toutes les sous-algèbres de Cartan sont conjuguées. Donc, à chaque algèbre de Lie semisimple complexe est associé un unique système de racines abstrait réduit.

- On appelle *rang* de $\mathfrak{g}$ ou *rang* de Δ, la dimension r de E.

- Réciproquement, on peut montrer que tout système de racines abstrait réduit provient d'une unique algèbre de Lie semisimple complexe. En outre, on peut classifier les systèmes de racines abstraits.

Démonstration Nous utiliserons fréquemment l'inclusion $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] \subset \mathfrak{g}_{\alpha+\beta}$.

a) Soit $X \in \mathfrak{g}_0$. Notons $X = X_s + X_n$ sa décomposition de Jordan (voir proposition 2.12). Comme X_s commute à $\mathfrak{h}$, X_s est dans $\mathfrak{h}$. On peut donc supposer que $X = X_n$ est nilpotent. Par le théorème 2.15 de Jacobson Morozov, il existe $H \in \mathfrak{g}$ tel que $[H, X] = 2X$. Quitte à remplacer H par sa projection sur $\mathfrak{g}_0$ parallèlement à $[\mathfrak{h}, \mathfrak{g}]$, on peut supposer que H est dans $\mathfrak{g}_0$. Notons $H = H_s + H_n$ la décomposition de Jordan de H. L'élément H_s commute encore à $\mathfrak{h}$, il est donc dans $\mathfrak{h}$. Ce qui contredit l'égalité $[H_s, X] = 2X$. Sauf si $X = 0$. Donc $\mathfrak{g}_0 = \mathfrak{h}$.

b) On a $B(\mathfrak{g}_\alpha, \mathfrak{g}_\beta) = 0$ si $\alpha + \beta \neq 0$. Comme B est non dégénérée, B induit une dualité non dégénérée entre $\mathfrak{g}_\alpha$ et $\mathfrak{g}_{-\alpha}$.

c) En effet, $B([X_\alpha, X_{-\alpha}], H) = B(X_\alpha, [X_{-\alpha}, H]) = B(X_\alpha, X_{-\alpha})\alpha(H)$.

d) Si $\alpha(H) = 0$. On choisit $X_{\pm\alpha} \in \mathfrak{g}_{\pm\alpha}$ tels que $B(X_\alpha, X_{-\alpha}) = 1$. Alors on a $[H_\alpha, X_\alpha] = [H_\alpha, X_{-\alpha}] = 0$ et $[X_\alpha, X_{-\alpha}] = H_\alpha$. Le théorème de Lie appliqué à l'algèbre de Lie résoluble $\mathbb{R}X_{-\alpha} \oplus \mathbb{R}H_\alpha \oplus \mathbb{R}X_\alpha$ prouve que H_α est nilpotent. Donc $H_\alpha = 0$. Contradiction.

Comme $\alpha(H'_\alpha) = 2$, on a bien $[H'_\alpha, X'_\alpha] = 2X'_\alpha$, $[H'_\alpha, X'_{-\alpha}] = -2X'_{-\alpha}$ et $[X'_\alpha, X'_{-\alpha}] = H'_\alpha$. On note $\mathfrak{g}_\alpha$ la sous-algèbre de Lie de $\mathfrak{g}$ engendrée par ce $\mathfrak{sl}_2$-triplet.

e) *i*) Si $\dim \mathfrak{g}_\alpha \geq 2$, il existe $X''_\alpha \in \mathfrak{g}_\alpha$ un élément tel que $B(X'_{-\alpha}, X''_\alpha) = 0$. Mais alors $[X'_{-\alpha}, X''_\alpha] = 0$ et X''_α engendre un $\mathfrak{s}_\alpha$-module de plus bas poids 2. Cela n'existe pas d'après la proposition 2.14.

ii) Si $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] = 0$. La somme $V' := \oplus_{n\in\mathbb{N}}\ \mathfrak{g}_{\beta-n\alpha}$ est un $\mathfrak{s}_\alpha$-sous-module de la somme $V := \oplus_{n\in\mathbb{Z}}\ \mathfrak{g}_{\beta+n\alpha}$. Ce sous-module V' a pour plus haut poids $\beta(H'_\alpha)$ et V/V' a pour plus bas poids $\beta(H'_\alpha) + 2$. Donc, d'après la proposition 2.14, on a $\beta(H'_\alpha) \geq 0$ et $\beta(H'_\alpha) + 2 \leq 0$. Contradiction.

iii) Quitte à remplacer α par $\alpha/2$, on peut supposer que $\alpha/2$ n'est pas une racine. On peut décomposer le $\mathfrak{s}_\alpha$-module $V := \oplus_{z\in\mathbb{C}}\ \mathfrak{g}_{z\alpha}$ en modules ficelles. Comme 1 n'est pas valeur propre de H'_α et que 2 est une valeur propre de multiplicité 1, on a d'après la proposition 2.14, $V = \mathfrak{g}_{-\alpha} \oplus \mathfrak{g}_0 \oplus \mathfrak{g}_\alpha$.

f) Montrons que la restriction de B à $\mathfrak{h}_\mathbb{R}$ est positive. Pour tout $H \in \mathfrak{h}_\mathbb{R}$, on a

$$B(H,H) = \textstyle\sum_{\alpha\in\Delta} \alpha(H)^2 = \sum_{\alpha\in\Delta} B(H_\alpha, H)^2 \qquad (1)$$

Il suffit donc de voir que, pour $\alpha, \beta \in \Delta$, $B(H_\alpha, H_\beta)$ est réel. Or

$$B(H_\alpha, H_\beta) = \beta(H_\alpha) = \tfrac{1}{2}\alpha(H_\alpha)\beta(H'_\alpha).$$

Comme H'_α fait partie d'un $\mathfrak{sl}_2$-triplet, ses valeurs propres $\beta(H'_\alpha)$ sont dans $\mathbb{Z}$. Il reste à voir que $\alpha(H_\alpha)$ est réel. Cela résulte des égalités

$$\alpha(H_\alpha) = B(H_\alpha, H_\alpha) = \tfrac{1}{4}\alpha(H_\alpha)^2 B(H'_\alpha, H'_\alpha) = \tfrac{1}{4}\alpha(H_\alpha)^2 \textstyle\sum_{\beta\in\Delta} \beta(H'_\alpha)^2.$$

Remarquons maintenant que Δ engendre $\mathfrak{h}^*$. En effet, si un élément $H \in \mathfrak{h}$ est dans le noyau de toutes les racines, il est dans le centre de $\mathfrak{g}$ et donc $H = 0$.

Montrons que B est non dégénérée sur $\mathfrak{h}_\mathbb{R}$. En effet, d'après (1), un élément $H \in \mathfrak{h}_\mathbb{R}$ tel que $B(H, H) = 0$ serait dans le noyau de toutes les racines et serait donc nul.

On en déduit que B est défini négatif sur $i\mathfrak{h}_\mathbb{R}$. Donc on a $\mathfrak{h}_\mathbb{R} \cap i\mathfrak{h}_\mathbb{R} = 0$, puis, comme Δ engendre $\mathfrak{h}$, on en déduit $\mathfrak{h} = \mathfrak{h}_\mathbb{R} \oplus i\mathfrak{h}_\mathbb{R}$.

c) L'espace $E = \mathfrak{h}^*_\mathbb{R}$ est euclidien et on a l'équivalence $\lambda \in E \Leftrightarrow H_\lambda \in \mathfrak{h}_\mathbb{R}$. En particulier Δ est inclus dans E et engendre E. Montrons que Δ est un système de racines abstrait. Soient $\alpha, \beta \in \Delta$, $q = 2\frac{\langle\alpha,\beta\rangle}{\langle\alpha,\alpha\rangle}$. On doit vérifier que $q \in \mathbb{Z}$ et que $\beta - q\alpha \in \Delta$. On peut supposer $q \geq 0$. Il résulte de la proposition 2.14 appliqué au $\mathfrak{s}_\alpha$-module $V := \oplus_{n\in\mathbb{Z}}\, \mathfrak{g}_{\beta+n\alpha}$ que la valeur propre $q = \beta(H'_\alpha)$ est un entier et que $(\mathrm{ad}X'_{-\alpha})^q(X'_\beta) \neq 0$. En effet, les valeurs propres de H'_α dans les modules ficelles sont entières et symétriques par rapport à l'origine. Donc $\mathfrak{g}_{\beta-q\alpha}$ est non nul et $\beta - q\alpha$ est une racine. □

Donnons pour finir la liste de toutes les algèbres de Lie simples complexes, liste qui se déduit de celle des systèmes de racines abstraits. Les quatre familles dites *classiques* et les cinq algèbres simples dites *exceptionnelles*

$$\begin{array}{ll} A_r = \mathfrak{sl}(r+1, \mathbb{C}) & (r \geq 1), \\ B_r = \mathfrak{so}(2r+1, \mathbb{C}) & (r \geq 2), \\ C_r = \mathfrak{sp}(r, \mathbb{C}) & (r \geq 3), \\ D_r = \mathfrak{so}(2r, \mathbb{C}) & (r \geq 4) \\ E_6,\ E_7,\ E_8,\ F_4,\ G_2. & \end{array}$$

3 Groupes de Lie semisimples

Nous démontrons entièrement dans ce chapitre un certains nombres de résultats classiques dûs à E. Cartan sur la structure des groupes et des algèbres de Lie semisimples. En particulier, l'existence d'une involution de Cartan, la décomposition de Cartan $G = KA^+K$ et la décomposition d'Iwasawa $G = KAU^+$. Résultats que nous utilisons à plusieurs reprises dans ce cours. Comme dans le cas complexe, le language des systèmes de racines permet de gérer tous les groupes de Lie semisimples réels. Néanmoins, nous rappellerons la signification de ces concepts pour $G = \mathrm{SL}(d, \mathbb{R})$.

3.1 Groupes de Lie compacts

Commençons par la descriptions des groupes de Lie compacts.

Pour tout groupe de Lie U, on note $\mathfrak{u} = \mathrm{Lie}(U)$ son algèbre de Lie et $\mathfrak{u}_{\mathbb{C}} := \mathfrak{u} \otimes_{\mathbb{R}} \mathbb{C}$ son algèbre de Lie comlexifiée. On note Ad l'action adjointe : pour $u \in U$, Adu est la dérivée de la conjugaison $g \mapsto ugu^{-1}$. Ad est un morphisme de groupes de Lie de U dans le groupe des automorphismes $\mathrm{Aut}(\mathfrak{u})$.

Théorème 3.1 *L'application $U \to \mathfrak{u}_{\mathbb{C}}$ met en bijection*

$$\left\{ \begin{array}{c} \textit{groupes de Lie compacts} \\ \textit{connexes à centre trivial} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{algèbres de Lie} \\ \textit{semisimples complexes} \end{array} \right\}.$$

Remarques - Il s'agit bien sûr d'une bijection "modulo isomorphisme" ou, plus précisément d'une "équivalence de catégories".

- On en déduit, avec la section 2.5, que tout groupe simple compact est, modulo le centre, un des groupes classiques $A_r = \mathrm{SU}(r+1)$, $B_r = \mathrm{SO}(2r+1)$, $C_r = \mathrm{Sp}(r)$, $D_r = \mathrm{SO}(2r)$ ou un des cinq groupes exceptionnels E_6, E_7, E_8,F_4, G_2.

Démonstration du théorème 3.1 Comme AdU est compact, il existe une forme bilinéaire définie positive B_0 sur $\mathfrak{u}$ qui est AdU-invariante. Pour tout $X \in \mathfrak{u}$ non nul, ad$X$ est antisymétrique pour B_0, donc $tr((\mathrm{ad}X)^2) < 0$. La forme de Killing B de $\mathfrak{u}$ est définie négative. Donc $\mathfrak{u}$ est semisimple et $\mathfrak{u}_{\mathbb{C}}$ aussi.

L'injectivité de l'application $U \to \mathfrak{u}_{\mathbb{C}}$ sera montrée dans la section 3.2.

On va montrer dans cette partie la surjectivité. □

Soit $\mathfrak{g}$ une algèbre de Lie semisimple complexe.

Définition 3.2 *On appelle forme réelle de $\mathfrak{g}$ une sous-algèbre de Lie réelle $\mathfrak{g}_{\mathbb{R}}$ telle que $\mathfrak{g} = \mathfrak{g}_{\mathbb{R}} \otimes_{\mathbb{R}} \mathbb{C}$. Une forme réelle $\mathfrak{g}_{\mathbb{R}}$ est dite compacte si la forme de Killing de $\mathfrak{g}_{\mathbb{R}}$ est définie négative.*

Il suffit de montrer que $\mathfrak{g}$ a une forme réelle compacte $\mathfrak{u}$. Car alors la composante connexe $U := \mathrm{Aut}(\mathfrak{u})_e$ du groupe des automorphismes de $\mathfrak{u}$ convient. C'est un groupe compact car il est fermé et préserve la forme de Killing. Son algèbre de Lie est isomorphe à $\mathfrak{u}$ car toute dérivation de $\mathfrak{u}$ est intérieure.

Pour montrer que $\mathfrak{g}$ a une forme réelle compacte, reprenons les notations de la section 2.5. Pour $\alpha \in \Delta$, choisissons X_α dans $\mathfrak{g}_\alpha$ tels que $[X_{-\alpha}, X_\alpha] = H_\alpha$ et définissons, pour $\alpha, \beta \in \Delta$ avec $\alpha + \beta \neq 0$, le nombre $N_{\alpha,\beta}$ par

$$[X_\alpha, X_\beta] = N_{\alpha,\beta} X_{\alpha+\beta} \text{ si } \alpha+\beta \text{ est dans } \Delta \text{ et par } N_{\alpha,\beta} = 0 \text{ sinon.}$$

Proposition 3.3 *On peut choisir les X_α de sorte que $N_{\alpha,\beta} = -N_{-\alpha,-\beta}$.*
Les nombres $N_{\alpha,\beta}$ sont alors réels.

Grace à cette proposition, on peut prendre pour forme réelle compacte de $\mathfrak{g}$

$$\mathfrak{u} = i\mathfrak{h}_{\mathbb{R}} \oplus (\oplus_{\alpha\in\Delta} \mathbb{R} i(X_\alpha + X_{-\alpha})) \oplus (\oplus_{\alpha\in\Delta} \mathbb{R}(X_\alpha - X_{-\alpha})) \,.$$

En effet, par construction, les facteurs de cette somme directe sont orthogonaux et B est donc définie négative sur $\mathfrak{u}$. Les égalités $N_{\alpha,\beta} = -N_{-\alpha,-\beta} \in \mathbb{R}$ assurent que $\mathfrak{u}$ est une algèbre de Lie.

Remarque Pour $\mathfrak{g} = \mathfrak{sl}(2,\mathbb{C})$, on obtient la base de $\mathfrak{su}(2)$

$$iH = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix},\ i(X+Y) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},\ X-Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Lemme 3.4 *a) Pour $\alpha, \beta \in \Delta$, on a $N_{\alpha,\beta} = -N_{\beta,\alpha}$.*
b) Pour $\alpha, \beta, \gamma \in \Delta$ avec $\alpha+\beta+\gamma = 0$, on a

$$N_{\alpha,\beta} = N_{\beta,\gamma} = N_{\gamma,\alpha} \quad \textit{et} \quad N_{\alpha,\beta} N_{-\alpha,-\beta} < 0.$$

c) Pour $\alpha, \beta, \gamma, \delta \in \Delta$ non deux à deux colinéaires, on a

$$N_{\alpha,\beta} N_{\gamma,\delta} + N_{\beta,\gamma} N_{\alpha,\delta} + N_{\gamma,\alpha} N_{\beta,\delta} = 0.$$

Démonstration du lemme 3.4 a) Clair.

b) Comme $\alpha+\beta+\gamma = 0$, on a $H_\alpha + H_\beta + H_\gamma = 0$. Or, l'identité de Jacobi appliquée à X_α, X_β, X_γ donne $N_{\beta,\gamma} H_\alpha + N_{\gamma,\alpha} H_\beta + N_{\alpha,\beta} H_\gamma = 0$. Donc $N_{\alpha,\beta} = N_{\beta,\gamma} = N_{\gamma,\alpha}$.

D'autre part, la proposition 2.14 qui classifie les $\mathfrak{sl}(2)$-modules prouve que $[X'_{-\alpha}, [X'_\alpha, X_\beta]] = a_{\alpha,\beta} X_\beta$ où $a_{\alpha,\beta}$ est un entier strictement positif. On en déduit que $N_{\alpha,\beta} N_{-\alpha,\alpha+\beta} > 0$.

c) Appliquer l'identité de Jacobi à $X_\alpha, X_\beta, X_\gamma$.

Démonstration de la proposition 3.3 Choisissons un ordre total sur $\mathfrak{h}^*_{\mathbb{R}}$ tel que la somme de deux éléments positifs est positif ; par exemple l'ordre lexicographique pour les coordonnées dans une base de $\mathfrak{h}^*_{\mathbb{R}}$. On note $\Delta^+ = \{\alpha \in \Delta \mid \alpha > 0\}$ l'ensemble des racines positives.

Pour $\rho \in \Delta^+$, posons $\Delta_\rho = \{\alpha \in \Delta \mid -\rho \leq \alpha \leq \rho\}$ et montrons par récurrence sur $\#\Delta_\rho$ qu'on peut choisir les X_α, pour $\alpha \in \Delta_\rho$ tels que

$$N_{\alpha,\beta} = -N_{-\alpha,-\beta} \quad \text{pour tout} \ \ \alpha, \beta, \alpha+\beta \in \Delta_\rho \tag{2}$$

Le nombre $N_{\alpha,\beta}$ est alors automatiquement réel par b).

Par hypothèse de récurrence, il ne reste à choisir que X_ρ car $X_{-\rho}$ s'en déduit.

Si on ne peut pas écrire $\rho = \gamma + \delta$ avec $\gamma, \delta \in \Delta^+$, on choisit X_ρ arbitrairement.

Si on peut écrire $\rho = \gamma + \delta$ avec $\gamma, \delta \in \Delta^+$, on prend $X_\rho = \lambda[X_\gamma, X_\delta]$ et $X_{-\rho} = \lambda[X_{-\gamma}, X_{-\delta}]$ où $\lambda \in \mathbb{C}^*$ est choisi de sorte que $B(X_\rho, X_{-\rho}) = 1$. Il reste à vérifier (2). Grace à b), il suffit de vérifier (2) lorsque $\alpha + \beta = \rho$. Ce qui résulte de l'égalité du c) appliquée à $\alpha, \beta, -\gamma, -\delta$ et à $-\alpha, -\beta, \gamma, \delta$ et de l'hypothèse de récurrence. □

Remarque On peut montrer que tout groupe topologique compact simple connexe est de Lie. Le théorème 3.1 donne donc la classification des groupes *compacts connexes* simples. C'est un des grands achèvement du début du vingtième siècle. Il ouvre la voie à la classification des groupes *finis* simples. Signalons que c'est seulement à la fin du vingtième siècle que cette dernière sera complétée.

3.2 Involutions de Cartan

> Ce sont les involutions de Cartan qui nous permettront de comprendre la structure des groupes de Lie semisimples et leurs liens avec les espaces symétriques.

Définition 3.5 *Une involution de Cartan d'une algèbre de Lie semisimple réelle* $\mathfrak{g}$ *est un automorphisme* θ *tel que* $\theta^2 = 1$ *et tel que la forme bilinéaire symétrique* B_θ *donnée par* $B_\theta(X, Y) = B(\theta X, Y)$ *est définie positive.*

On a alors la *décomposition de Cartan* $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{q}$ où $\mathfrak{k} = \{X \in \mathfrak{g} \mid \theta(X) = X\}$ et $\mathfrak{q} = \{X \in \mathfrak{g} \mid \theta(X) = -X\}$. Ces sous-espaces $\mathfrak{k}$ et $\mathfrak{q}$ sont orthogonaux pour la forme de Killing B qui est définie négative sur $\mathfrak{k}$ et définie positive sur $\mathfrak{q}$.

Exemples - Pour $\mathfrak{g} = \mathfrak{sl}(d, \mathbb{R})$ ou $\mathfrak{g} = \mathfrak{so}(p, q)$, on peut prendre $\theta(X) = -{}^tX$.

- L'algèbre de Lie $\mathfrak{g}_\mathbb{C}$ considérée comme une algèbre de Lie réelle admet comme involution de Cartan la conjugaison σ par rapport à une forme réelle compacte $\mathfrak{u}$. On a alors $\mathfrak{k} = \mathfrak{u}$ et $\mathfrak{q} = i\mathfrak{u}$.

Proposition 3.6 *a) Toute algèbre de Lie semisimple réelle* $\mathfrak{g}$ *admet une involution de Cartan* θ*.*
b) Deux involutions de Cartan θ *et* θ_1 *de* $\mathfrak{g}$ *sont toujours conjuguées.*

Remarques - *Conjugué* signifie "*conjugué par un élément de* $\mathrm{Aut}(\mathfrak{g})_e$*"*.

- Le point b) prouve l'injectivité de l'application $U \to \mathfrak{u}_\mathbb{C}$ du théorème 3.1.

Démonstration de la proposition 3.6 a) Soient τ la conjugaison complexe par rapport à $\mathfrak{g}$ et N l'automorphisme de $\mathfrak{g}_\mathbb{C}$ produit $N = \sigma\tau$ où σ est comme dans l'exemple. Pour tout $X, Y \in \mathfrak{g}$, on a

$$B_\sigma(NX, Y) = B(\tau X, Y) = B(X, \tau Y) = B_\sigma(X, NY).$$

Donc N est semisimple à valeurs propres réelles. Soit P l'élément $P := N^2$. On peut donc écrire $P = P^1$ pour un groupe à un paramètre $t \to P^t$ de bjections linéaires de l'espace vectoriel réel $\mathfrak{g}_{\mathbb{C}}$ qui sont semisimples à valeurs propres positives. Pour tout t, P^t est dans $\mathrm{Aut}(\mathfrak{g}_{\mathbb{C}})$, P^t commute à N et on a $\sigma P^t \sigma^{-1} = P^{-t}$. En effet, cela résulte de la remarque du lemme 4.9 car ces affirmations sont polynomiales et vraies pour t entiers. On pose alors $Q = P^{-\frac{1}{4}}$ et $\sigma' = Q\sigma Q^{-1}$. On calcule

$$\sigma'\tau = Q\sigma Q^{-1}\tau = Q^2\sigma\tau = P^{-\frac{1}{2}}N = N^{-1}P^{\frac{1}{2}} = \tau\sigma Q^{-2} = \tau Q\sigma Q^{-1} = \tau\sigma'.$$

On en déduit que $\sigma'(\mathfrak{g}) \subset \mathfrak{g}$ et que $\theta := \sigma'|_{\mathfrak{g}}$ est une involution de Cartan de $\mathfrak{g}$.

b) Comme en a), on peut poser $Q := ((\theta\theta_1)^2)^{-\frac{1}{4}} \in \mathrm{Aut}(\mathfrak{g})$, $\theta' := Q\theta_1 Q^{-1}$ et prouver que θ et θ' commutent.

On diagonalise alors simultanément θ et θ' : on a

$$\mathfrak{g} = (\mathfrak{k} \cap \mathfrak{k}') \oplus (\mathfrak{k} \cap \mathfrak{q}') \oplus (\mathfrak{q} \cap \mathfrak{k}') \oplus (\mathfrak{q} \cap \mathfrak{q}')$$

où $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{q}$ et $\mathfrak{g} = \mathfrak{k}' \oplus \mathfrak{q}'$ sont les décompositions de Cartan de $\mathfrak{g}$ pour θ et θ'. La forme de Killing est définie négative sur $\mathfrak{k}$ et $\mathfrak{k}'$ et est définie positive sur $\mathfrak{q}$ et $\mathfrak{q}'$. Donc, on a $\mathfrak{k} \cap \mathfrak{q}' = \mathfrak{q} \cap \mathfrak{k}' = 0$, puis $\mathfrak{k} = \mathfrak{k}'$ et $\mathfrak{q} = \mathfrak{q}'$, c'est-à-dire $\theta = \theta'$. □

Remarques - Les éléments de $\mathfrak{k}$ sont elliptiques. Ceux de $\mathfrak{q}$ sont hyperboliques.

- Notons $G = \mathrm{Aut}(\mathfrak{g})_e$ le groupe de Lie connexe à centre trivial d'algèbre de Lie $\mathfrak{g}$. Le sous groupe $K = \{g \in G \mid g\theta = \theta g\}$ est donc un sous-groupe compact maximal de G. L'espace G/K, muni de la métrique riemannienne G-invariante donnée par la forme de Killing sur $\mathfrak{q}$ est un "espace symétriques riemanniens simplement connexe à courbure négative ou nulle sans facteur euclidien". L'application $\mathfrak{g} \longleftrightarrow G/K$ est une bijection entre les algèbres de Lie semisimples réelles et ces espace symétriques. Cette bijection est due à E. Cartan.

3.3 Sous-algèbres de Cartan

Soit $\mathfrak{g}$ une algèbre de Lie semisimple réelle.

Définition 3.7 *Une sous-algèbre de Cartan $\mathfrak{h}$ de $\mathfrak{g}$ est une sous-algèbre commutative formée d'éléments semisimples et maximale pour cette propriété.*

Proposition 3.8 *Soit $\mathfrak{h}$ une sous-algèbre de Cartan de $\mathfrak{g}$ et θ une involution de Cartan de $\mathfrak{g}$. Alors*
a) La complexifiée $\mathfrak{h}_{\mathbb{C}}$ est une sous-algèbre de Cartan de $\mathfrak{g}_{\mathbb{C}}$.
b) Il existe un conjugué de $\mathfrak{h}$ qui est θ-stable.

Démonstration a) La démonstration du théorème 2.20.a est valable pour $k = \mathbb{R}$. Donc $\mathfrak{h}$ est commutative maximale et $\mathfrak{h}_{\mathbb{C}}$ aussi.

b) D'après la proposition 3.6, il suffit de construire une involution de Cartan θ' de $\mathfrak{g}$ telle que $\theta'(\mathfrak{h}) = \mathfrak{h}$. Soit $\mathfrak{u}$ une forme réelle compacte de $\mathfrak{g}_{\mathbb{C}}$ construite à partir de $\mathfrak{h}_{\mathbb{C}}$ par la méthode de la section 3.1. Notons σ (resp. τ) la conjugaison complexe par rapport à $\mathfrak{u}$ (resp. $\mathfrak{g}$). Comme dans la proposition 3.6.a, on peut poser $Q := ((\sigma\tau)^2)^{-\frac{1}{4}}$, $\sigma' := Q \circ \sigma \circ Q^{-1}$, $\theta' := \sigma'|_{\mathfrak{g}}$ et montrer que θ' est une involution de Cartan de $\mathfrak{g}$. Comme $Q(\mathfrak{h}_{\mathbb{C}}) = \mathfrak{h}_{\mathbb{C}}$, on a $\theta'(\mathfrak{h}) = \mathfrak{h}$. □

3.4 Sous-espaces de Cartan

Soit $\mathfrak{g}$ une algèbre de Lie semisimple réelle.

Définition 3.9 *Un sous-espace de Cartan $\mathfrak{a}$ de $\mathfrak{g}$ est une sous-algèbre commutative formée d'éléments hyperboliques et maximale pour cette propriété.*

Par définition tout élément hyperbolique fait partie d'un sous-espace de Cartan.

On peut diagonaliser $\mathfrak{g}$ sous l'action adjointe de $\mathfrak{a}$. On désigne par Σ l'ensemble des *racines restreintes*, i.e. l'ensemble des poids non triviaux pour cette action. Comme en 2.5, la théorie des $\mathfrak{sl}_2$-triplets permet de montrer que Σ est un système de racines abstrait (pas toujours réduit). On a une décomposition

$$\mathfrak{g} = \mathfrak{l} \oplus (\oplus_{\lambda\in\Sigma}\, \mathfrak{g}_\lambda), \quad \text{où}$$

$$\mathfrak{g}_\lambda := \{Y \in \mathfrak{g} \,/\, \forall X \in \mathfrak{a}\ ,\ \mathrm{ad}X(Y) = \lambda(X)Y\}$$

est l'espace radiciel associé à λ et $\mathfrak{l}$ est le centralisateur de $\mathfrak{a}$.

Soient $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{q}$ une décomposition de Cartan associée à une involution de Cartan θ et $K := \{g \in \mathrm{Aut}(\mathfrak{g}) \mid \theta g = g\theta\}$. Ce groupe K est compact et son algèbre de Lie est $\mathfrak{k}$.

Proposition 3.10 *a) Tout sous-espace de Cartan $\mathfrak{a}$ de $\mathfrak{g}$ est conjugué à un sous-espace de Cartan inclus dans $\mathfrak{q}$.*
b) Deux sous-espaces de Cartan inclus dans $\mathfrak{q}$ sont toujours conjugués par un élément de K_e.

Démonstration a) Mettons $\mathfrak{a}$ dans une sous-algèbre de Cartan $\mathfrak{h}$ de $\mathfrak{g}$. On peut supposer grâce à la proposition 3.8 que $\mathfrak{h}$ est θ-stable. Mais alors $\mathfrak{h} = (\mathfrak{h} \cap \mathfrak{k}) \oplus (\mathfrak{h} \cap \mathfrak{q})$. Comme $\mathfrak{h} \cap \mathfrak{q}$ est l'ensemble des éléments hyperboliques de $\mathfrak{h}$, on a $\mathfrak{a} \subset \mathfrak{q}$.

b) Soient $\mathfrak{a}_1$, $\mathfrak{a}_2$ deux sous-espaces de Cartan dans $\mathfrak{q}$. Choisissons $X_i \in \mathfrak{a}_i$ en dehors des noyaux des racines restreintes de sorte qu'un élément X de $\mathfrak{g}$ qui commute à X_i commute aussi à $\mathfrak{a}_i$.

On peut supposer que la fonction définie sur K $g \mapsto B(X_1, gX_2)$ atteint son minimum pour $g = e$. On a alors, pour tout $Z \in \mathfrak{k}$, $B(X_1, [Z, X_2]) = 0$ et donc $B(Z, [X_1, X_2]) = 0$. Comme $[X_1, X_2]$ est dans $\mathfrak{k}$, on en déduit $[X_1, X_2] = 0$, puis $[\mathfrak{a}_1, \mathfrak{a}_2] = 0$ et enfin $\mathfrak{a}_1 = \mathfrak{a}_2$. □

Corollaire 3.11 *Soit $\mathfrak{g}_{\mathbb{C}}$ (resp. $\mathfrak{g}$, $\mathfrak{u}$) une algèbre de Lie semisimple complexe (resp. réelle, réelle compacte).*
a) Toutes les sous-algèbres de Cartan de $\mathfrak{u}$ sont conjuguées.
b) Toutes les sous-algèbres de Cartan de $\mathfrak{g}_{\mathbb{C}}$ sont conjuguées.
c) $\mathfrak{g}$ n'a qu'un nombre fini de classes de conjugaison de sous-algèbres de Cartan.

La dimension commune des sous-algèbres (resp. sous-espaces) de Cartan de $\mathfrak{g}$ est appelé le *rang* (resp. *rang réel*) de $\mathfrak{g}$.

Démonstration a) L'égalité $\mathfrak{u}_{\mathbb{C}} = \mathfrak{u} \oplus i\mathfrak{u}$ est une décomposition de Cartan. Si $\mathfrak{t}$ est un sous-algèbre de Cartan de $\mathfrak{u}$, $i\mathfrak{t}$ est un sous-espace de Cartan de $\mathfrak{u}_{\mathbb{C}}$ inclus dans $i\mathfrak{u}$. On peut donc appliquer la proposition 3.10.b.

b) Soient $\mathfrak{h}_1$ et $\mathfrak{h}_2$ deux sous-algèbres de Cartan de $\mathfrak{g}_{\mathbb{C}}$. D'après la construction du théorème 3.1, il existe des formes réelles compactes $\mathfrak{u}_i$ telles que $\mathfrak{t}_i := \mathfrak{u}_i \cap \mathfrak{h}_i$ est une sous-algèbre de Cartan de $\mathfrak{u}_i$. D'après la proposition 3.6, on peut supposer $\mathfrak{u}_1 = \mathfrak{u}_2$. On applique alors le a).

c) Fixons un sous-espace de Cartan $\mathfrak{a}$ dans $\mathfrak{p}$. Chaque classe de conjugaison contient une sous-algèbre de Cartan θ-stable $\mathfrak{h}_1$. D'après la proposition 3.10.b, on peut supposer que $\mathfrak{a}_1 := \mathfrak{h}_1 \cap \mathfrak{q}$ est inclus dans $\mathfrak{a}$. Soient $\Sigma_1 := \{\lambda \in \Sigma \mid \lambda(\mathfrak{a}_1) = 0\}$ et $\mathfrak{a}_1' := \{X \in \mathfrak{a}_1 \mid \lambda(X) = 0 \text{ pour tout } \lambda \in \Sigma_1\}$. Comme $\mathfrak{a}_1'$ contient $\mathfrak{a}_1$ et que tout élément de $\mathfrak{a}_1'$ commute au commutant de $\mathfrak{a}_1$, par maximalité de $\mathfrak{h}_1$, on a $\mathfrak{a}_1 = \mathfrak{a}_1'$. Donc $\mathfrak{a}_1$ est entièrement déterminé par Σ_1 qui ne peut prendre qu'un nombre fini de valeurs.

Il reste à comprendre que, si $\mathfrak{h}_2$ est une autre sous-algèbre de Cartan θ-stable telle que $\mathfrak{h}_2 \cap \mathfrak{q} = \mathfrak{a}_1$, alors $\mathfrak{h}_1$ et $\mathfrak{h}_2$ sont conjuguées. Soient $\mathfrak{m}_1$ le centralisateur de $\mathfrak{a}_1$ dans $\mathfrak{k}$, $\mathfrak{z}_1$ le centre de $\mathfrak{m}_1$ et $\mathfrak{m}_1' = \mathfrak{m}_1/\mathfrak{z}_1$. L'algèbre de Lie $\mathfrak{m}_1'$ est semisimple compacte et les $\mathfrak{t}_i' := (\mathfrak{h}_i \cap \mathfrak{k})/\mathfrak{z}_1$ sont des sous-algèbres de Cartan de $\mathfrak{m}_1'$. Le a) permet alors de conclure. □

Notons Σ^+ un système de racines positives de Σ, c'est à dire une partie de Σ telle que $\Sigma^+ \cap -\Sigma^+ = \emptyset$, $\Sigma^+ \cup -\Sigma^+ = \Sigma$ et $(\Sigma^+ + \Sigma^+) \cap -\Sigma^+ = \emptyset$.

L'ensemble Π des racines simples de Σ^+, c'est à dire des éléments minimaux de Σ^+, est une base de $\mathfrak{a}^\star$. Les sous algèbres $\mathfrak{u}^\pm := \oplus_{\lambda \in \Sigma^\pm} \mathfrak{g}_\lambda$ sont nilpotentes et la sous-algèbre $\mathfrak{p} = \mathfrak{l} \oplus \mathfrak{u}^+$ est appelée la *sous-algèbre parabolique minimale* associée à Σ^+.

Lemme 3.12 *On a la décomposition d'Iwasawa $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{a} \oplus \mathfrak{u}^+$.*

Démonstration Cela résulte de l'égalité $\theta(\mathfrak{g}_\lambda) = \mathfrak{g}_{-\lambda}$.

3.5 Décomposition de Cartan et Iwasawa

Soit G un groupe de Lie semisimple connexe de centre fini d'algèbre de Lie $\mathfrak{g}$. On garde les notations ci-dessus. On a, en particulier, choisi une involution de

Cartan θ de G, un sous-espace de Cartan $\mathfrak{a} \subset \mathfrak{q}$ et un système de racines positives Σ^+. Notons $\mathfrak{a}^+ := \{X \in \mathfrak{a} \ / \ \forall \alpha \in \Sigma^+ \ , \ \alpha(X) \geq 0\}$ la *chambre de Weyl* dans $\mathfrak{a}$ associée à Σ^+.

Notons K l'ensemble des points fixes de θ dans G et $A := \exp(\mathfrak{a})$. Par définition, le *rang réel* de G est la dimension de A. L'ensemble des caractères réels du groupe de Lie A peut être identifié au dual $\mathfrak{a}^\star$. Notons aussi

$$A^+ := \{a \in A \ / \ \forall \alpha \in \Sigma^+ \ , \ \alpha(a) \geq 1\}$$

la *chambre de Weyl* dans A associée à Σ^+.

On a la *décomposition de Cartan.*

Théorème 3.13
a) L'application $K \times \mathfrak{q} \to G; (k, X) \mapsto ke^X$ est un difféomorphisme.
b) On a l'égalité $G = KA^+K$.

Démonstration On peut supposer G à centre trivial i.e. $G = \mathrm{Aut}(\mathfrak{g})_e$.

a) C'est la même que pour $\mathrm{SL}(d, \mathbb{R})$. On veut écrire $g = kq$ avec $k \in K$ et $q \in \exp(\mathfrak{q})$. Comme $\theta(g)^{-1}g$ est symétrique définie positive pour la forme B_θ, on peut écrire $\theta(g)^{-1}g = e^{2X}$ avec e^{tX} groupe à un paramètre de matrices symétriques définies positives. On utilise encore la remarque du lemme 4.9 pour conclure que le groupe à un paramètre e^{tX} est dans G. On prend $q = e^X$ et $k = gq^{-1}$.

b) Utiliser le a) et la proposition 3.10 qui assure que tout élément de $\mathfrak{q}$ est conjugué sous K à un élément de $\mathfrak{a}$. Utiliser enfin la théorie des petits $\mathfrak{sl}_2$ qui permet, pour $\lambda \in \Sigma$, de relever les symétries s_λ en des éléments du normalisateur de $\mathfrak{a}$ dans K et donc de conjuguer tout élément de $\mathfrak{a}$ en un élément de la chambre de Weyl $\mathfrak{a}^+$. □

Le normalisateur $P := N_G(\mathfrak{p})$ est appelé le *sous-groupe parabolique minimal* associé à Σ^+. Notons L le centralisateur de $\mathfrak{a}$ dans G et $U^\pm$ les sous-groupes connexes d'algèbre de Lie $\mathfrak{u}^\pm$.

On a la *décomposition d'Iwasawa.*

Théorème 3.14
a) La multiplication donne un difféomorphisme $K \times A \times U^+ \simeq G$.
b) Le quotient P/AU^+ est compact.
c) La multiplication $m : U^- \times P \to G$ est un difféomorphisme sur un ouvert de mesure pleine.

Un élément g de G est dit *hyperbolique* si on peut écrire $g = e^X$ avec $X \in \mathfrak{g}$ hyperbolique i.e. si il est conjugué à un élément de A.

Un élément g de G est dit *unipotent* si on peut écrire $g = e^X$ avec $X \in \mathfrak{g}$ nilpotent i.e. si il est conjugué à un élément de U^+.

Un élément g de G est dit *elliptique* si il est conjugué à un élément de K.

Démonstration du théorème 3.14 On peut supposer G à centre trivial.

a) Notons W le groupe résoluble $W = AU^+$ et $\mathfrak{w}$ son algèbre de Lie. Comme $A \cap U^+ = \{e\}$, la multiplication $A \times U^+ \to W$ est un difféomorphisme.

Comme $\mathfrak{w}$ ne contient pas d'élément elliptique, $\mathfrak{w}$ ne rencontre aucun conjugué de $\mathfrak{k}$ et donc, les doubles classes KgW sont ouvertes. Elles sont donc aussi fermées. Donc $G = KW$. Comme W ne contient pas de sous-groupe compact, on a $K \cap W = \{e\}$.

b) Comme AU^+ est inclus dans P, ce la résulte du a).

c) On montre tout d'abord une version complexifiée de cette assertion. Notons $G_{\mathbb{C}} = \mathrm{Aut}(\mathfrak{g}_{\mathbb{C}})$, $U^{\pm}_{\mathbb{C}}$ les sous-groupes connexes d'algèbre de Lie $\mathfrak{u}^{\pm}_{\mathbb{C}} =: \mathfrak{u}^{\pm} \otimes_{\mathbb{R}} \mathbb{C}$ et $P_{\mathbb{C}}$ le normalisateur de $\mathfrak{p}_{\mathbb{C}} := \mathfrak{p} \otimes_{\mathbb{R}} \mathbb{C}$. L'intersection $P_{\mathbb{C}} \cap U^-_{\mathbb{C}}$ est triviale car l'action adjointe d'un élément g de $P_{\mathbb{C}} \cap U^-_{\mathbb{C}}$ doit préserver les $\mathfrak{p}_{\mathbb{C}}$-sous-modules et les $\mathfrak{u}^-_{\mathbb{C}}$-sous-modules de $\mathfrak{g}_{\mathbb{C}}$, il doit donc préserver tous les espaces radiciels complexifiés $(\mathfrak{g}_\lambda)_{\mathbb{C}}$ et agir trivialement dessus. Comme en outre $\mathfrak{u}^-_{\mathbb{C}} \oplus \mathfrak{p}_{\mathbb{C}} = \mathfrak{g}_{\mathbb{C}}$, La multiplication $m_{\mathbb{C}} : U^-_{\mathbb{C}} \times P_{\mathbb{C}} \to G_{\mathbb{C}}$ est injective d'image ouverte. Comme ces groupes sont algébriques, d'après la proposition 4.4, l'image est un ouvert de Zariski. Par injectivité de $m_{\mathbb{C}}$, on a $U^-P = U^-_{\mathbb{C}} P_{\mathbb{C}} \cap G$. Donc le complémentaire de U^-P est un fermé de Zariski de G. Il est donc de mesure nulle. □

3.6 Sous-groupes paraboliques

Pour toute partie $\theta \subset \Pi$, on note $<\theta>$ l'espace vectoriel engendré par θ,

$$\Sigma_\theta := \Sigma \cap <\theta> , \quad \Sigma^{\pm}_\theta := \Sigma_\theta \cap \Sigma^{\pm},$$

$$\mathfrak{l}_\theta := \mathfrak{l} \oplus \oplus_{\alpha \in \Sigma_\theta} \mathfrak{g}_\alpha , \quad \mathfrak{u}^{\pm}_\theta := \oplus_{\alpha \in \Sigma^{\pm} \setminus \Sigma^{\pm}_\theta} \mathfrak{g}_\alpha,$$

$U^{\pm}_\theta$ les groupes connexes associés, $A_\theta := \{a \in A \ / \ \forall \alpha \in \theta \ , \ \alpha(a) = 1\}$, $A^+_\theta := A^+ \cap A_\theta$, L_θ le centralisateur de A_θ dans G. Soit $\mathfrak{p}_\theta := \mathfrak{l}_\theta \oplus \mathfrak{u}^+_\theta$ and $P_\theta := L_\theta U^+_\theta$ les *sous-algèbres et sous-groupes paraboliques* associés à θ. On a alors les assertions.

Proposition 3.15 *a) Tout sous-groupe contenant P est égal à l'un des P_θ.*
b) P_θ est engendré par les sous-groupes $P_{\{\alpha\}}$ pour $\alpha \in \theta$.
c) Si $\theta_1 \subset \theta_2$, alors $\Sigma_{\theta_1} \subset \Sigma_{\theta_2}$, $P_{\theta_1} \subset P_{\theta_2}$ et $U^+_{\theta_1} \supset U^+_{\theta_2}$.

Démonstration

3.7 Exemples

Décrivons explicitement ces notations pour $G = \mathrm{SL}(d, \mathbb{R})$. On peut prendre

$K = \mathrm{SO}(d, \mathbb{R})$,
$A = \{a = \mathrm{diag}(a_1, \ldots, a_d) \ / \ a_i > 0 \ , \ a_1 \cdots a_d = 1\}$,
$A^+ = \{a \in A \ / \ a_1 \geq \cdots \geq a_d\}$,
$\Sigma = \{\varepsilon_i - \varepsilon_j \ , \ i \neq j \ , \ 1 \leq i, j \leq d\}$,
$\Sigma^+ = \{\varepsilon_i - \varepsilon_j \ , \ 1 \leq i < j \leq d\}$,
$\Pi = \{\varepsilon_{i+1} - \varepsilon_i \ , \ 1 \leq i < d\}$, où $\varepsilon_i \in \mathfrak{a}^\star$ est donné par : $\varepsilon_i(a) = a_i$,
$\mathfrak{g}_{\varepsilon_i - \varepsilon_j} = \mathbb{R}E_{i,j}$ avec $E_{i,j} = e_j^\star \otimes e_i$,
$\mathfrak{l} = \mathfrak{a}$

$$\mathfrak{u}^+ = \left\{ \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix} \right\} \quad , \quad \mathfrak{p} = \left\{ \begin{pmatrix} * & & * \\ & \ddots & \\ 0 & & * \end{pmatrix} \right\} \quad , \quad \mathfrak{u}^- = \left\{ \begin{pmatrix} 0 & & 0 \\ & \ddots & \\ * & & 0 \end{pmatrix} \right\} \quad .$$

$$\mathfrak{u}_\theta^+ = \left\{ \begin{pmatrix} 0 & * & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{pmatrix} \right\} \quad , \quad \mathfrak{p}_\theta = \left\{ \begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & 0 & * \end{pmatrix} \right\} \quad , \quad \mathfrak{u}_\theta^- = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ * & 0 & 0 \\ * & * & 0 \end{pmatrix} \right\} \quad ,$$

$$\mathfrak{l}_\theta = \left\{ \begin{pmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix} \right\} \quad , \quad A_\theta = \left\{ \begin{pmatrix} b_1 Id & 0 & 0 \\ 0 & b_2 Id & 0 \\ 0 & 0 & b_3 Id \end{pmatrix} \in A \right\} \quad ,$$

$A_\theta^+ = A_\theta \cap A^+$. On a pris θ^c avec seulement deux racines simples. Une autre partie θ aurait donné un nombre et des tailles différentes de matrices blocs.

4 Groupes algébriques

Rappelons quelques définitions de la théorie des groupes algébriques. Nous avons choisi un point de vu naïf, probablement pas suffisamment précis, intrinsèque et général pour le puriste, mais qui suffit bien pour une première approche de ce sujet... et pour les applications que nous avons en vue.

4.1 Variétés algébriques

Tout d'abord quelques mots sur les variétés algébriques.

Soient K un corps algébriquement clos de caractéristique nulle, k un sous-corps de K, $\mathbf{V}_k \sim k^d$ un k-espace vectoriel, $\mathbf{V} = K \otimes_k \mathbf{V}_k \simeq K^d$ et $k[\mathbf{V}]$ l'anneau des polynomes sur $\mathbf{V}_k$ à valeurs dans k.

Une *variété (algébrique) affine* $\mathbf{Z} \subset \mathbf{V}$ ou *fermé de Zariski* est un sous-ensemble qui est l'ensemble des zéros d'une famille de polynômes sur $\mathbf{V}$. On note $I(\mathbf{Z}) \subset K[\mathbf{V}]$ l'idéal des polynômes nuls sur $\mathbf{Z}$.

On dit que $\mathbf{Z}$ est une *k-variété* si $I(\mathbf{Z})$ est engendré par l'intersection $I_k(\mathbf{Z}) := I(\mathbf{Z}) \cap k[\mathbf{V}]$. L'anneau quotient $k[\mathbf{Z}] := k[\mathbf{V}]/I_k(\mathbf{Z})$ est l'anneau des fonctions *k-régulières* sur $\mathbf{Z}$. L'ensemble $\mathbf{Z}_k := k^d \cap \mathbf{Z}$ est l'ensemble des *k-points* de $\mathbf{Z}$.

Un *k-morphisme* ou application *k-régulière* de k-variétés $\varphi : \mathbf{Z}_1 \to \mathbf{Z}_2$ est une application telle que, pour tout f dans $k[\mathbf{Z}_2]$, la composée $f \circ \varphi$ est dans $k[\mathbf{Z}_1]$.

La *topologie de Zariski* sur $\mathbf{Z}$ est la topologie dont les fermés sont les sous-variétés de $\mathbf{Z}$. La toplogie induite sur $\mathbf{Z}_k$ s'appelle aussi *topologie de Zariski*. On parlera ainsi de parties *Zariski connexes* ou de parties *Zariski denses*.

Une variété $\mathbf{Z}$ est dite *k-irréductible* si on ne peut pas l'écrire comme réunion de deux k-sous-variétés propre ou, ce qui est équivalent, si l'anneau $k[\mathbf{Z}]$ est intègre. On note alors $k(\mathbf{Z})$ le corps des fractions de $k[\mathbf{Z}]$. Les éléments de $k(\mathbf{Z})$ sont les fonctions *k-rationnelles*. Par noethérianité de $k[\mathbf{Z}]$, toute k-variété est réunion finie de k-sous-variétés k-irréductibles.

La *dimension* $\dim \mathbf{Z}$ d'une variété k-irréductible $\mathbf{Z}$ est le degré de transcendance sur k de $k(\mathbf{Z})$. L'espace tangent $T_z\mathbf{Z}$ à $\mathbf{Z}$ en un point $z \in \mathbf{Z}$ est l'intersection des différentielles $dP(z)$ des polynômes P de l'idéal $I(\mathbf{Z})$. Un point $z \in \mathbf{Z}$ est *lisse* si $m = \dim(T_z\mathbf{Z})$ est minimum. L'ensemble des points lisses d'une k-variété est donc un ouvert de Zariski non vide défini sur k. En un point lisse z, on a $\dim(T_z\mathbf{Z}) = m = \dim \mathbf{Z}$. Autrement dit, localement au voisinage de z, $\mathbf{Z}$ s'identifie aux zéros de $d-m$ polynômes P_i tels que $T_z\mathbf{Z} = \cap_i dP_i(z)$. On dit que $\mathbf{Z}$ est *lisse* si tous ses points sont lisses.

Lorsque $\mathbf{Z}$ est lisse et que le corps de base k est $\mathbb{R}$, $\mathbb{C}$ ou une extension finie de $\mathbb{Q}_p$, i.e. k est un corps local de caractéristique nulle, l'ensemble $\mathbf{Z}_k$ des k-points de $\mathbf{Z}$ est une sous-variété k-analytique lisse de k^d de dimension $\dim \mathbf{Z}$ dont l'espace tangent en un k-point z s'identifie aux k-points de l'espace tangent en z à la k-variété $\mathbf{Z}$.

Disons, de façon heuristique, que l'intérêt de ce point de vue qui consiste à "travailler avec les points dans une clôture algébrique K mais avec des formules à coefficients dans k", est qu'il permet de développer le sujet sans savoir s'il existe des k-points.

Il est souvent utile d'étendre les définitions ci-dessus à un cadre projectif.

Ainsi une *k-variété (algébrique) projective* $\mathbf{Z} \subset \mathbb{P}(\mathbf{V})$ ou *fermé de Zariski* est un sous-ensemble qui est l'ensemble des zéros d'une famille de polynômes homogènes sur $\mathbf{V}$ à coefficients dans k. L'ensemble $\mathbf{Z}_k := \mathbb{P}(k^d) \cap \mathbf{Z}$ est l'ensemble des *k-points* de $\mathbf{Z}$. On a encore une notion d'applications k-régulières, de topologie de Zariski sur $\mathbf{Z}$ et sur $\mathbf{Z}_k$...

Une *k-variété (algébrique) quasiprojective* est un ouvert de Zariski défini sur k d'une k-variété projective.

Le théorème suivant est au coeur de la théorie de *l'élimination des quantificateurs* ou théorie des ensembles *constructibles*.

Théorème 4.1 (Chevalley) *Soit $\varphi : \mathbf{Z}_1 \to \mathbf{Z}_2$ une application régulière entre deux variétés algébriques. Alors l'image $\varphi(\mathbf{Z}_1)$ contient un ouvert de son adhérence (pour la topologie de Zariski).*

Remarque $\varphi((\mathbf{Z}_1)_k)$ ne contient pas toujours un ouvert de Zariski de l'ensemble des k-points de $\varphi(\mathbf{Z}_1)$. Par exemple $\varphi : \mathbb{R} \to \mathbb{R}; t \mapsto t^2$.

Démonstration On peut supposer que les variétés $\mathbf{Z}_1$ et $\mathbf{Z}_2$ sont affines et irréductibles sur K et que $\varphi(\mathbf{Z}_1)$ est Zariski dense dans $\mathbf{Z}_2$. L'application φ induit alors une injection entre les anneaux de fonctions régulières $A := K[\mathbf{Z}_2] \hookrightarrow B := K[\mathbf{Z}_1]$. Remarquons que la donnée d'un point x de $\mathbf{Z}_1$ équivaut à la donnée d'un morphisme d'anneaux $\psi : B \to K$: le morphisme donné par $\psi(P) = P(x)$ pour tout $P \in B$. Le théorème est donc une conséquence du lemme suivant. □

Lemme 4.2 *Soit $A \hookrightarrow B$ des K-algèbres telles que B est une A-algèbre de type fini intègre. Alors pour tout $b \in B$ non nul, il existe $a \in A$ tel que, tout morphisme $\psi : A \to K$ tel que $\psi(a) \neq 0$ se prolonge en un morphisme $\widetilde{\psi} : B \to K$ tel que $\widetilde{\psi}(b) \neq 0$.*

Démonstration Par récurrence sur le nombre de générateurs de B comme A-algèbre, on peut supposer que B est engendré par un élément x. Notons alors $P(T) = \sum_{0 \leq i \leq \ell} p_i T^i \in A[T]$ un polynôme non nul de degré minimal ℓ tel que $P(x) = 0$. Remarquons tout d'abord que si le polynôme P n'existe pas alors $B \simeq A[T]$ et la conclusion du lemme 4.2 est claire. Notons L le corps des fractions de A. L'idéal $I := \{P_1 \in L[T] \mid P_1(x) = 0\}$ annulateur de x dans $L[T]$ est engendré par P.

Notons aussi $Q = \sum q_i T^i \in A[T]$ un polynôme non nul de degré au plus $\ell - 1$ tel que b divise $Q(x)$. On prend alors $a = p_\ell \, q_i$ où q_i est un des coefficients non

nuls de Q. Notons $\lambda \in K$ une racine du polynôme $\sum_{0\leq i\leq \ell} \psi(p_i)T^i \in K[T]$ qui est de degré ℓ. La formule $\widetilde{\psi}(\sum a_i x^i) = \sum \psi(a_i)\lambda^i$ définit bien un morphisme de B dans K qui prolonge ψ et tel que $\widetilde{\psi}(b)$ divise $\sum_i \psi(q_i)\lambda^i \neq 0$. □

Soit $\varphi : \mathbf{Z}_1 \to \mathbf{Z}_2$ une application k-régulière entre deux variétés algébriques irréductibles. On dit que φ est *dominante* si φ induit une injection $k[\mathbf{Z}_2] \to k[\mathbf{Z}_1]$ i.e. si l'image de φ est Zariski dense. On dit que φ est un plongement si φ induit une surjection $k[\mathbf{Z}_2] \to k[\mathbf{Z}_1]$ i.e. si φ est injective d'image Zariski fermée.

Remarque Le théorème de Chevalley dit que l'image de tout morphisme dominant contient un ouvert de Zariski dense. Si on examine la preuve du théorème de Chevalley, on obtient la précision suivante :

Corollaire 4.3 *Soit $\varphi : \mathbf{Z}_1 \to \mathbf{Z}_2$ une application régulière dominante entre deux variétés algébriques irréductibles. Alors, il existe un ouvert de Zariski dense $\mathbf{Z}'_1 \subset \mathbf{Z}_1$ lisse défini sur k sur lequel φ est une submersion i.e. sur lequel la différentielle $d\varphi$ est surjective.*

Démonstration Remplacer dans la preuve du lemme 4.2, la constante $a = p_\ell\, q_i$ par $a = \delta p_\ell\, q_i$ où δ est le discriminant de P. □

4.2 Groupes algébriques

Nous ne parlerons ici que de groupes algébriques linéaires. Voici donc quelques définitions.

Un *groupe algébrique (linéaire) défini sur k* ou, plus brièvement un *k-groupe* est une k-variété $\mathbf{G} \subset \mathrm{GL}(\mathbf{V}) \subset \mathrm{End}(\mathbf{V})$ qui est un groupe pour la composition des endomorphismes.

Par exemple, le *k-groupe additif* $\mathbf{G}_a := \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in K\}$,

le *k-groupe multiplicatif* $\mathbf{G}_m := \{\begin{pmatrix} y & 0 \\ 0 & z \end{pmatrix} \mid y, z \in K,\ xy = 1\}$

ou le *k-groupe linéaire* $\mathrm{GL}(\mathbf{V}) \simeq \{(g, \delta) \in \mathrm{End}(\mathbf{V}) \times K \mid \delta \det g = 1\}$.

On a $k[\mathbf{G}_a] = k[x]$ et $k[\mathbf{G}_m] = k[y, y^{-1}]$.

On note $\mathbf{G}_k := \mathbf{G} \cap GL(d, k)$ le *groupe des k-points* de $\mathbf{G}$, et plus généralement, pour tout sous-anneau A de K, $\mathbf{G}_A = \mathbf{G} \cap GL(d, A)$ est un sous-groupe de $\mathbf{G}$.

Un *k-morphisme* de k-groupes $\varphi : \mathbf{G}_1 \to \mathbf{G}_2$ est un k-morphisme de k-variétés qui est aussi un morphisme de groupes.

Une *k-isogénie* est un k-morphisme surjectif de noyau fini (on notera que le morphisme entre les k-points n'est pas toujours surjectif ; exemple : $y \to y^2$ dans $\mathbf{G}_m$).

Un *k-caractère* de $\mathbf{G}$ est un k-morphisme $\chi : \mathbf{G} \to \mathbf{G}_m$.

Un *k-cocaractère* de $\mathbf{G}$ est un k-morphisme $\chi : \mathbf{G}_m \to \mathbf{G}$.

Une *k-représentation* de $\mathbf{G}$ dans un k-espace vectoriel $\mathbf{W}_k$ est un k-morphisme $\rho : \mathbf{G} \to \mathrm{GL}(\mathbf{W})$.

Une *k-action* de $\mathbf{G}$ sur une k-variété $\mathbf{Z}$ est une action $\mathbf{G} \times \mathbf{Z} \to \mathbf{Z}$ qui est donnée par une application k-régulière.

L'algèbre de Lie $\mathfrak{g}$ d'un k-groupe $\mathbf{G}$ est l'ensemble des dérivations invariantes à gauche de l'algèbre $K[\mathbf{G}]$. L'algèbre de Lie $\mathfrak{g}$ s'identifie à l'espace tangent en e à $\mathbf{G}$, c'est à dire à l'intersection des noyau $\mathrm{Ker}(dP(e))$, pour $P \in I(\mathbf{G})$. On note $\mathfrak{g}_k$ les k-points de $\mathfrak{g}$. Lorsque $k = \mathbb{R}$, $\mathbb{C}$ ou une extension finie de $\mathbb{Q}_p$, $\mathfrak{g}_k$ est aussi l'algèbre de Lie du groupe de Lie k-analytique $\mathbf{G}_k$.

Avant de poursuivre cette importante liste de définitions, faisons une pause pour décrire quelques propriétés des k-groupes et leurs actions.

4.3 Actions algébriques

> L'un des intérêts majeurs des "groupes et actions algébriques" est la propriété suivante de leurs orbites qui contraste fortement avec les orbites des actions ergodiques.

Proposition 4.4 *Les orbites d'une k-action algébrique sont ouvertes dans leur adhérence (pour la topologie de Zariski).*

Démonstration Le théorème 4.1 prouve qu'au moins un point de l'orbite est dans l'intérieur de l'adhérence cette l'orbite. Ils y sont donc tous. □

Corollaire 4.5 *L'image $\varphi(\mathbf{G})$ d'un k-morphisme de k-groupes $\varphi : \mathbf{G} \to \mathbf{H}$ est un k-sous-groupe.*

Démonstration L'adhérence de Zariski $\overline{\varphi(\mathbf{G})}$ est un k-sous-groupe. D'après la proposition 4.4, l'image $\varphi(\mathbf{G})$ est ouverte dans cette adhérence. Or un sous-groupe ouvert est aussi fermé. □

Nous aurons souvent besoin de la proposition suivante qui joue un rôle central dans la théorie des groupes algébriques et qui affirme que tout espace homogène $\mathbf{G}/\mathbf{H}$ de k-groupes peut se réaliser comme une orbite dans l'espace projectif d'une k-représentation de $\mathbf{G}$.

Proposition 4.6 (Chevalley) *Soit $\mathbf{G}$ un k-groupe et $\mathbf{H} \subset \mathbf{G}$ un k-sous-groupe. Alors, il existe une k-représentation de $\mathbf{G}$ dans un espace vectoriel $\mathbf{V}_k$ et un point x dans l'espace projectif $\mathbb{P}(\mathbf{V}_k)$ dont le stabilisateur dans $\mathbf{G}$ est $\mathbf{H}$, i.e. $\mathbf{H} = \{g \in \mathbf{G} \,/\, g\,x = x\}$.*

En particulier, l'espace homogène $\mathbf{G}/\mathbf{H}$ a une structure naturelle de k-variété quasiprojective.

Démonstration de la proposition 4.6 Nous aurons besoin des notations : $I(\mathbf{H}) := \{P \in K[\mathbf{G}] \mid P|_{\mathbf{H}} = 0\}$, $K^m[\mathbf{G}] := \{P \in K[\mathbf{G}] \mid d^\circ P \leq m\}$ et $I^m(\mathbf{H}) := I(\mathbf{H}) \cap K^m[\mathbf{G}]$. Puisque $K[\mathbf{G}]$ est noethérien, on peut trouver m tel que $I^m(\mathbf{H})$ engendre l'idéal $I(\mathbf{H})$ de $K[\mathbf{G}]$. L'action de $\mathbf{G}$ sur $K^m[\mathbf{G}]$ donnée par $(\pi(g)P)(g') := P(g'g)$ est une k-représentation. La k-représentation que nous cherchons est la représentation dans la $p^{\text{ième}}$ puissance exterieure $\mathbf{V} := \Lambda^p(K^m[\mathbf{G}])$, où $p := \dim I^m(\mathbf{H})$ et x est la droite de $\mathbf{V}$ définie par $x := \Lambda^p(I^m(\mathbf{H}))$. Par construction, on a l'égalité requise $\mathbf{H} = \{g \in \mathbf{G} \,/\, g\,x = x\}$. □

Corollaire 4.7 *Soit* $\mathbf{G}$ *un* k*-groupe et* $\mathbf{H} \subset \mathbf{G}$ *un* k*-sous-groupe. Supposons que* $\mathbf{H}$ *n'a pas de* k*-caractère non trivial. Alors, il existe une* k*-représentation de* $\mathbf{G}$ *dans un espace vectoriel* $\mathbf{V}_k$ *et un point* $v \in \mathbf{V}_k$ *dont le stabilisateur dans* $\mathbf{G}$ *est* $\mathbf{H}$*, i.e.* $\mathbf{H} = \{g \in \mathbf{G} \,/\, g\,v = v\}$.

Démonstration L'action de $\mathbf{H}$ sur la droite x est triviale puisque tous les k-caractères de $\mathbf{H}$ sont triviaux. On prend v sur cette droite. □

Lorsque le corps k n'est pas algébriquement clos, on ne peut pas espérer des énoncés aussi nets que la proposition 4.4 au niveau des k-points. Néanmoins lorsque le corps de base k est $\mathbb{R}$, $\mathbb{C}$ ou une extension finie de $\mathbb{Q}_p$ on obtient de tels énoncés au niveau des k-points mais pour la topologie analytique, i.e. celle issue de la topologie du corps localement compact k.

Proposition 4.8 *Soient* $k = \mathbb{R}$, $\mathbb{C}$ *ou une extension finie de* $\mathbb{Q}_p$ *et* $\mathbf{G}$ *un* k*-groupe.*
a) Si $\mathbf{G}$ *est Zariski-connexe, le groupe* $\mathbf{G}_k$ *est Zariski dense dans* $\mathbf{G}$.
b) Soit $\rho : \mathbf{G} \times \mathbf{Z} \to \mathbf{Z}$ *une* k*-action de* $\mathbf{G}$ *sur une* k*-variété* $\mathbf{Z}$*. Alors, pour tout* $v \in \mathbf{Z}_k$*, les orbites de* $\mathbf{G}_k$ *dans* $(\mathbf{G}v)_k := \mathbf{G}v \cap \mathbf{Z}_k$ *sont ouvertes et fermées (pour la topologie analytique).*

Remarque l'assertion *a*) est encore vraie sans aucune hypothèse sur le corps infini k. Voir [7] cor. 18.3.

Démonstration a) Le groupe $\mathbf{G}_k$ est un groupe de Lie sur k dont l'algèbre de Lie $\mathfrak{g}_k$ s'identifie aux k-points de l'algèbre de Lie de $\mathbf{G}$. L'adhérence de Zariski $\mathbf{H}$ de $\mathbf{G}_k$ est un k-sous-groupe de $\mathbf{G}$ dont l'algèbre de Lie contient $\mathfrak{g}$. On a donc $\mathbf{H} = \mathbf{G}$.

b) On peut supposer que $\mathbf{Z} = \mathbf{G}v$. En particulier, $\mathbf{G}$ et $\mathbf{Z}$ sont des k-variétés lisses. Leurs k-points $\mathbf{G}_k$ et $\mathbf{Z}_k$ sont donc des k-variétés analytiques lisses dont les espaces tangents analytiques s'identifient aux k-points des espaces tangents algébriques à $\mathbf{G}$ et $\mathbf{Z}$. Notons $\rho_v : \mathbf{G} \to \mathbf{Z}; g \mapsto gv$ l'application orbitale. C'est une application surjective. Par le corollaire 4.3, sa différentielle est donc surjective sur un ouvert de Zariski non vide. Par $\mathbf{G}$-invariance, la différentielle $d\rho_v : T_e\mathbf{G} \to T_v\mathbf{Z}$

est surjective. Par le théorème des fonctions implicites, l'application $\rho_v : \mathbf{G}_k \to \mathbf{Z}_k$ est donc ouverte au voisinage de e. Donc les $\mathbf{G}_k$-orbites dans $(\mathbf{G}v)_k$ sont ouvertes dans $(\mathbf{G}v)_k$. Par suite ces orbites sont aussi fermées. □

Remarques - On peut aussi montrer que $\mathbf{G}_k$ n'a qu'un nombre fini d'orbites dans $\mathbf{G}v \cap \mathbf{Z}_k$.

- Lorsque $k = \mathbb{R}$, ces $\mathbf{G}_k$-orbites dans $(\mathbf{G}v)_k$ sont des unions de composantes connexes analytiques de $(\mathbf{G}v)_k$.

4.4 Eléments semisimples et unipotents

Rappelons dans ce cadre les définitions d'éléments *semisimple* et *unipotent* et leurs principales propriétés.

Un élément $g \in \mathrm{End}(\mathbf{V})$ est *semisimple* si il est diagonalisable sur K et *unipotent* si $g - 1$ est nilpotent. Le lemme suivant est la classique décomposition de Jordan.

Lemme 4.9 *Soient $g \in \mathrm{GL}(\mathbf{V})$ et $\mathbf{G} \subset \mathrm{GL}(\mathbf{V})$ un k-groupe.*
i) g peut s'écrire de façon unique $g = su = us$ avec s semisimple et u unipotent.
ii) Tout sous-espace $\mathbf{W} \subset \mathbf{V}$ invariant par g est aussi invariant par s et u.
iii) $g \in \mathbf{G} \Longrightarrow s, u \in \mathbf{G}$.
iv) $g \in \mathbf{G}_k \Longrightarrow s, u \in \mathbf{G}_k$.

Démonstration *i*) Classique.

ii) Les composantes s et u peuvent être exprimées comme des polynômes en g.

iii) Considérer l'action de $\mathbf{G}$ sur $K^m[\mathrm{End}\mathbf{V}] := \{P \in K[\mathrm{End}\mathbf{V}] \ / \ d^\circ P \leq m\}$ donnée par $(\pi(g)P)(x) := P(xg)$. On remarque tout d'abord que l'action sur $K^m[\mathrm{End}\mathbf{V}]$ d'un élément semisimple ou unipotent de $\mathrm{GL}(\mathbf{V})$ est encore semisimple ou unipotente.

Le sous-espace $I^m[\mathbf{G}] := I[\mathbf{G}] \cap K^m[\mathrm{End}\mathbf{V}]$ est invariant par g. Donc il est aussi invariant par sa composante semisimple et unipotente qui n'est autre que $\pi(s)$ et $\pi(u)$. Donc pour tout $P \in I^m[\mathbf{G}]$, on a $P(s) = (\pi(s)P)(1) = 0$ et $P(u) = (\pi(u)P)(1) = 0$. Donc s et u sont dans $\mathbf{G}$.

iv) Par unicité, s et u sont invariants par le groupe de Galois $\mathrm{Gal}(K/k)$. □

Remarques - Soit $g \in \mathbf{G}_k$. Comme char$k = 0$, on peut écrire $u = e^N$ avec N nilpotent. La même preuve assure que, pour tout $t \in k$, l'élément $u^t := e^{tN}$ est dans $\mathbf{G}_k$.

- Lorsque $k = \mathbb{R}$, on peut écrire de façon unique $s = hk = kh$ avec $h = e^H$ où H est diagonalisable sur $\mathbb{R}$ et k semisimple à valeurs propres de module 1. La même preuve assure que, pour tout $t \in \mathbb{R}$, l'élément $h^t := e^{tH}$ est dans $\mathbf{G}_\mathbb{R}$.

Lemme 4.10 *Soient $\rho : \mathbf{G} \to \mathbf{H}$ un k-morphisme de k-groupes et $g \in \mathbf{G}$.*
a) g est semisimple $\Longrightarrow \rho(g)$ est semisimple.
b) g est unipotent $\Longrightarrow \rho(g)$ est unipotent.

Proof. On peut supposer que $k = K$ et que $\mathbf{G}$ est le plus petit K-groupe contenant g. Le point principal est alors de prouver que tous les k-morphismes $\varphi : \mathbf{G}_a \to \mathbf{G}_m$ et $\psi : \mathbf{G}_m \to \mathbf{G}_a$ sont triviaux. On a $k[\mathbf{G}_a] = k[x]$ et $k[\mathbf{G}_m] = k[y, y^{-1}]$. Alors $y \circ \varphi$ est un élément inversible de $k[x]$, donc est une constante, et $x \circ \psi$ est un élément $F(y) \in k[y, y^{-1}]$ tel que $F(y) = F(y^n)/n$ pour tout $n \geq 1$, et est donc une constante. □

4.5 Groupes algébriques (suite)

Reprenons maintenant la liste des définitions relatives aux groupes algébriques.

Voici tout d'abord des notions stables par changement de corps de base.

Un k-groupe $\mathbf{G}$ est *connexe* si il est connexe pour la topologie de Zariski (lorsque $k = \mathbb{C}$, cela équivaut à la connexité pour la topologie analytique).

Un k-groupe $\mathbf{G}$ est *simplement connexe* si toute k-isogénie $\mathbf{H} \to \mathbf{G}$ avec $\mathbf{H}$ connexe est injective (lorsque $k = \mathbb{C}$, cela équivaut à la simple connexité pour la topologie analytique).

Un k-groupe est *unipotent* si tous ses éléments sont unipotents.

Le *radical unipotent* d'un k-groupe est le plus grand sous-groupe distingué unipotent.

Un k-groupe est un *k-tore* si il est abélien et si tous ses éléments sont semi-simples i.e. s'il est isomorphe sur K à une puissance $(\mathbf{G}_m)^r$ du groupe multiplicatif.

Un k-groupe est *réductif* si son radical unipotent est trivial.

Un k-groupe est *semisimple* si il ne contient pas de k-sous-groupe distingué connexe abélien. Autrement dit il est semisimple ssi il est réductif à centre fini.

Un k-groupe semisimple est dit *adjoint* si son centre est trivial.

Une k-représentation d'un k-groupe est *semisimple* si tout k-sous-espace invariant admet un supplémentaire invariant.

Voici maintenant des notions qui dépendent fortement du corps de base.

Un k-tore est *k-déployé* si il est isomorphe sur k à une puissance $(\mathbf{G}_m)^r$.

Un k-groupe est *k-déployé* si il contient un k-sous-tore maximal qui est k-déployé.

Un k-groupe $\mathbf{G}$ est dit *k-isotrope* si il contient un k-sous-tore k-déployé non trivial et *k-anisotrope* sinon.

Un k-groupe $\mathbf{G}$ est dit *k-quasisimple* si il est connexe et si tout k-sous-groupe distingué propre est fini.

Une k-représentation d'un k-groupe $\mathbf{G}$ est *k-irréductible* si 0 et $\mathbf{W}$ sont les seuls k-sous-espaces $\mathbf{G}$-invariants.

Proposition 4.11 *Lorsque $\mathbf{G}$ est semisimple, on a l'équivalence : $\mathbf{G}$ est k-isotrope ssi $\mathbf{G}_k$ contient des éléments unipotents non triviaux.*

Démonstration Pour l'implication directe on diagonalise l'algèbre de Lie $\mathfrak{g}$ pour l'action adjointe d'un tore k-isotrope $\mathbf{T}$. Chaque espace propre $\mathfrak{g}_\chi$ associé à un caractère non trivial χ de $\mathbf{T}$ est défini sur k et est formé d'éléments nilpotents. On retrouvera cet argument en montrant le lemme 5.5.b.

La réciproque résulte de la proposition 2.14 et du théorème 2.15 de Jacobson Morozov. Chaque élément nilpotent X de $\mathfrak{g}_k$ fait partie d'un $\mathfrak{sl}_2$-triplet (X, H, Y) dont l'élément H engendre l'algèbre de Lie d'un k-tore déployé de dimension 1.□

Proposition 4.12 *Une k-représentation d'un k-groupe semisimple $\mathbf{G}$ est semi-simple.*

Démonstration Pour montrer cela on peut, comme pour la proposition 2.14 supposer $k = \mathbb{C}$, et appliquer l'astuce unitaire avec le sous-groupe compact $K \subset \mathbf{G}_\mathbb{C}$ dont l'algèbre de Lie $\mathfrak{k}$ est une forme réelle compacte de l'algèbre de Lie $\mathfrak{g}$ de $\mathbf{G}_\mathbb{C}$. On a vu que ce groupe K existe dans le théorème 3.1. □

Remarque La catégorie des $\mathbb{R}$-*groupes semisimples simplement connexes* $\mathbf{G}$ est équivalente la catégorie des *groupes de Lie semisimples réels simplement connexes* G ou à celle des *algèbres de Lie semisimples réelles* $\mathfrak{g}$. Une équivalence entre ces catégories est donnée par les foncteurs $\mathbf{G} \mapsto G \mapsto \mathfrak{g}$ où G est le revêtement universel de $\mathbf{G}_\mathbb{R}$ et $\mathfrak{g} := Lie(G)$. C'est un yoga utile de passer d'un language à l'autre.

Par exemple, un sous-espace de Cartan $\mathfrak{a}$ de $\mathfrak{g}$ n'est rien d'autre que "l'algèbre de Lie des points réels d'un tore $\mathbb{R}$-déployé maximal $\mathbf{A}$ de $\mathbf{G}$". Ou encore, la catégorie des *représentations de dimension finie de* $\mathfrak{g}$ est équivalente à la catégorie des $\mathbb{R}$-*représentations de* $\mathbf{G}$.

Les géomètres différentiels et les analystes préfèrent souvent le deuxième language car il est plus adapté aux questions géométriques et topologiques. Les géomètres algébristes et les arithméticiens préfèrent souvent le premier language car il ouvre la voie à des extensions à d'autres corps que $\mathbb{R}$. Ces languages parlent presque du même objet, tout comme le *coffee* américain et le *caffè* italien désignent presque la même boisson...

On a vu à plusieurs reprises ces deux points de vue s'éclairer l'un l'autre. Rappelons en deux exemples particulièrement importants : L'*astuce unitaire* pour montrer la semisimplicité des k-représentations. La *décomposition de Jordan dans* $\mathbf{G}$ pour montrer la décomposition de Cartan de G.

5 Groupes arithmétiques

Nous avons montré dans le chapitre 1, que, pour une forme quadratique entière non dégénérée, le sous-groupe $\mathbf{G}_{\mathbb{Z}}$ des matrices orthogonales entières est un réseau dans le groupe $\mathbf{G}_{\mathbb{R}}$ des matrices orthogonales réelles.

Le but de ce chapitre est de montrer comment la preuve s'adapte à tous les $\mathbb{Q}$-groupes et d'obtenir ainsi le théorème de Borel et Harish-Chandra.

5.1 Groupes arithmétiques

Donnons tout d'abord la définition d'un sous-groupe arithmétique d'un $\mathbb{Q}$-groupe et vérifions qu'elle ne dépend pas, à commensurabilité près, du plongement du $\mathbb{Q}$-groupe dans un groupe de matrices.

Rappelons que l'expression $\mathbb{Q}$-*groupe* est un raccourci pour *groupe algébrique linéaire défini sur* $\mathbb{Q}$. On renvoie au chapitre 4 pour les définitions précises des notions relatives aux groupes algébriques que nous utiliserons.

Définition 5.1 *Soit* $\mathbf{G}$ *un* $\mathbb{Q}$*-groupe. Le sous-groupe* $\mathbf{G}_{\mathbb{Z}}$ *de* $\mathbf{G}$ *est appelé sous-groupe arithmétique.*

Cette définition 5.1 est provisoire : nous l'étendrons dans le chapitre 11.

Deux sous-groupes Γ_1 et Γ_2 d'un groupe Γ sont dits *commensurables* si l'intersection $\Gamma_1 \cap \Gamma_2$ est d'indice fini à la fois dans Γ_1 et Γ_2.

Le corollaire ci-dessous affirme que le sous-groupe arithmétique d'un $\mathbb{Q}$-groupe $\mathbf{G}$ est bien défini à commensurabilité près, indépendamment de "la réalisation de $\mathbf{G}$ comme groupe de matrices".

Lemme 5.2 *Soit* ρ *une* $\mathbb{Q}$*-représentation d'un* $\mathbb{Q}$*-groupe* $\mathbf{G}$ *dans un* $\mathbb{Q}$*-espace vectoriel* $\mathbf{V}_{\mathbb{Q}}$*. Alors,*
a) Le groupe $\mathbf{G}_{\mathbb{Z}}$ *préserve un réseau* $\Delta \subset \mathbf{V}_{\mathbb{Q}}$*.*
b) Tout réseau $\Delta_0 \subset \mathbf{V}_{\mathbb{Q}}$ *est préservé par un sous-groupe d'indice fini de* $\mathbf{G}_{\mathbb{Z}}$*.*

Démonstration a) Choisissons une base de $\mathbf{V}_{\mathbb{Q}}$. Les coefficients des matrices $\rho(g)-1$ s'expriment comme des polynômes à coefficients dans $\mathbb{Q}$ en les coefficients des matrices $g-1$. Le coefficient constant de ces polynômes est nul. Donc il existe un entier $m \geq 1$ tel que, si g est dans le *sous-groupe de congruence*

$$\Gamma_m := \{g \in \mathbf{G}_{\mathbb{Z}} \,/\, g = 1 \bmod m\},$$

alors $\rho(g)$a des coefficients entiers. Puisque Γ_m est d'indice fini dans $\mathbf{G}_{\mathbb{Z}}$, ce groupe $\mathbf{G}_{\mathbb{Z}}$ préserve aussi un réseau de $\mathbf{V}_{\mathbb{Q}}$.

b) C'est une conséquence du a) puisqu'on peut trouver des entiers $N, N_0 \geq 1$ tels que $N\Delta \subset N_0\Delta_0 \subset \Delta$. □

On en déduit facilement le corollaire suivant.

Corollaire 5.3 *Soit $\varphi : \mathbf{G}_1 \to \mathbf{G}_2$ un $\mathbb{Q}$-isomorphisme de $\mathbb{Q}$-groupes. Alors les groupes $\varphi(\mathbf{G}_{1,\mathbb{Z}})$ et $\mathbf{G}_{2,\mathbb{Z}}$ sont commensurables.*

Le but principal de ce chapitre est de démontrer le théorème suivant dont le point a) est dû à Borel, Harish-Chandra et le point b) à Godement.

Théorème 5.4 *Soit $\mathbf{G}$ un $\mathbb{Q}$-groupe.*
a) Si $\mathbf{G}$ n'a pas de $\mathbb{Q}$-caractère non trivial, alors $\mathbf{G}_\mathbb{Z}$ est un réseau de $\mathbf{G}_\mathbb{R}$.
b) Si $\mathbf{G}$ n'a pas de $\mathbb{Q}$-cocaractère non trivial, alors $\mathbf{G}_\mathbb{Z}$ est cocompact dans $\mathbf{G}_\mathbb{R}$.

Remarque Les réciproques des points *a*) et *b*) sont vraies et beaucoup plus facile :

Lemme 5.5 *Soit $\mathbf{G}$ un $\mathbb{Q}$-groupe.*
a) Si $\mathbf{G}$ a un $\mathbb{Q}$-caractère non trivial, alors $\mathbf{G}_\mathbb{Z}$ n'est pas un réseau de $\mathbf{G}_\mathbb{R}$.
b) Si $\mathbf{G}$ a un $\mathbb{Q}$-cocaractère non trivial, alors $\mathbf{G}_\mathbb{Z}$ n'est pas cocompact dans $\mathbf{G}_\mathbb{R}$.

Remarque Un k-groupe $\mathbf{G}$ a un k-caractère non trivial ssi il a un k-cocaractère central non trivial. En effet, pour le vérifier, on peut supposer, en quotientant $\mathbf{G}$ par son radical unipotent, que $\mathbf{G}$ est réductif. Comme $\mathbf{G}$ est presque produit de son centre connexe et de son groupe dérivé, on peut supposer que $\mathbf{G}$ est un tore. On remarque alors que $\mathbf{G}$ est presque produit d'un tore k-isotrope par un tore k-anisotrope. On renvoie à [7] pour plus de détails.

Démonstration du lemme 5.5 a) Par la proposition 4.8, l'image $\chi(\mathbf{G}_\mathbb{R})$ contient $\mathbb{R}_+^\star$, alors que, par le lemme 5.2, l'image $\chi(\mathbf{G}_\mathbb{Z})$ est incluse dans $(\mathbf{G}_m)_\mathbb{Z} = \{\pm 1\}$.

b) D'après le lemme 4.10, l'algèbre de Lie de l'image d'un $\mathbb{Q}$-cocaractère est de dimension 1 et est engendrée par un élément H diagonalisable. Comme les seuls caratères du groupe multiplicatif $\mathbf{G}_m$ sont les puissances $z \mapsto z^n$, on peut supposer que les valeurs propres de H sont entières. Par le *a*) et la remarque ci-dessus, cet élément H n'est pas dans le centre de $\mathfrak{g}$. Il existe donc un entier $p \neq 0$ et un élément non nul $X \in \mathfrak{g}$ à coefficients entiers tel que $[H, X] = pX$. Par le théorème 2.4 de Lie, cet élément X est nilpotent. En particulier, l'orbite adjointe $\mathrm{Ad}\mathbf{G}_\mathbb{R}(X)$ contient 0 dans son adhérence. Si $\mathbf{G}_\mathbb{Z}$ était cocompact dans $\mathbf{G}_\mathbb{R}$, comme $\mathrm{Ad}\mathbf{G}_\mathbb{Z}(X)$ est un ensemble discret formée de matrices à coefficients entiers, l'orbite adjointe $\mathrm{Ad}\mathbf{G}_\mathbb{R}(X)$ serait fermée. Contradiction. □

Corollaire 5.6 *Soit $\mathbf{G}$ un $\mathbb{Q}$-groupe semisimple.*
a) Alors $\mathbf{G}_\mathbb{Z}$ est un réseau de $\mathbf{G}_\mathbb{R}$.
b) $\mathbf{G}_\mathbb{Z}$ est cocompact dans $\mathbf{G}_\mathbb{R}$ ssi $\mathbf{G}_\mathbb{Z}$ n'a pas d'élément unipotent non trivial.

Remarque On a les équivalences : $\mathbf{G}_\mathbb{Z}$ *n'a pas d'élément unipotent non trivial* $\Leftrightarrow$ $\mathbf{G}_\mathbb{Q}$ *n'a pas d'élément unipotent non trivial* $\Leftrightarrow$ $\mathfrak{g}_\mathbb{Q}$ *n'a pas d'élément nilpotent non nul.*

En effet, l'application $X \to e^X - 1$ et son inverse $X \to \log(1+X)$ sont données par des polynômes à coefficients rationnels quand on les applique à des matrices nilpotentes.

Démonstration de : théorème 5.4 $\Rightarrow$ corollaire 5.6

a) Un groupe semisimple n'a pas de caractère.

b) On a déjà vu dans la démonstration du point b) du lemme 5.5 que si $\mathbf{G}$ a des $\mathbb{Q}$-cocaractères non triviaux alors $\mathfrak{g}_\mathbb{Q}$ contient des éléments nilpotents non nuls.

Réciproquement, lorsque $\mathbf{G}$ est semisimple, *un réseau cocompact* Γ *de* $\mathbf{G}_\mathbb{R}$ *ne peut pas contenir d'élément unipotent non trivial*. Voici pourquoi.

D'une part, la classe de conjugaison d'un élément unipotent contient e dans son adhérence : c'est facile pour $\mathrm{SL}(2,\mathbb{R})$, le cas général s'en déduit par le théorème 2.15 de Jacobson Morozov.

D'autre part, la classe de conjugaison d'un élément $\gamma_0 \in \Gamma$ est fermée car l'ensemble des conjugués $\{\gamma\gamma_0\gamma^{-1} \mid \gamma \in \Gamma\}$ est discret et $\mathbf{G}_\mathbb{R}/\Gamma$ est compact. $\square$

Remarque Soit $\mathbf{G}$ un $\mathbb{Q}$-groupe sans $\mathbb{Q}$-caractère. Alors $\mathbf{G}_\mathbb{R}$ est unimodulaire. En effet, comme l'application adjointe Ad est définie sur $\mathbb{Q}$, le caractère $g \mapsto \det(\mathrm{Ad}(g))$ est un $\mathbb{Q}$-caractère. Il est donc trivial. Or, la fonction module est la valeur absolue de la restriction à $\mathbf{G}_\mathbb{R}$ de ce caractère.

5.2 Stratégie de démonstration du théorème 5.4.a

> Soit $\mathbf{G}$ un $\mathbb{Q}$-groupe sans $\mathbb{Q}$-caractère. On veut montrer que la mesure $\mathbf{G}_\mathbb{R}$-invariante λ sur $\mathbf{G}_\mathbb{R}/\mathbf{G}_\mathbb{Z}$ est finie.

La première étape est un joli argument de plongement (proposition 5.7) qui permettra, dès qu'on se donne une $\mathbb{Q}$-représentation fidèle de $\mathbf{G}$ dans $\mathbf{V}_\mathbb{Q}$, de voir cette mesure λ comme une mesure de Radon sur l'espace X des réseaux de volume 1 de $\mathbf{V}_\mathbb{R}$.

On veut alors appliquer encore une combinaison des corollaires 1.5 et 1.14. Pour cela, il suffit de construire une probabilité μ portée par $\mathbf{G}_\mathbb{R}$ vérifiant la condition **[HI]**. Remarquons de nouveau que cette condition ne fait plus intervenir le groupe $\mathbf{G}_\mathbb{Z}$. Cette stratégie aboutira uniquement lorsque $\mathbf{G}$ est $\mathbb{Q}$-simple, adjoint et $\mathbb{Q}$-isotrope. Ce sera la deuxième étape du raisonnement. Notons que cette étape est la plus délicate, le groupe $\mathbf{G}_\mathbb{Z}$ y apparaissant comme un réseau non cocompact.

La troisième étape, le cas où $\mathbf{G}$ est $\mathbb{Q}$-simple, adjoint et $\mathbb{Q}$-anisotrope, est une application du critère de Mahler. Elle prouvera que dans ce cas le quotient $\mathbf{G}_\mathbb{R}/\mathbf{G}_\mathbb{Z}$ est compact. Cette étape contient le critère de compacité de Godement.

Dans la quatrième étape, on passera du cas $\mathbb{Q}$-simple adjoint au cas réductif sans $\mathbb{Q}$-caractère. Ce sera de nouveau une application du critère de Mahler (proposition 5.11). Cette étape importante contient le cas où $\mathbf{G}$ est un tore $\mathbb{Q}$-anisotrope. Elle contient donc en particulier le théorème des unités de Dirichlet.

Enfin, dans la cinquième et dernière étape, la décomposition de Levi pour les $\mathbb{Q}$-groupes $\mathbf{G} = \mathbf{RU}$ comme produit semidirect d'un $\mathbb{Q}$-groupe reductif $\mathbf{R}$ et d'un $\mathbb{Q}$-groupe unipotent $\mathbf{U}$ (décomposition que nous admettrons) permettra de montrer le théorème pour tous les $\mathbb{Q}$-groupes sans $\mathbb{Q}$-caractère. □

5.3 Le plongement dans l'espace des réseaux

Le plongement suivant permet de relier l'étude du quotient $\mathbf{G}_\mathbb{R}/\mathbf{G}_\mathbb{Z}$ à celle de l'espace des réseaux de $\mathbb{R}^d$.

Proposition 5.7 *Soit $\mathbf{G} \subset \mathbf{H} = \mathrm{GL}(d, \mathbb{C})$ un $\mathbb{Q}$-groupe sans $\mathbb{Q}$-caractère non trivial. Alors l'injection $\mathbf{G}_\mathbb{R}/\mathbf{G}_\mathbb{Z} \hookrightarrow X = \mathbf{H}_\mathbb{R}/\mathbf{H}_\mathbb{Z}$ est propre.*

Autrement dit, cette injection est un homéomorphisme sur une partie fermée de X

Démonstration Nous devons montrer que pour toute suite $g_n \in \mathbf{G}_\mathbb{R}$, telle que $g_n\mathbf{H}_\mathbb{Z}$ converge dans dans $\mathbf{H}_\mathbb{R}/\mathbf{H}_\mathbb{Z}$, la suite $g_n\mathbf{G}_\mathbb{Z}$ converge dans $\mathbf{G}_\mathbb{R}/\mathbf{G}_\mathbb{Z}$.

D'après la proposition 4.6 (avec $\mathbf{H}$ pour $\mathbf{G}$ et $\mathbf{G}$ pour $\mathbf{H}$), il existe une $\mathbb{Q}$-représentation de $\mathbf{H}$ dans un $\mathbb{Q}$-espace vectoriel $\mathbf{V}_\mathbb{Q}$ et un pointr $x \in \mathbb{P}(\mathbf{V}_\mathbb{Q})$ dont le stabilisateur dans $\mathbf{H}$ est $\mathbf{G}$. Puisque tous les $\mathbb{Q}$-caractères de $\mathbf{G}$ sont triviaux, le stabilisateur de tout point non nul v sur la droite x est aussi égal à $\mathbf{G}$. Par le lemme 5.2, le groupe $\mathbf{H}_\mathbb{Z}$ stabilise un réseau $\Delta \subset \mathbf{V}_\mathbb{Q}$. On peut choisir Δ contenant v. Donc la $\mathbf{H}_\mathbb{Z}$-orbite de v est discrète dans $\mathbf{V}_\mathbb{R}$.

Soit $h_n \in \mathbf{H}_\mathbb{Z}$ tel que $\lim_{n\to\infty} g_n h_n = h$. La suite $h_n^{-1}v$ converge vers $h^{-1}v$ et est donc constante pour n grand. On peut donc écrire, pour n grand, $h_n = \gamma_n h$ avec $\gamma \in \mathbf{G}_\mathbb{Z}$, $h \in \mathbf{H}_\mathbb{Z}$. La suite $g_n\gamma_n$ est alors convergente. □

5.4 Le cas $\mathbb{Q}$-simple et $\mathbb{Q}$-isotrope

Voici un cas particulier du théorème de Borel et Harish-Chandra qui se trouve être le cas le plus délicat.

Lemme 5.8 *Soit $\mathbf{G}$ un $\mathbb{Q}$-groupe $\mathbb{Q}$-simple, adjoint et $\mathbb{Q}$-isotrope Alors $\mathbf{G}_\mathbb{Z}$ est un réseau de $\mathbf{G}_\mathbb{R}$*

Démonstration Le premier point est de voir que, comme $\mathbf{G}$ est adjoint, $\mathbf{G}$ admet une $\mathbb{Q}$-représentation fidèle ρ qui est $\mathbb{R}$-irréductible. La représentation adjointe est somme directe $\rho_1 \oplus \cdots \oplus \rho_\ell$ de représentations irréductibles de $\mathbf{G} = \mathbf{G}_1 \times \cdots \times \mathbf{G}_\ell$ qui correspondent aux idéaux $\mathfrak{g}_i$ de l'algèbre de Lie de $\mathbf{G}$. Chaque représentation

ρ_i est irréductible sous l'action de $\mathbf{G}_i$ et ces représentations sont permutées par le groupe de Galois $\mathrm{Gal}(\mathbb{C},\mathbb{Q})$. On prend pour ρ le produit tensoriel $\rho = \rho_1 \otimes \cdots \otimes \rho_\ell$ de ces représentations. C'est une représentation fidèle de $\mathbf{G}$ définie sur $\mathbb{Q}$ qui est $\mathbb{C}$-irréductible. Elle est donc $\mathbb{R}$-irréductible.

Le deuxième point est de voir que, comme $\mathbf{G}$ est $\mathbb{Q}$-simple et $\mathbb{Q}$-isotrope, le groupe $\mathbf{G}_\mathbb{R}$ n'a pas de facteur compact. En effet, comme $\mathbf{G}$ est $\mathbb{Q}$-simple, un tel facteur est le groupe $(\mathbf{G}_i)_\mathbb{R}$ des $\mathbb{R}$-points d'un facteur $\mathbb{R}$-simple $\mathbf{G}_i$ de $\mathbf{G}$ vu comme $\mathbb{R}$-groupe. Mais, comme $\mathbf{G}$ est $\mathbb{Q}$-simple et $\mathbb{Q}$-isotrope, un tel facteur est $\mathbb{R}$-isotrope et donc non compact.

Le troisième point est d'utiliser le lemme 5.9 suivant qui permet de construire une probabilité μ portée par $\mathbf{G}_\mathbb{R}$ vérifiant la condition **[HI]**. Ce qui permet de conclure grâce à la stratégie décrite ci-dessus. □

Lemme 5.9 *Soit $\mathbf{G} \subset \mathrm{GL}(d,\mathbb{C})$ un $\mathbb{R}$-groupe semisimple.Alors*
a) il existe un produit scalaire euclidien sur $\mathbb{R}^d$ tel que, pour tout g dans $\mathbf{G}$, l'adjoint ${}^t g$ est aussi dans $\mathbf{G}$.
b) Dans ce cas, si $\mathbf{G}_\mathbb{R}$ n'a pas de facteur compact, $\mathbf{G}_\mathbb{R}$ est engendré par $\mathbf{G}_\mathbb{R} \cap S^+$

Rappelons que S^+ est l'ensemble des matrices symétriques définies positives.

Démonstration L'algèbre de Lie $\mathfrak{g}_\mathbb{R}$ de $\mathbf{G}_\mathbb{R}$ admet une involution de Cartan θ qui correspond à une décomposition de Cartan $\mathfrak{g}_\mathbb{R} = \mathfrak{k} \oplus \mathfrak{q}$ (voir chapitre 3). La sous-algèbre $\mathfrak{u} = \mathfrak{k} \oplus i\mathfrak{q}$ a une forme de Killing définie négative. Elle est donc l'algèbre de Lie d'un sous-groupe compact $U_\mathbb{R}$ de $\mathrm{GL}(d,\mathbb{C})$. Ce groupe $U_\mathbb{R}$ préserve une forme hermitienne sur $\mathbb{C}^d$. On prend pour produit scalaire la partie réelle de la restriction à $\mathbb{R}^d$ de cette forme hermitienne.

b) Dans la décomposition $\mathfrak{g}_\mathbb{R} = \mathfrak{k} \oplus \mathfrak{q}$, les éléments M de $\mathfrak{q}$ sont symétriques et leurs exponentielles $\exp(M)$ sont symétriques définies positives. Comme $[\mathfrak{q},\mathfrak{q}] \oplus \mathfrak{q}$ est un idéal de $\mathfrak{g}_\mathbb{R}$ et que $\mathbf{G}_\mathbb{R}$ n'a pas de facteur compact, on a l'égalité $\mathfrak{g}_\mathbb{R} = [\mathfrak{q},\mathfrak{q}] \oplus \mathfrak{q}$ et $\mathbf{G}_\mathbb{R}$ est engendré par $\exp(\mathfrak{q})$. □

5.5 Le cas $\mathbb{Q}$-simple et $\mathbb{Q}$-anisotrope

Cette étape est plus simple que la précédente : Elle n'utilise que le plongement et le critère de Mahler.

Corollaire 5.10 *Soit $\mathbf{G}$ un $\mathbb{Q}$-groupe $\mathbb{Q}$-simple et $\mathbb{Q}$-anisotrope.*
Alors $\mathbf{G}_\mathbb{Z}$ est un réseau cocompact de $\mathbf{G}_\mathbb{R}$

Démonstration Comme $\mathbf{G}$ est adjoint, on peut supposer que $\mathbf{G}$ est inclus dans le groupe $\mathrm{Aut}(\mathfrak{g})$ des automorphismes de l'algèbre de Lie $\mathfrak{g}$.

Par la proposition 5.7, le quotient $\mathbf{G}_\mathbb{R}/\mathbf{G}_\mathbb{Z}$ est homéomorphe au sous-ensemble fermé $\{\mathrm{Ad}g(\mathfrak{g}_\mathbb{Z}) \mid g \in \mathbf{G}_\mathbb{R}\}$ de l'ensemble des réseaux de $\mathfrak{g}_\mathbb{R}$. En outre tous ces réseaux sont de même covolume. Si le quotient n'était pas compact, le critère de

compacité de Mahler, i.e. la proposition 1.8, assurerait qu'il existerait $g_n \in \mathbf{G}_\mathbb{R}$ et $X_n \in \mathfrak{g}_\mathbb{Z} - \{0\}$ tel que $\mathrm{Ad}(g_n)(X_n)$ converge vers 0. Pour tout $i \geq 1$, la suite d'entiers $n \to tr(X_n^i)$ converge vers 0. Elle donc nulle pour n grand. Donc pour n grand, X_n est nilpotent. Et $\mathbf{G}$ n'est pas $\mathbb{Q}$-anisotrope. Contradiction.

5.6 Le cas réductif

Le lemme clef pour passer du cas $\mathbb{Q}$-simple adjoint au cas réductif est la proposition suivante.

Proposition 5.11 *Soit $\mathbf{G}$ un $\mathbb{Q}$-groupe réductif, $\mathbf{C}$ le centre de $\mathbf{G}$ et $\mathbf{H}$ le $\mathbb{Q}$-groupe quotient $\mathbf{H} = \mathbf{G}/\mathbf{C}$. On suppose que $\mathbf{G}$ n'a pas de $\mathbb{Q}$-caractère. Alors, l'application induite $\pi : \mathbf{G}_\mathbb{R}/\mathbf{G}_\mathbb{Z} \to \mathbf{H}_\mathbb{R}/\mathbf{H}_\mathbb{Z}$ est une application propre.*

Remarques Ce quotient $\mathbf{H}$ est un $\mathbb{Q}$-groupe semisimple adjoint. Il est donc produit de groupes $\mathbb{Q}$-simples adjoints.

Démonstration Soit $\mathbf{G} \subset \mathrm{End}(\mathbf{V})$ notre $\mathbb{Q}$-groupe et $\mathbf{A} := \mathrm{End}_\mathbf{C}(\mathbf{V})$ le commutant de $\mathbf{C}$ dans $\mathrm{End}(\mathbf{V})$. Comme le centre $\mathbf{C}$ est réductif et défini sur $\mathbb{Q}$, l'algèbre associative $\mathbf{A}$ est semisimple et définie sur $\mathbb{Q}$, en particulier, l'anneau $\mathbf{A}_\mathbb{Z} = \mathbf{A} \cap \mathrm{End}(\mathbf{V}_\mathbb{Z})$ est un réseau de $\mathbf{A}_\mathbb{R} := \mathbf{A} \cap \mathrm{End}(\mathbf{V}_\mathbb{R})$ que l'on peut supposer de covolume 1.

Le groupe $\mathbf{G}$ agit de deux façons sur l'algèbre $\mathbf{A}$: l'action ρ par translation à gauche et l'action σ par conjugaison qui factorise en une action de $\mathbf{H}$. Rappelons que $\mathbf{G}$ n'a pas de $\mathbb{Q}$-caractère. En appliquant deux fois la proposition 5.7 on obtient, d'une part, que le quotient $\mathbf{G}_\mathbb{R}/\mathbf{G}_\mathbb{Z}$ est homéomorphe à l'ensemble des translatés $\{g\mathbf{A}_\mathbb{Z} \mid g \in \mathbf{G}_\mathbb{R}\}$ et, d'autre part, le quotient $\mathbf{H}_\mathbb{R}/\mathbf{H}_\mathbb{Z}$ est homéomorphe à l'ensemble des conjugués $\{h(\mathbf{A}_\mathbb{Z}) \mid h \in \mathbf{H}_\mathbb{R}\}$. En outre tous ces réseaux sont de covolume 1. Supposons par l'absurde que l'application π n'est pas propre, il existe donc une suite $g_n \in \mathbf{G}_\mathbb{R}$ telle que $g_n\mathbf{A}_\mathbb{Z}$ n'est pas bornée tandis que $g_n\mathbf{A}_\mathbb{Z}g_n^{-1}$ est bornée.

Le critère de compacité de Mahler, i.e. la proposition 1.8, assure qu'il existe une suite $a_n \in \mathbf{A}_\mathbb{Z} - \{0\}$ telle que $g_n a_n$ converge vers 0 et que toute suite $a'_n \in \mathbf{A}_\mathbb{Z}$ telle que $g_n a'_n g_n^{-1}$ converge vers 0 est nulle pour n grand.

Puisque l'algèbre associative semisimple $\mathbf{A}$ est somme directe de ses idéaux bilatères définis sur $\mathbb{Q}$ minimaux $\mathbf{B}$, on peut supposer que a_n est dans l'un des $\mathbf{B}_\mathbb{Z} - \{0\}$. Soit b_i une base de $\mathbf{B}_\mathbb{Z}$. Puisque $\det_\mathbf{B} g_n = 1$, par le lemme 1.10 de Minkowski, on peut trouver $C_0 > 0$ et des éléments non nuls $c_n \in \mathbf{B}_\mathbb{Z}$ tels que $\|c_n g_n^{-1}\| \leq C_0$. Les éléments $g_n a_n b_i c_n g_n^{-1}$ convergent aussi vers 0. Donc, pour $n \gg 0$, on a successivement, $a_n b_i c_n = 0$, $a_n \mathbf{B} c_n \mathbf{B} = 0$, $a_n \mathbf{B} = 0$, et $a_n = 0$. Contradiction. □

Corollaire 5.12 *Soit $\varphi : \mathbf{G} \to \mathbf{H}$ une $\mathbb{Q}$-isogénie entre deux $\mathbb{Q}$-groupes réductifs. Alors les groupes $\varphi(\mathbf{G}_\mathbb{Z})$ et $\mathbf{H}_\mathbb{Z}$ sont commensurables.*

Démonstration Quitte à remplacer $\mathbf{G}$ et $\mathbf{H}$ par l'intersection des noyaux de leurs $\mathbb{Q}$-caractères, on peut supposer $\mathbf{G}$ et $\mathbf{H}$ sans $\mathbb{Q}$-caractère. Notons $\mathbf{Z_G}$ le centre de $\mathbf{G}$ et $\mathbf{Z_H}$ le centre de $\mathbf{H}$. On remarque que l'application φ induit un isomorphisme $\mathbf{G}/\mathbf{Z_G} \simeq \mathbf{H}/\mathbf{Z_H}$. On applique alors deux fois la proposition 5.11 à $\mathbf{G}$ puis à $\mathbf{H}$ pour en déduire que l'application $\mathbf{G}_\mathbb{R}/\mathbf{G}_\mathbb{Z} \to \mathbf{H}_\mathbb{R}/\mathbf{H}_\mathbb{Z}$ est propre. □

Remarque L'analogue de ce corollaire pour les $\mathbb{Q}$-points est inexact : les groupes $\varphi(\mathbf{G}_\mathbb{Q})$ et $\mathbf{H}_\mathbb{Q}$ ne sont pas toujours commensurables. Prendre par exemple $\mathbf{G} = \mathrm{SL}(2)$ et $\mathbf{H} = \mathrm{PGL}(2)$ et regarder les éléments de $\mathbf{H}_\mathbb{Q}$ donnés par $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$.

5.7 Conclusion

En utilisant la structure des $\mathbb{Q}$-groupes, nous pouvons maintenant terminer par récurrence notre raisonnement.

Démonstration du théorème 5.4 Remarquons tout d'abord que si $\mathbf{G} = \mathbf{H} \ltimes \mathbf{N}$ est une décomposition d'un $\mathbb{Q}$-groupe $\mathbf{G}$ en un produit semidirect d'un $\mathbb{Q}$-sous-groupe $\mathbf{H}$ et d'un $\mathbb{Q}$-sous-groupe distingué $\mathbf{N}$, alors le groupe $\mathbf{H}_\mathbb{Z}\mathbf{N}_\mathbb{Z}$ est inclus dans $\mathbf{G}_\mathbb{Z}$. En particulier si $\mathbf{H}_\mathbb{Z}$ est un réseau de $\mathbf{H}_\mathbb{R}$ et $\mathbf{N}_\mathbb{Z}$ est un réseau de $\mathbf{N}_\mathbb{R}$, alors $\mathbf{G}_\mathbb{Z}$ est un réseau de $\mathbf{G}_\mathbb{R}$

D'après la décomposition de Levy, valable sur tout corps k de caractéristique 0, tout k-groupe $\mathbf{G}$ est un produit semidirect $\mathbf{L} \ltimes \mathbf{U}$ d'un k-groupe réductif $\mathbf{L}$ et d'un k-sous-groupe distingué unipotent $\mathbf{U}$.

En outre, tout k-groupe unipotent de dimension $n \geq 1$ est un produit semidirect du k groupe additif $\mathbf{G}_a$ de dimension 1 et d'un k-sous-groupe distingué unipotent U' de dimension $n-1$.

Puisque le sous-groupe arithmétique $(\mathbf{G}_a)_\mathbb{Z} \simeq \mathbb{Z}$ est un réseau cocompact du groupe de Lie $(\mathbf{G}_a)_\mathbb{R} \simeq \mathbb{R}$, ces remarques ramènent la démonstration du théorème 5.4 au cas réductif que nous avons obtenu dans la proposition 5.11. □

6 Mélange et comptage

Ce chapitre est encore au coeur des thèmes de ce cours reliant théorie des nombres et théorie ergodique à travers la théorie des groupes.

L'objectif arithmétique est de donner l'asymptotique en r du nombre de matrices de $SL(d,\mathbb{Z})$ de norme au plus r. Nous obtiendrons plus généralement un tel asymptotique pour tous les réseaux Γ des groupes de Lie quasisimples G.

La propriété ergodique est ici le *mélange* de l'action des éléments de G sur le quotient de volume fini G/Γ.

La théorie des représentations unitaires joue un rôle central dans cette propriété de mélange.

Les démonstrations ci-dessous sont self-contained pour $SL(d,\mathbb{Z})$, sauf pour une formule explicite pour la mesure de Haar dans la décomposition de Cartan . Dans le cas général, nous utiliserons en plus quelques propriétés sur la structure des groupes de Lie semisimples réels, décompositions de Cartan et d'Iwasawa, que nous avons démontrées au chapitre 3.

6.1 Représentations unitaires et mélange

Commençons par la partie théorie des représentations unitaires et énonçons une propriété générale, due à Howe et Moore, de décroissance des coefficients des représentations unitaires.

Définition 6.1 *Une représentation unitaire π d'un groupe localement compact G dans un espace de Hilbert (séparable) $\mathcal{H}_\pi$ est un morphisme de G dans le groupe $U(\mathcal{H}_\pi)$ des transfomations unitaires de $\mathcal{H}_\pi$, tel que, pour tout v dans $\mathcal{H}_\pi$, l'application $G \to \mathcal{H}_\pi; g \mapsto \pi(g)v$ est continue.*

Pour tout v, w dans $\mathcal{H}_\pi$, le coefficient est la fonction continue $c_{v,w} : G \to \mathbb{C}$ donnée par $c_{v,w}(g) = <\pi(g)v, w>$.

Exemples - La *représentation triviale* est la représentation constante $\pi(g) = Id$. Ses coefficients sont des fonctions constantes.
- Quand G est compact, toute représentation unitaire est une somme hilbertienne orthogonale de représentations unitaires irréductibles. Par Peter-Weyl, elles sont de dimension finie.
- Supposons que G agisse continûment sur un espace localement compact X en préservant une mesure de Radon ν. Alors la formule $(\pi(g)\varphi)(x) := \varphi(g^{-1}x)$ définit une représentation unitaire π de G dans $L^2(X,\nu)$ Pour montrer la continuité des applications $g \mapsto \pi(g)\varphi$, on la montre tout d'abord pour les fonctions continues à support compact puis on utilise la densité de ces fonctions dans $L^2(X,\nu)$.

Les coefficients

$$c_{\varphi,\psi} : g \to \int_X \varphi(x)\overline{\psi}(gx)d\nu(x)$$

de cette représentation sont aussi appelés *coefficients de corrélation*.

Pour tout sous-groupe H de G, notons

$$\mathcal{H}_\pi^H := \{v \in \mathcal{H}_\pi \ / \ \forall h \in H,\ \pi(h)v = v\}$$

le sous-espace des vecteurs H-invariants.

Rappelons qu'un groupe de Lie G est *semisimple* si son algèbre de Lie $\mathfrak{g}$ est *semisimple*, et que G est *quasisimple* si $\mathfrak{g}$ simple (voir chapitre 3). Par exemple les groupes de Lie $\mathrm{SL}(d,\mathbb{R})$ et $\mathrm{SO}(p,q)$ sont quasisimples pour $d \geq 2$ et $p+q \geq 3$.

Théorème 6.2 (Howe, Moore) *Soit G un groupe de Lie réel connexe semisimple à centre fini et π une représentation unitaire de G. Supposons que $\mathcal{H}_\pi^{G_i} = 0$ pour tout sous-groupe connexe normal $G_i \neq 1$.*

Alors, pour tout v, w dans $\mathcal{H}_\pi$, on a $\lim_{g\to\infty} <\pi(g)v, w> = 0$.

Remarques - La preuve de ce théorème est reportée à la section 6.3.
- Le symbole $g \to \infty$ signifie que g sort de tout compact de G.
- D'après le théorème 2.7, il n'y a qu'un nombre fini de G_i.
- Quand $\mathfrak{g}$ est simple, l'hypothèse est $\mathcal{H}_\pi^G = 0$.

Corollaire 6.3 *Soit G un groupe de Lie réel connexe semisimple à centre fini et π une représentation unitaire de G sans vecteur G-invariant non nul. Soit H un sous-groupe fermé de G dont les images dans tous les groupes quotients $G/G_i \neq 1$ sont non compactes. Alors $\mathcal{H}_\pi^H = 0$.*

Remarque - Quand $\mathfrak{g}$ est simple, l'hypothèse sur H équivaut à *H non compact*.

Démonstration Par récurrence, en écrivant $\mathcal{H}_\pi = \mathcal{H}_\pi^{G_i} \oplus (\mathcal{H}_\pi^{G_i})^\perp$, on peut supposer que $\mathcal{H}_\pi^{G_i} = 0$ pour tout i. Soit v un vecteur H-invariant. Le coefficient $c_{v,v}$ est constant sur H. Par le théorème 6.2, il doit être nul. Donc $v = 0$. □

Corollaire 6.4 *Soit G un groupe de Lie réel connexe quasisimple à centre fini, $\Gamma \subset G$ un réseau. Alors l'action de G est mélangeante sur $X = G/\Gamma$, i.e. on a la propriété suivante de "décroissance des corrélations" : pour tout $\varphi, \psi \in L^2(X, dx)$,*

$$\lim_{g\to\infty} \int_X \varphi(x)\psi(gx)dx = \int_X \varphi(x)dx \int_X \psi(x)dx.$$

- Pour simplifier, on a noté $dx = \lambda_X$ la probabilité G-invariante sur X.
- Une extension aux réseaux irréductibles sera donnée dans le corollaire 7.7.

Remarque En particulier, pour tout élément $g \in G$ qui engendre un sous-groupe non-borné de G, l'action de g sur X est *ergodique*, i.e. toute partie mesurable g-invariante A de X vérifie $\lambda_X(A) = 0$ ou 1 (voir chapitre 8).

Démonstration du corollaire 6.4 Ecrivons $L^2(X,dx) = \mathbb{C}\mathbf{1} \oplus L^2_0(X,dx)$ où $L^2_0(X,dx)$ désigne le sous-espace des fonctions d'intégrale nulle. D'après le théorème 6.2, il suffit de remarquer que les fonctions G-invariantes φ de $L^2_0(X,dx)$ sont nulles. Cela résulte de Fubini car si, pour tout g dans G, $\varphi(gx) = \varphi(x)$ pour presque tout $x \in X$, alors on peut trouver $x \in X$ tel que, $\varphi(gx) = \varphi(x)$ pour presque tout $g \in G$. Et donc φ est presque sûrement constante. Donc $\varphi = 0$. □

6.2 Vecteurs invariants pour SL(2)

Commençons par une preuve directe du corollaire 6.3 pour le groupe $\mathrm{SL}(2,\mathbb{R})$.

Pour $t > 0$ et s dans $\mathbb{R}$, soit

$$a_t := \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix},\ u_s := \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix},\ u_s^- := \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}.$$

Proposition 6.5 *Soit π une représentation unitaire de $G = \mathrm{SL}(2,\mathbb{R})$, $t \neq 1$, $s \neq 0$ et $v \in \mathcal{H}_\pi$. Si v est soit a_t-invariant, u_s-invariant ou u_s^--invariant alors, il est G-invariant.*

Remarque La proposition 6.5 et sa démonstration sont encore valables pour le groupe S revêtement universel de $\mathrm{SL}(2,\mathbb{R})$, en remplaçant les groupes à un paramètre a_t, u_s et u_s^- par leur relèvement dans S.

On utilisera le lemme suivant.

Lemme 6.6 (Mautner) *Soit π une représentation unitaire d'un groupe localement compact G. Pour v dans $\mathcal{H}_\pi$, notons $S_v = \{g \in G \ / \ \pi(g)v = v\}$ son stabilisateur dans G. Alors*
a) $S_v = \{g \in G \ / \ c_{v,v}(g) = \|v\|^2\}$.
b) Soit g dans G tel qu'il existe g_n dans G, s_n, s'_n dans S_v avec $\lim_{n\to\infty} g_n = g$, $\lim_{n\to\infty} s_n g_n s'_n = e$. Alors g est dans S_v.

Démonstration a) Utiliser l'égalité $\|\pi(g)v - v\|^2 = 2\|v\|^2 - 2\,\mathrm{Re}(c_{v,v}(g))$.
b) Faire tendre n vers l'infini dans l'égalité $c_{v,v}(g_n) = c_{v,v}(s_n g_n s'_n)$ pour obtenir $c_{v,v}(g) = \|v\|^2$. □

Démonstration de la proposition 6.5 Il suffit de montrer que l'invariance de v par l'un des trois a_t, u_s, u_s^- implique l'invariance par les deux autres. Grâce aux symétries, il n'y a que deux cas à traiter :

$\mathbf{a_t}$-invariant $\Longrightarrow$ $\mathbf{u_s}$-invariant. On peut supposer $t > 1$. On utilise le lemme 6.6.b avec $g_n = g = u_s$, $s_n = a_t^{-n}$ et $s'_n = a_t^n$. On vérifie facilement que $\lim_{n\to\infty} s_n g_n s'_n = \lim_{n\to\infty} u_{t^{-2n}s} = e$.

$\mathbf{u_s}$-invariant $\Longrightarrow$ $\mathbf{a_t}$-invariant. On peut supposer que t est rationnel, $t = \frac{p}{q}$. On utilise le lemme 6.6.b avec $g = a_t$, $g_n = \begin{pmatrix} \frac{p}{q} & 0 \\ \frac{t-1}{snp} & \frac{q}{p} \end{pmatrix}$, $s_n = u_s^{-np}$ and $s'_n = u_s^{nq}$. On vérifie facilement que $\lim_{n\to\infty} s_n g_n s'_n = \lim_{n\to\infty} \begin{pmatrix} 1 & 0 \\ \frac{t-1}{snp} & 1 \end{pmatrix} = e$. □

6.3 Décroissance des coefficients

Dans cette section, nous donnons la preuve du théorème 6.2.

Nous aurons besoin du lemme suivant qui est un cas spécial du corollaire 6.3 que nous n'avons pas encore démontré.

Lemme 6.7 *Soit π une représentation unitaire d'un groupe de Lie réel connexe quasisimple G à centre fini, $a \neq 1$ un élément hyperbolique de G, et $u \neq 1$ un élément unipotent de G. Si un élément v de $\mathcal{H}_\pi$ est soit a-invariant ou u-invariant alors il est G-invariant.*

Rappelons qu'un élément $g \in G$ est *unipotent* (resp. *hyperbolique*) si $g = e^X$ avec $X \in \mathfrak{g}$ et $\mathrm{ad}X$ nilpotent (resp. diagonalisable sur $\mathbb{R}$).

Démonstration 1$^{\mathbf{er}}$ cas : v est a-invariant. Ecrivons $a = e^X$ et décomposons $\mathfrak{g}$ en $\mathfrak{g} = \mathfrak{u} \oplus \mathfrak{l} \oplus \mathfrak{u}^-$ où $\mathfrak{u}$ (resp. $\mathfrak{l}$, $\mathfrak{u}^-$) sont la somme des espaces propres de $\mathrm{ad}X$ associés aux valeurs propres strictement négatives (resp. nulles, strictement positives). Ce sont des sous-algèbres de Lie. On note U (resp L, U^-) les sous-groupes de Lie connexes correspondants. Le même argument que dans la proposition 6.5 montre que v est invariant par U et U^-. On conclut que v est G-invariant grâce au fait suivant : *les deux groupes U et U^- engendrent G*. Pour montrer ce fait, on remarquera juste que la somme directe $\mathfrak{u}^- \oplus ([\mathfrak{u}^-, \mathfrak{u}] \cap \mathfrak{l}) \oplus \mathfrak{u}$ est un idéal de $\mathfrak{g}$ et est donc égal à $\mathfrak{g}$.

2$^{\mathbf{ème}}$ cas : v est u-invariant. Notons $u = e^N$ avec $N \in \mathfrak{g}$ nilpotent. D'après le théorème 2.15 de Jacobson-Morozov, il existe une sous-algèbre de Lie $\mathfrak{s} \simeq \mathfrak{sl}(2, \mathbb{R})$ de $\mathfrak{g}$ contenant X. Par la proposition 6.5, v est invariant par le sous-groupe S d'algèbre de Lie $\mathfrak{s}$. La proposition 2.14 qui classifie les représentations de $\mathfrak{s}$ prouve que S contient des éléments hyperboliques, nous sommes de nouveau dans le premier cas. □

Remarque Lorsque $\mathfrak{g} = \mathfrak{sl}(d, \mathbb{R})$, la démonstration du théorème de Jacobson Morozov est très facile. On veut montrer que *toute matrice nilpotente N est dans l'image d'une représentation de l'algèbre de Lie $\mathfrak{s} = \mathfrak{sl}(2, \mathbb{R})$*. Rappelons que $\mathfrak{s}$ a pour base X, H, Y avec

$$X := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \; H := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \; Y := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

qui vérifient les relations

$$[H, X] = 2X, \;\; [H, Y] = -2Y \;\text{ et }\; [X, Y] = H.$$

Dans une base convenable, N est une matrice formée de blocs de Jordan. On se ramène facilement au cas où N est un seul bloc de Jordan. Or la représentation ρ_d de $\mathfrak{sl}(2,\mathbb{R})$ dans l'espace vectoriel $\mathbf{V}_d$ des polynômes de degré $d-1$ sur $\mathbb{R}^2$ envoie X, H, Y respectivement sur

$$x\frac{\partial}{\partial y} \ , \ x\frac{\partial}{\partial x} - y\frac{\partial}{\partial y} \text{ et } y\frac{\partial}{\partial x}.$$

En particulier, dans la base $x^{d-1}, x^{d-2}y, \ldots, y^{d-1}$, $\rho_d(X)$ est un bloc de Jordan de taille d et $\rho_d(H)$ est diagonale. C'est ce que l'on voulait.

Démonstration du théorème 6.2 L'idée est d'utiliser la compacité faible de la boule unité de $\mathcal{H}_\pi$ et la décomposition de Cartan $G = KA^+K$ de G pour construire dans $\mathcal{H}_\pi$ un vecteur v_0 invariant par un unipotent $u \in G$.

La décomposition de Cartan de G (voir chapitre 3) affirme qu'il existe un sous-groupe compact K de G et une partie A^+, appelée chambre de Weyl, d'un sous groupe commutatif A formé d'éléments hyperboliques tels que $G = KA^+K$.

Si le coefficient $<\pi(g)v, w>$ ne décroit pas vers 0, on peut trouver des suites $g_n = k_n a_n k'_n \in G = KAK$ telles que

$$\lim_n <\pi(g_n)v, w> = \ell \neq 0 \ , \ \lim_n k_n = k \ , \ \lim_n k'_n = k' \ ,$$

et pour certaines racines α de A dans $\mathfrak{g}$, $\lim_n \alpha(a_n) = \infty$. En particulier,il existe un élément unipotent $u \in G$ non trivial tel que $a_n^{-1} u a_n \to e$. On peut supposer que $k = k' = e$.

La compacité faible de la boule unité de $\mathcal{H}_\pi$ affirme que, toute suite $v_n \in \mathcal{H}_\pi$ avec $\|v_n\| \leq 1$ a une sous-suite v_{n_k} qui converge faiblement vers un vecteur v_∞ i.e. pour tout $v' \in \mathcal{H}_\pi$, on a $\lim_{k\to\infty} \langle v_{n_k}, v' \rangle = \langle v_\infty, v' \rangle$.

On peut donc, quitte à extraire, supposer que la suite $\pi(a_n)v$ a une limite faible $v_0 \in \mathcal{H}_\pi$. Vérifions que ce vecteur v_0 est non nul.
Comme $\lim_n \|\pi(k'_n)v - v\| = \lim_n \|\pi(k_n^{-1})v - v\| = 0$, on a bien

$$\begin{aligned} <v_0, w> &= \lim_n <\pi(a_n)v, w> = \lim_n <\pi(a_n)\pi(k'_n)v, \pi(k_n^{-1})w> \\ &= \lim_n <\pi(g_n)v, w> \neq 0 \end{aligned}$$

En outre, ce vecteur est u-invariant, parce que, comme $a_n^{-1} u a_n \to e$, on a

$$\|\pi(u)v_0 - v_0\| \leq \overline{\lim_n} \ \|\pi(a_n)(\pi(a_n^{-1}ua_n)v - v)\| = 0 \ .$$

Ceci contredit le lemme 6.7. □

Remarque Pour $G = \mathrm{SL}(d,\mathbb{R})$, le groupe K est le groupe $\mathrm{SO}(d,\mathbb{R})$ et la chambre de Weyl A^+ est l'ensemble des éléments diagonaux de G à coefficients positifs et rangés en ordre décroissant. La décomposition de Cartan $G = KA^+K$ est une conséquence des deux faits élémentaires suivants. Primo : *toute matrice réelle inversible est (de façon unique) le produit d'une matrice orthogonale et d'une matrice symétrique définie positive.* Secundo : *toute matrice symétrique définie positive est diagonalisable dans une base orthonormée.*

6.4 Comptage des points d'un réseau

Rappelons que notre objectif dans ce chapitre est de compter les points dans $\mathrm{SL}(d,\mathbb{Z})$. Ce comptage sera un corollaire immédiat du théorème général suivant dû à Duke, Rudnick et Sarnak.

Soit $G \hookrightarrow \mathrm{SL}(d,\mathbb{R})$ un sous-groupe de Lie quasisimple connexe, K un sous-groupe compact maximal de G, $\|\|$ une norme euclidienne K-invariante sur $\mathbb{R}^d$. On note de la même façon la norme induite sur les matrices.

Notons $B_r := \{g \in G \mid \|g\| \leq r\}$ la trace sur G de la boule de rayon r.

Soit Γ un réseau de G. On veut estimer $\#(\Gamma \cap B_r)$. Notons λ_G la mesure de Haar sur G que l'on normalise de sorte que la mesure induite λ_X sur le quotient $X := G/\Gamma$ soit de volume 1. Posons $v_r := \lambda_G(B_r)$.

Lorsque f et g sont deux fonctions positives sur $]0,\infty[$, on dira que f et g sont asymptotiquement équivalentes et on notera $f \sim g$ lorsque $\lim_{r\to\infty} \dfrac{f(r)}{g(r)} = 1$.

Théorème 6.8 (Duke, Rudnick, Sarnak) $\#(\Gamma \cap B_r) \sim v_r$

La fin de ce chapitre est consacrée à la démonstration du théorème 6.8. Nous suivrons la démonstration d'Eskin et Mc Mullen.

Corollaire 6.9 *Soit $\|\|$ une norme euclidienne sur $\mathbb{R}^d$ et, pour $g \in \mathrm{GL}(d,\mathbb{R})$, notons $\|g\| = \sup_{\|v\|=1} \|gv\|$. Alors, il existe $c > 0$, tel que,*

$$\#\{g \in \mathrm{SL}(d,\mathbb{Z}) \mid \|g\| \leq r\} \sim c\, r^{d^2-d}.$$

Remarques - Il est possible, à partir du raisonnement ci-dessous de calculer explicitement la constante c.

- La croissance de v_r est donc exponentielle... comme fonction de $R := \log r$.

6.5 Equidistribution des grandes sphères

La première étape de la démonstration consiste à pousser une probabilité K-invariante sur le quotient $X = G/\Gamma$ par de grands éléments de G et à montrer que les mesures obtenues ainsi s'équirépartissent i.e. ces mesures convergent vers la probabilité G-invariante sur X.

Notons $x_0 = \Gamma$ le point base de $X = G/\Gamma$, $Y = Kx_0$ sa K-orbite et λ_Y la probabilité K-invariante sur Y.

Proposition 6.10 *On a* $\lim_{g\to\infty} g_\star \lambda_Y = \lambda_X$.

Cette limite est la limite pour la convergence faible des mesures. Elle signifie que pour toute fonction continue à support compact $\varphi \in C_c(X)$,

$$\lim_{g\to\infty} \int_Y \varphi(gy) d\lambda_Y(y) = \int_X \varphi(x) d\lambda_X(x).$$

Remarque Cette proposition a une signification géométrique importante : elle implique que l'image dans le quotient $\Gamma\backslash G/K$ des "grandes sphères de l'espace symétrique riemannien" G/K s'équirépartissent dans ce quotient.

Démonstration On va non seulement utiliser la décomposition de Cartan $G = KA^+K$ de G comme dans la démonstration du théorème 6.2 mais aussi la décomposition d'Iwasawa $G = U^-AK$ où U^- est le groupe de Lie connexe dont l'algèbre de Lie $\mathfrak{u}^-$ est la somme des espaces radiciels associés aux racines négatives (voir chapitre 3).

1er cas : Supposons que $g = a$ est dans A^+. Fixons $\varepsilon > 0$. Par uniforme continuité de φ, il existe un voisinage ouvert G_ε de e dans G tel que

$$|\varphi(ux) - \varphi(x)| \leq \varepsilon \quad \text{pour tout } u \in G_\varepsilon \text{ et } x \in X.$$

Soit W le groupe résoluble $W = U^-A$. La décomposition d'Iwasawa donne un difféomorphisme $W \times K \to G; (w,k) \mapsto wk$. Dans cette carte, la mesure de Haar λ_G de G est le produit $\lambda_W \otimes \lambda_K$ de la mesure de Haar à gauche de W et de la mesure de Haar de K.

Comme l'action adjointe de A^+ sur l'algèbre de Lie de W est simultanément diagonalisable avec des valeurs propres toujours de modules au plus 1, on peut trouver un ouvert $W_\varepsilon \subset W \cap G_\varepsilon$ tel que

$$aW_\varepsilon a^{-1} \subset W_\varepsilon \quad \text{pour tout } a \in A^+.$$

Par compacité de K, on peut aussi supposer W_ε suffisamment petit pour que l'application $W_\varepsilon \times Y \to X; (w,y) \mapsto wy$ soit un difféomorphisme sur son image $W_\varepsilon Y \subset X$. Notons alors β_ε la fonction L^2 sur X, $\beta_\varepsilon = \frac{1}{\lambda_X(W_\varepsilon Y)} \mathbf{1}_{W_\varepsilon Y}$. On veut montrer que, lorsque $a \in A^+$ tend vers l'infini, l'intégrale

$$I_a := \int_Y \varphi(ay) d\lambda_Y(y)$$

converge vers $I := \int_X \varphi(x) d\lambda_X(x)$. Pour cela on compare l'intégrale I_a à l'intégrale

$$J_a := \int_X \varphi(ax) \beta_\varepsilon(x) d\lambda_X(x).$$

D'une part, la propriété de mélange pour l'action de G sur X (corollaire 6.4) prouve que

$$\lim_{a\to\infty} J_a = I.$$

D'autre part, pour tout $a \in A^+$, on a

$$J_a = \frac{1}{\lambda_W(W_\varepsilon)} \int_{W_\varepsilon \times Y} \varphi(awy) d\lambda_W(w) d\lambda_Y(y)$$

et, par le choix de W_ε, on a, en écrivant $awy = (awa^{-1})ay$,

$$|\varphi(awy) - \varphi(ay)| \leq \varepsilon \text{ pour tout } w \in W_\varepsilon \text{ et } a \in A^+.$$

On en déduit la majoration,

$$|I_a - J_a| \leq \varepsilon \text{ pour tout } a \in A^+.$$

Donc pour a suffisamment grand, on a $|I_a - I| \leq 2\varepsilon$ et donc $\lim_{a\to\infty} I_a = I$.

2ème cas : Cas général. On peut supposer que g tend vers l'infini selon une suite g_n. Ecrivons grâce à la décomposition de Cartan $g_n = k_n a_n k'_n$ avec $k_n, k'_n \in K$ et $a_n \in A^+$. La K-invariance de λ_Y permet de supposer $k'_n = 1$. Comme K est compact, on peut aussi supposer que la suite k_n converge vers un élément $k_\infty \in K$. La suite de fonctions $\varphi \circ k_n$ converge alors uniformément vers $\varphi \circ k_\infty$. On a donc, en utilisant le premier cas,

$$\begin{aligned} \lim_{n\to\infty} \int_Y \varphi(g_n y) d\lambda_Y(y) &= \lim_{n\to\infty} \int_Y \varphi(k_\infty a_n y) d\lambda_Y(y) \\ &= \int_X \varphi(k_\infty x) d\lambda_X(x) = \int_X \varphi(x) d\lambda_X(x). \end{aligned}$$

C'est ce que l'on voulait. □

Remarque Pour $G = \mathrm{SL}(d, \mathbb{R})$, La décomposition d'Iwasawa $G = U^- AK$ est une conséquence du procédé d'orthonormalisation de Gramm-Schmidt qui affirme que *toute matrice réelle inversible est (de façon unique) le produit d'une matrice orthogonale et d'une matrice triangulaire inférieure à coefficients diagonaux positifs.*

6.6 Comptage faible

> Dans la deuxième étape de la démonstration du théorème 6.8, plutôt que d'estimer directement le nombre N_r de points de Γ dans une boule B_r, on va tout d'abord estimer une moyenne sur g du nombre de points des translatés $g\Gamma$ dans ces boules B_r.

On introduit donc la fonction

$$\begin{aligned} F_r : X &\to \mathbb{N} \\ x = g\Gamma &\mapsto F_r(x) := \#(B_r \cap g\Gamma) = \sum_{\gamma\in\Gamma} \mathbf{1}_{B_r}(g\gamma). \end{aligned}$$

Lemme 6.11 *On a la convergence faible* $\lim_{r\to\infty} \dfrac{F_r}{v_r} = 1$.

Autrement dit, pour toute fonction continue à support compact $\varphi \in C_c(X)$,

$$\lim_{r\to\infty} \frac{1}{v_r} \int_X F_r(x)\varphi(x) d\lambda_X(x) \;=\; \int_X \varphi(x) d\lambda_X(x).$$

Démonstration On commence par un simple calcul du membre de gauche, en remarquant que la boule B_r est K-invariante.

$$\begin{aligned}
\frac{1}{v_r} \int_X F_r(x)\varphi(x) d\lambda_X(x) &= \frac{1}{v_r} \int_{G/\Gamma} \sum_{\gamma\in\Gamma} \mathbf{1}_{B_r}(g\gamma)\varphi(gx_0) d\lambda_X(g\Gamma) \\
&= \frac{1}{v_r} \int_G \mathbf{1}_{B_r}(g)\varphi(gx_0) d\lambda_G(g) \\
&= \frac{1}{v_r} \int_{B_r} \left(\int_K \varphi(gkx_0) d\lambda_K(k) \right) d\lambda_G(g)
\end{aligned}$$

La proposition 6.10 assure que la fonction $g \to \int_K \varphi(gkx_0) d\lambda_K(k)$ converge pour $g \to \infty$ vers la constante $\int_X \varphi(x) d\lambda_X(x)$. La moyenne de cette fonction sur la boule B_r a la même limite pour $r \to \infty$ car le volume v_r tend vers l'infini. □

6.7 Estimation de volumes

La dernière étape de la démonstration du théorème 6.8 consiste à déduire le comptage à partir du comptage faible. Pour cela on a besoin d'un équivalent asymptotique pour le volume v_r. Nous ne démontrerons cet équivalent que pour $G = \mathrm{SL}(d, \mathbb{R})$.

Lemme 6.12 *Il existe* $a > 0$, $b \geq 0$, $c > 0$ *tels que* $v_r \sim c\, r^a (\log r)^b$.

Montrons tout d'abord comment on en déduit le comptage.

Démonstration du théorème 6.8 Fixons $\varepsilon > 0$. Introduisons l'ouvert de G, $G_\varepsilon := \{g \in G \mid \max(\|g\|, \|g^{-1}\|) \leq e^\varepsilon\}$. C'est, pour ε petit, un petit voisinage de l'identité dans G que l'on peut identifier via la projection $p : G \to X = G/\Gamma$ à un voisinage de x_0. Choisissons une fonction continue positive $\widetilde{\varphi} \in C_c(G)$ d'intégrale égale à 1 et dont le support est inclus dans G_ε. Notons $\varphi \in C_c(X)$ la fonction à support dans $p(G_\varepsilon)$, donnée par $\varphi(p(g)) = \widetilde{\varphi}(g)$, pour tout $g \in G_\varepsilon$. On a donc les inégalités

$$\widetilde{\varphi}(g)\mathbf{1}_{B_{re^{-\varepsilon}}}(g\gamma) \leq \widetilde{\varphi}(g)\mathbf{1}_{B_r}(\gamma) \leq \widetilde{\varphi}(g)\mathbf{1}_{B_{re^{\varepsilon}}}(g\gamma),$$

En sommant ces inégalités pour $\gamma \in \Gamma$ et en les intégrant pour $g \in G_\varepsilon$, on obtient,

$$\frac{1}{v_r} \int_X \varphi(x) F_{re^{-\varepsilon}}(x) d\lambda_X(x) \leq \frac{1}{v_r} N_r \leq \frac{1}{v_r} \int_X \varphi(x) F_{re^{\varepsilon}}(x) d\lambda_X(x).$$

En faisant tendre r vers l'infini, on obtient, grâce au lemme 6.11 de comptage faible et au lemme 6.12 qui donne l'asymptotique du volume

$$e^{-a\varepsilon} = \lim_{r\to\infty} \frac{v_{re^{-\varepsilon}}}{v_r} \leq \liminf_{r\to\infty} \frac{N_r}{v_r} \leq \limsup_{r\to\infty} \frac{N_r}{v_r} \leq \lim_{r\to\infty} \frac{v_{re^{\varepsilon}}}{v_r} = e^{a\varepsilon}.$$

Comme $\varepsilon > 0$ est arbitrairement petit, le quotient $\frac{N_r}{v_r}$ tend bien vers 1. □

Pour montrer le lemme 6.12, nous aurons besoin de la formule suivante pour la mesure de Haar dans la décomposition de Cartan $G = KA^+K$. On note, comme dans la section 3.5, Σ^+ l'ensemble des racines positives de A^+ dans $\mathfrak{g}$ et m_α la dimension de l'espace radiciel $\mathfrak{g}_\alpha$ associé à une racine α.

Lemme 6.13 *Il existe $c_0 > 0$, tel que, pour tout $f \in C_c(G)$, on a*

$$\int_G f(g)dg = c_0 \int_{K\times\mathfrak{a}^+\times K} f(ke^X k') \left(\prod_{\alpha\in\Sigma^+} \sinh(\alpha(X))^{m_\alpha} \right) dk dX dk'.$$

Nous avons simplifié dans cette formule les notations $d\lambda_G(g)$ et $d\lambda_K(k)$ en dg et dk, et nous avons considéré les racines restreintes α comme des formes linéaires sur $\mathfrak{a}$ et noté $\mathfrak{a}^+ = \log(A^+) = \{X \in \mathfrak{a} \mid \alpha(X) \geq 0, \text{ pour tout } \alpha \in \Sigma^+\}$.

Nous admettrons cette formule 6.13 dont la démonstration se ramène à un calcul de Jacobien et peut être trouvée dans le livre de Helgason p.186.

Démonstration du corollaire 6.9 et du lemme 6.12 pour $\mathrm{SL}(d,\mathbb{R})$
C'est un calcul dont nous donnons simplement les grandes lignes. Appliquons la formule pour la mesure de Haar pour $G = \mathrm{SL}(d,\mathbb{R})$, en notant les éléments $X \in \mathfrak{a}^+$ sous la forme

$$X = \mathrm{diag}(u, u - t_1, \dots, u - t_1 - \cdots - t_{d-1}),$$

avec $u = \frac{1}{d}\left((d-1)t_1 + (d-2)t_2 + \cdots + t_{d-1}\right)$. On obtient,

$$v_r = c_0 \int_{[0,\infty[^{d-1}} \mathbf{1}_{\{e^u \leq r\}} \prod_{1\leq i<j\leq d-1} \sinh(t_i + \cdots + t_j) dt_1 \dots dt_{d-1}.$$

On cherche un équivalent pour v_r. Pour tout $\varepsilon > 0$, on obtiendra le même équivalent en restreignant l'intégrale au cône donné par $\max(t_1, \dots, t_{d-2}) \leq \varepsilon t_{d-1}$. On peut donc remplacer les $d-1$ facteurs $\sinh(t_i + \cdots + t_{d-1})$ par $\frac{1}{2}e^{t_i+\cdots+t_{d-1}}$ sans changer l'équivalent. On intègre alors en la variable t_{d-1} sur l'intervalle $[0, d\log r - (d-1)t_1 - \cdots - 2t_{d-2}]$. Tous calculs faits, on obtient, avec une intégrale qui est finie,

$$v_r \sim \frac{c_0\, r^{d(d-1)}}{(d-1)2^{d-1}} \int_{[0,\infty[^{d-2}} \prod_{1\leq i<j\leq d-2} \sinh(t_i + \cdots + t_j) \prod_{1\leq i\leq d-2} e^{-d(d-i-1)t_i} dt_1 \dots dt_{d-2}.$$

On obtient bien l'équivalent $v_r = c\, r^{d(d-1)}$ annoncé où c/c_0 est un nombre rationnel. □

7 Réseaux

Nous étudions dans cette partie les réseaux Γ des groupes de Lie semisimples réels. En particulier comment une action de Γ induit une action Γ-équivariante entre les bords. L'étude des propriétés de cette application aux bords sera la clef de la superrigidité. Les applications les plus intéressantes de ces méthodes, par exemple le théorème d'arithméticité, nous obligent à travailler non seulement sur $\mathbb{R}$ ou $\mathbb{C}$ mais aussi sur des extensions finies de $\mathbb{Q}_p$.

7.1 Zariski densité des réseaux

Le théorème suivant, dû à Borel, est souvent bien utile. La démonstration ci-dessous, due à Furstenberg, est bien dans l'esprit de ce cours : Elle utilise, d'une part, un théorème de Chevalley sur les espaces homogènes de groupes algébriques et, d'autre part, l'étude des groupes de transformations linéaires qui préservent une probabilité sur l'espace projectif.

Théorème 7.1 *Soient $k = \mathbb{R}$ et $G = \mathbf{G}_k$ le groupe des k-points d'un k-groupe Zariski connexe. On suppose qu'il n'existe pas de sous-groupe distingué Zariski fermé $G' \subsetneq G$ tel que le quotient G/G' est compact. Alors tout réseau Γ de G est Zariski dense.*

Remarque L'hypothèse du théorème 7.1 est très facile à vérifier en pratique. Elle est satisfaite par exemple lorsque G est quasisimple et isotrope.

Plus généralement, soit G le produit d'un nombre fini de groupes G_p avec p premier ou ∞, où G_p est le groupe des $\mathbb{Q}_p$-points d'un $\mathbb{Q}_p$-groupe Zariski connexe et où $\mathbb{Q}_\infty = \mathbb{R}$. On appelle *topologie de Zariski* sur G la topologie produit des topologies de Zariski sur les G_p. Alors, la même preuve donnera aussi.

Théorème 7.1 (bis) *Soit G le produit d'un nombre fini de groupes G_p avec p premier ou ∞, où G_p est le groupe des $\mathbb{Q}_p$-points d'un $\mathbb{Q}_p$-groupe Zariski connexe.*

On suppose qu'il n'existe pas de sous-groupe distingué Zariski fermé $G' \subsetneq G$ tel que le quotient G/G' est compact. Alors tout réseau de G est Zariski dense dans G.

Démonstration du théorème 7.1 Soit $\mathbf{H}$ l'adhérence de Zariski de Γ. D'après le lemme 7.2 ci-dessous, le groupe $\mathbf{H}$ est défini sur k. D'après le théorème 4.6 de Chevalley, il existe une k-représentation ρ de $\mathbf{G}$ dans un espace vectoriel $\mathbf{V} = K^d$ de dimension d et une droite $x_0 \in \mathbb{P}(k^d)$ dont $\mathbf{H}$ est le stabilisateur : $\mathbf{H} = \{g \in \mathbf{G} \mid \rho(g)x_0 = x_0\}$. On peut supposer que l'orbite $\mathbf{G}x_0$ engendre K^d. Par la proposition 4.8, le groupe G est Zariski dense dans $\mathbf{G}$ et donc Gx_0 engendre l'espace vectoriel

k^d. Cette même proposition et le corollaire 4.5 prouvent aussi que le groupe image $\rho(G)$ est fermé dans les k-points du groupe algébrique image $\rho(\mathbf{G}) \subset \mathbf{PGL}_d$.

Comme x_0 est Γ-invariant, on a une application G-équivariante $i : G/\Gamma \to \mathbb{P}(k^d)$ donnée par $i(g\Gamma) = \rho(g)x_0$. La probabilité $i_*(\mu)$ image de la probabilité G invariante μ sur G/Γ est une probabilité $\rho(G)$-invariante sur $\mathbb{P}(k^d)$. Le lemme 7.3 ci-dessous prouve alors que $\rho(G)$ est compact pour la topologie analytique. Ceci contredit notre hypothèse à moins que $\rho(G) = 1$. On a donc $\mathbf{H} = \mathbf{G}$. □

Lemme 7.2 *Soit $k \subset K$ deux corps, $\mathbf{V} = K^d$ et $\mathbf{Z} \subset K^d$ une K-variété telle que l'ensemble des k-points $\mathbf{Z}_k$ est Zariski dense dans $\mathbf{Z}$. Alors $\mathbf{Z}$ est définie sur k.*

Démonstration du lemme 7.2 Soit $I \subset K[\mathbf{V}]$ l'idéal annulateur de $\mathbf{Z}$ et $I^m = I \cap K^m[\mathbf{V}]$. Comme $\mathbf{Z}_k$ est Zariski dense dans $\mathbf{Z}$, les sous-espaces I^m sont définis par un système d'équations linéaires à coefficients dans k. Ils ont donc une base à coefficients dans k. L'idéal I aussi. □

Lemme 7.3 (Furstenberg) *Soit $k = \mathbb{R}$, $\mathbb{C}$ ou une extension finie de $\mathbb{Q}_p$. Soient $E = k^d$, $\mathbb{P}(E)$ l'espace projectif de E, $\mathrm{PGL}(E)$ le groupe des transformations projectives de E et ν une probabilité sur $\mathbb{P}(E)$. Supposons que le support de ν ne peut être inclus dans une réunion $\mathbb{P}(E_1) \cup \mathbb{P}(E_2)$ pour deux sous-espaces propres $E_1, E_2 \subsetneq E$ tels que $\dim E_1 + \dim E_2 = \dim E$. Alors*
a) le stabilisateur $S := \{g \in \mathrm{PGL}(E) \mid g_*\nu = \nu\}$ de ν est compact.
b) Plus généralement, il n'existe pas de probabilité μ sur $\mathbb{P}(E)$ et de suite $g_p \in G$ non bornée telle que $\lim_{p\to\infty} (g_p)_*\mu = \nu$.

Démonstration Il est clair que S est fermé. Il suffit donc de montrer le point b). Supposons par l'absurde que μ et g_p existent. Quitte à extraire, on peut supposer que la suite g_p a une limite $g \in \mathbb{P}(\mathrm{End}E)$ qui n'est pas inversible. Notons $\mathrm{Ker}g$ et $\mathrm{Im}g$ le noyau et l'image de g. Plus précisément il s'agit du noyau et de l'image communs à tous les éléments non nuls de la droite g. On peut supposer que la limite $E_1 = \lim_{p\to\infty} g_p(\mathrm{Ker}g)$ existe et on pose $E_2 = \mathrm{Im}g$.

Remarquons que si $x \notin \mathbb{P}(\mathrm{Ker}g)$, alors $\lim_{p\to\infty} g_p x = gx \in \mathbb{P}(E_2)$ et que si $x \in \mathbb{P}(\mathrm{Ker}g)$, alors toutes les valeurs d'adhérence de la suite $g_p x$ sont dans $\mathbb{P}(E_1)$.

Donc, pour toute fonction φ continue à support dans $\mathbb{P}(E) - (\mathbb{P}(E_1) \cup \mathbb{P}(E_2))$, le théorème de convergence dominée prouve que

$$\int_{\mathbb{P}(E)} \varphi \circ g_p \, d\mu \longrightarrow 0.$$

Mais cette limite est $\int_{\mathbb{P}(E)} \varphi \, d\nu$. Donc cette intégrale est nulle. Le support de ν est inclus dans $\mathbb{P}(E_1) \cup \mathbb{P}(E_2)$. Contradiction. □

7.2 Réseaux irréductibles

Nous montrons dans cette section que l'étude des réseaux des groupes de Lie semisimples se ramène à celle des réseaux irréductibles.

On dit qu'un groupe localement compact G est *presque produit* de sous-groupes distingués fermés H_i si la multiplication $\prod_i H_i \to G$ a un noyau fini et une image d'indice finie dans G. On dit qu'un groupe G est *sans facteur compact* si il n'admet pas de décomposition en presque produit H_1H_2 avec H_1 compact infini.

Par exemple, soit $k = \mathbb{R}$, $\mathbb{C}$ ou une extension finie de $\mathbb{Q}_p$. Le groupe G des k-points d'un k-groupe $\mathbf{G}$ semisimple est presque produit des groupes G_j des k-points de ses facteurs k-quasisimples $\mathbf{G}_j$. Le groupe G est sans facteur compact ssi le k-groupe $\mathbf{G}$ n'a pas de facteur $\mathbf{G}_j$ qui soit k-anisotrope.

Définition 7.4 *Un réseau Γ d'un groupe localement compact G est dit réductible si G admet une décomposition en presque produit H_1H_2 où H_1 et H_2 sont des sous-groupes distingués fermés infinis tels que $(\Gamma \cap H_1)(\Gamma \cap H_2)$ est d'indice fini dans Γ.*

Le réseau Γ est dit irréductible sinon.

Exemples - Tout réseau du groupe $G = \mathbf{G}_k$ des k-points d'un k-groupe $\mathbf{G}$ connexe k-quasisimple est irréductible.

- Le groupe $\Gamma = \{(g, g^\sigma) \mid g \in \mathrm{SL}(2, \mathbb{Z}[\sqrt{2}])\}$, où σ est l'automorphisme non trivial du corps $\mathbb{Q}[\sqrt{2}]$, est un réseau irréductible de $\mathrm{SL}(2,\mathbb{R}) \times \mathrm{SL}(2,\mathbb{R})$.

- Le groupe $\Gamma = \{(g, g) \mid g \in \mathrm{SL}(2, \mathbb{Z}[\frac{1}{p}])\}$ est un réseau irréductible de $\mathrm{SL}(2,\mathbb{R}) \times \mathrm{SL}(2,\mathbb{Q}_p)$.

Proposition 7.5 *Soit $k = \mathbb{R}$ et $G = \mathbf{G}_k$ le groupe des k-points d'un k-groupe $\mathbf{G}$ semisimple connexe. On suppose G sans facteur compact. Donnons-nous une décomposition $G = H_1H_2$ de G en presque produit de deux sous-groupes distingués H_i et notons $\Gamma_i := \Gamma \cap H_i$ et $\pi_i : G \to G/H_i$ la projection. Alors les assertions suivantes sont équivalentes :*
i) $\pi_1(\Gamma)$ *est discret.*
ii) Γ_1 *est un réseau de* H_1.
iii) $\pi_2(\Gamma)$ *est discret.*
iv) Γ_2 *est un réseau de* H_2.
v) $\Gamma_1\Gamma_2$ *est d'indice fini dans* Γ.

Remarque Plus généralement, la conclusion et la démonstration de la proposition 7.5 est valable pour un groupe G sans facteur compact qui est produit d'un nombre fini de groupes G_p avec p premier ou ∞, où G_p est le groupe des $\mathbb{Q}_p$-points d'un $\mathbb{Q}_p$-groupe semisimple connexe.

Démonstration de la proposition 7.5

i) $\rightarrow$ *ii)* Cela résulte de la fibration $H_1/\Gamma_1 \rightarrow G/\Gamma \rightarrow H_2/\pi_1(\Gamma)$.

ii) $\rightarrow$ *iii)* Le groupe $\Gamma_1' := \pi_2(\Gamma_1)$ est donc un réseau de $H_1' := G/H_2$ normalisé par le groupe $\Delta_1 := \pi_2(\Gamma)$. Or, le normalisateur N de Γ_1' dans H_1' est discret. En effet, les petits éléments de N commutent avec les éléments de Γ_1', donc l'algèbre de Lie $\mathfrak{n}$ de N est centralisé par les éléments de Γ_1'. Comme G est sans facteur compact, le théorème de densité de Borel prouve que H_1' centralise $\mathfrak{n}$. Donc $\mathfrak{n} = 0$, N est discret et Δ_1 aussi.

iii) $\rightarrow$ *iv)* et *iv)* $\rightarrow$ *i)* se montrent comme ci-dessus.

ii) $+$ *iv)* $\rightarrow$ *v)* Le groupe $\Gamma_1\Gamma_2$ est un réseau de G inclus dans le réseau Γ. Il est donc d'indice fini égal au rapport des covolumes.

v) $\rightarrow$ *ii)* $+$ *iv)* Si l'un des Γ_i n'est pas un réseau dans H_i le groupe discret $\Gamma_1\Gamma_2$ ne peut pas être un réseau dans le presque produit H_1H_2. □

Lemme 7.6 *Soit $k = \mathbb{R}$ et $G = \mathbf{G}_k$ le groupe des k-points d'un k-groupe $\mathbf{G}$ semisimple connexe. On suppose G sans facteur compact. Pour tout réseau Γ de G, il existe une décomposition $\mathbf{G} = \mathbf{H}_1 \cdots \mathbf{H}_m$ en presque produit de k-sous-groupes distingués connexes $\mathbf{H}_i$ tels que, pour tout i, $\Gamma \cap H_i$ est un réseau irréductible du groupe H_i des k-points de $\mathbf{H}_i$.*

Cette décomposition est unique

Démonstration On prend pour $\mathbf{H}_i$ les k-sous-groupes distingués connexes minimaux de $\mathbf{G}$ pour lesquels $\Gamma \cap H_i$ est un réseau du groupe H_i.

Par minimalité, $\Gamma \cap H_i$ est un réseau irréductible de H_i. En effet un sous-groupe distingué fermé de H_i est ouvert dans son adhérence de Zariski.

D'après la proposition 7.5, le produit des $\mathbf{H}_i$ est égal à $\mathbf{G}$. Il reste à vérifier que, pour tout $i \neq j$, $\mathbf{H}_i \cap \mathbf{H}_j$ est fini. Grace à la proposition 7.5, il suffit pour cela de remarquer que, comme les images de Γ dans G/H_i et G/H_j sont discrètes, l'image de Γ dans $G/(H_i \cap H_j)$ est aussi discrète. □

Le théorème d'ergodicité de Howe Moore s'étend facilement aux réseaux irréductibles.

Corollaire 7.7 *Soient $k = \mathbb{R}$ et $G = \mathbf{G}_k$ le groupe des k-points d'un k-groupe semisimple, $\Gamma \subset G$ un réseau irréductible. Notons G_e le plus petit sous-groupe ouvert de G et supposons que $\Gamma G_e = G$. Alors, l'action de G est mélangeante sur $X = G/\Gamma$. En particulier, pour tout élément $g \in G$ qui engendre un sous-groupe non-borné de G, l'action de g sur X est ergodique*

Remarque Comme $k = \mathbb{R}$, le groupe G_e est la composanre connexe de G. Mais bien sûr, le corollaire est encore valable pour une extension finie k de $\mathbb{Q}_p$.

Démonstration du corollaire 7.7 D'après le théorème 6.2, il suffit de remarquer que pour tout sous-groupe distingué fermé non compact G' de G les seules fonctions G'-invariantes de $L^2(X, dx)$ sont les fonctions constantes.

Soit φ une telle fonction. On peut supposer que G' est le plus grand sous-groupe distingué laissant φ invariante. On peut aussi supposer φ bornée. Supposons par l'absurde que $\dim G' < \dim G$. Comme G' est distingué, on peut voir φ comme une fonction mesurable sur G invariante par translation à droite par le groupe $G'\Gamma$. Comme la translation de G sur $L^\infty(G)$ pour la topologie faible est continue, φ est aussi invariante par le groupe H adhérence de $G'\Gamma$. Comme Γ est irréductible, la proposition 7.5 prouve que l'on a $\dim H > \dim G'$. Par Zariski densité, l'algèbre de Lie $\mathfrak{h}$ de H est un idéal de $\mathfrak{g}$. Ceci contredit la maximalité de G'. Donc G' est ouvert dans G. L'hypothèse $G = \Gamma G_e$ assure alors que $G' = G$. □

7.3 Groupes moyennables

Un espace vectoriel topologique localement convexe est dit *espace de Fréchet* s'il est métrisable et complet.

Définition 7.8 *Un groupe topologique G est moyennable si, pour tout espace de Fréchet E, tout compact convexe non vide $C \subset E$ et toute action linéaire continue de G sur E laissant stable C, il existe un point fixe c de G dans C.*

Voici quelques exemples.

Lemme 7.9 *a) Un groupe compact est moyennable.*
b) Un groupe abélien est moyennable.
c) Une extension de groupes moyennables est moyennable.
d) Un groupe de Lie semisimple connexe non compact n'est pas moyennable.

Démonstration a) Notons G ce groupe compact et dg sa probabilité de Haar. Alors, pour tout point $v \in C$, le barycentre $c := \int_G g.v\, dg$ convient.

b) Notons G ce groupe abélien. Pour tout sous-groupe H de G, on note E^H le Fréchet $E^H := \{v \in E \mid Hv = v\}$ et C^H le compact convexe $C^H := C \cap E^H$. On veut montrer que C^G est non vide. Montrons tout d'abord que si H est engendré par un élément g, alors C^H est non vide. On emploie l'argument classique de Kakutani. On part d'un point $v \in C$ et on considère la suite $v_n = \frac{1}{n}(v + \cdots + g^{n-1}v)$ dans C. Elle admet une valeur d'adhérence $c \in C$. Comme $g^n v$ reste dans C, la suite $gv_n - v_n = \frac{1}{n}(g^n v - v)$ converge vers 0. Donc le point c est g invariant.

Par récurrence sur le nombre de générateurs, on en déduit que, pour tout sous-groupe H de type fini de G, on a $C^H \neq \emptyset$. Cette famille de compacts non vide C^H est stable par intersection finie, donc l'intersection C^G de tous ces compacts est non vide. Le groupe G a bien un point fixe dans C.

c) Notons $1 \to H \to G \to K \to 1$ cette extension où H et K sont moyennable. Comme H est moyennable l'ensemble $C^H := \{v \in C \mid Hv = v\}$ est un compact convexe non vide du Fréchet $E^H := \{v \in E \mid Hv = v\}$ sur lequel le groupe moyennable $K = G/H$ agit continument. Le groupe K a donc un point fixe dans C^H, c'est le point cherché.

d) Notons G ce groupe de Lie semisimple, P un sous-groupe parabolique minimal de G, $X = G/P$, $E = \mathcal{M}(X)$ l'espace des mesures finies sur X. Comme X est compact, E est le dual de l'espace $C(X)$ des fonctions continues sur X. On munit $C(X)$ de la norme $\|\varphi\|_\infty = \sup_{x\in X} |\varphi(x)|$. On munit E de la topologie faible : elle est définie par la famille de semi-normes $p_\varphi : \mu \to p_\varphi(\mu) = \left|\int_X \varphi \, d\mu\right|$ avec $\varphi \in C(X)$. C'est un Fréchet.

Soit $C = \mathcal{P}(X) \subset E$ le convexe des probabilités sur X. Ce convexe C est un fermé dans la boule unité de E pour la norme forte $\|\mu\| = \sup_{\|\varphi\|_\infty=1} |P_\varphi(\mu)|$. Comme la boule unité est faiblement compact, C aussi.

Mais G n'a pas de points fixes dans C. En effet, le compact maximal K de G agit transitivement sur X. Il y a donc une seule probabilité K-invariante ν sur X. Malheureusement cette probabilité n'est pas invariante par un élément a de l'intérieur de la chambre de Weyl car, en notant x_0 le point base de G/P, pour tout x dans l'ouvert $U^- x_0$, on a $\lim_{n\to\infty} a^n x = x_0$. □

Corollaire 7.10 *a) Un groupe de Lie connexe est moyennable ssi le quotient par son radical résoluble est compact.*
b) Soit G un groupe de Lie réel semisimple connexe et P un sous-groupe parabolique minimal de G. Alors P est moyennable.

Démonstration a) Cela résulte directement du lemme 7.9.
b) Cela résulte du théorème 3.14.b et du lemme 7.9. □

Remarques - On a donc trouvé dans G un sous-groupe moyennable P tel que le quotient G/P est compact.

- Plus généralement, soit $k = \mathbb{R}$, $\mathbb{C}$ ou une extension finie de $\mathbb{Q}_p$. Soit $\mathbf{G}$ un k-groupe semisimple et $\mathbf{P}$ un k-sous-groupe parabolique minimal. Alors le groupe $\mathbf{P}_k$ est moyennable et le quotient $\mathbf{G}_k/\mathbf{P}_k$ est compact.

7.4 L'application aux bords

Partant de l'action d'un réseau Γ sur un espace compact X, on va construire une *application aux bords*.

Proposition 7.11 (Furstenberg) *Soient G un groupe de Lie semisimple, $\Gamma \subset G$ un réseau et $P \subset G$ un sous-groupe parabolique minimal. Pour toute action continue de Γ sur un espace métrique compact X, il existe une application mesurable Γ-équivariante $\Phi : G/P \to \mathcal{P}(X)$.*

- Rappelons qu'on a noté $\mathrm{C}(X) := \{$fonctions continues sur $X\}$, $\mathcal{M}(X) := \{$mesures bornées sur $X\}$ et $\mathcal{P}(X) := \{$probabilités sur $X\}$.

- Nous avons muni implicitement G/P d'une mesure G-quasiinvariante, par exemple une mesure K-invariante ν_0.

- *Mesurable* signifie que pour toute partie borelienne E' de l'espace métrique compact $\mathcal{P}(X)$, l'image inverse $\Phi^{-1}(E')$ est mesurable dans G/P i.e. égale à une partie borélienne G/P modulo une partie négigable.

- Γ-*équivariante* signifie que pour tout $\gamma \in \Gamma$ et presque tout $\xi \in G/P$, on a $\Phi(\gamma\xi) = \gamma\Phi(\xi)$.

- L'application Φ est appelée *application aux bords*, puisque G/P peut être vue comme un bord de l'espace symétrique G/K.

Démonstration Soit $F := L^1_\Gamma(G, \mathrm{C}(X))$ l'espace des applications mesurables Γ-équivariantes $f : G \to \mathrm{C}(X)$ telles que $\|f\| := \displaystyle\int_{\Gamma\backslash G} \|f(g)\|_\infty dg < \infty$. Soit $E := L^\infty_\Gamma(G, \mathcal{M}(X))$ l'espace des applications mesurables bornées Γ-équivariantes $m : G \to \mathcal{M}(X)$. La dualité

$$< m, f >:= \int_{\Gamma\backslash G} < m(g), f(g) > dg$$

identifie E avec le dual continu F, parce que si Y est un domaine fondamental de Γ dans G, on a $F \simeq L^1(Y, \mathrm{C}(X))$ et $E \simeq L^\infty(Y, \mathrm{C}(X)^\star) \simeq F^\star$. La partie $A = L^\infty_\Gamma(G, \mathcal{P}(X)) \subset E$ est convexe, fermée et bornée, elle est donc faiblement compacte. La translation à droite sur G induit des actions continues de G sur F, E et A.

Par le corollaire 7.10.b, le groupe P est moyennable, il a donc un point fixe Φ dans A. Ce point Φ est l'application mesurable cherchée. En effet, un élément P-invariant de E est presque sûrement égal à une fonction mesurable qui est constante sur les orbites de P. □

- Cette application au bord jouera pour le théorème de superrigidité le rôle de l'application au bord construite par Mostow par des méthodes géométriques pour montrer son théorème de rigidité. Nous aurons besoin d'outils issus de la théorie ergodique pour l'exploiter

8 Théorie ergodique

Ce court chapitre est constitué de rappels de théorie ergodique, en vue de leur utilisation dans la démonstration du théorème de superrigidité et du théorème de Ratner.

8.1 Probabilités ergodiques

Soit $(X, \mathcal{B}, \mu, f)$ un système dynamique probabilisé, autrement dit $\mathcal{B}$ est une σ-algèbre de parties de X, μ est une mesure de probabilité sur $\mathcal{B}$ et $f : X \to X$ une application $\mathcal{B}$-mesurable qui préserve μ.

Plus généralement, soit f une transformation $\mathcal{B}$-mesurable qui préserve la classe de μ.

Définition 8.1 *On dit que f est ergodique (pour μ) si toute partie mesurable f-invariante est négligeable ou de complémentaire négligeable, i.e. pour tout $A \in \mathcal{B}$, $f^{-1}(A) = A \Longrightarrow \mu(A) = 0$ ou 1.*

Remarque Lorsque la transformation f est sous-entendue, c'est la mesure μ que l'on qualifie d'ergodique.

La proposition suivante donne une interprétation L^2 de l'ergodicité d'une transformation f qui préserve une probabilité μ. Cette interprétation relie donc les propriétés dynamiques de f aux propriétés spectrales de l'opérateur unitaire $U_f : \varphi \mapsto \varphi \circ f$ de $L^2(X, \mu)$.

Proposition 8.2 *La transformation f est ergodique ssi les fonctions constantes sont les seuls éléments f-invariants de $L^2(X, \mu)$.*

Démonstration $\Leftarrow$ La fonction caractéristique $\varphi = \mathbf{1}_A$ d'une partie f-invariante est un élément f-invariant de $L^2(X, \mu)$. On a donc $\varphi = 0$ ou $\varphi = 1$.

$\Rightarrow$ Soit $\varphi \in L^2(X, \mu)$ un élément f-invariant. Cela signifie que $\varphi \circ f = \varphi$ μ-presque sûrement. Une telle fonction φ est μ-presque sûrement égale à une fonction φ_0 telle que $\varphi_0(x) = \varphi_0(f(x))$ pour tout $x \in X$. Les parties $A_t = \varphi_0^{-1}([t, \infty))$ sont f-invariantes et donc de mesure 0 ou 1. La fonction φ_0 est donc presque sûrement constant. □

8.2 Dynamique des transformations ergodiques

Voici une proposition qui permet de comprendre la force de la notion d'ergodicité. Cette proposition étaye l'intuition "je passe partout" sous-jacente au mot ergodique dans un contexte topologique.

Proposition 8.3 *Soit X un espace métrique localement compact séparable, μ une probabilité borélienne sur X et $f : X \to X$ un homéomorphisme qui préserve la classe μ. Si f est ergodique alors μ-presque toute orbite $O_x := \{f^n(x) \mid n \in \mathbb{Z}\}$ est dense dans* $\mathrm{supp}(\mu)$.

Démonstration On peut supposer que $X = \mathrm{supp}(\mu)$ Soient D une partie dénombrable dense de X et $\mathcal{D}$ l'ensemble des boules ouvertes centrées en D de rayon rationnel positif. Pour tout $B \in \mathcal{D}$, l'ensemble $A_B := \cup_{p\in\mathbb{Z}} f^{-p}(B)$ des points dont l'orbite passe dans B vérifie $f^{-1}(A_B) = A_B$. Par ergodicité de f, on a $\mu(A_B) = 1$. L'intersection $A = \cap_{B\in\mathcal{D}} A_B$ vérifie aussi $\mu(A) = 1$. Les orbites des points de A sont denses dans X. □

Remarque Toute transformation continue f d'un espace compact X préserve au moins une probabilité borélienne. Cela résulte du lemme 7.9.b. En outre, cette probabilité f-invariante peut-être choisie ergodique. Cela résulte du théorème de Krein-Milman car une probabilité G-invariante est ergodique ssi c'est un point extrémal du convexe fermé $\mathcal{P}(X)^G$ des probabilités G invariantes sur X.

Plus généralement, soit G un groupe localement compact séparable qui agit de façon mesurables sur un espace probabilisé $(X, \mathcal{B}, \mu)$ en préservant la classe de μ. Cette action est dite *ergodique* si les seules parties mesurables G-invariantes vérifient $\mu(A) = 0$ ou 1.

On a l'extension suivante de la proposition 8.3.

Proposition 8.4 *Soit X un espace métrique localement compact séparable, μ une probabilité borélienne sur X et G un groupe localement compact séparable qui agit continument sur X en préservant la classe de μ. On suppose l'action de G ergodique. Alors μ-presque toute orbite Gx est dense dans* $\mathrm{supp}(\mu)$.

Démonstration C'est la même que celle de la proposition 8.3.

Corollaire 8.5 *On garde les notations et hypothèses de la proposition 8.4. Soit $\mathcal{R}$ une relation d'équivalence sur X dont les classes d'équivalence sont localement fermées et G-invariantes. Alors il existe une classe d'équivalence Ω telle que $\mu(\Omega) = 1$.*

Démonstration Soit Ω une classe d'équivalence rencontrant une des orbites Gx dont l'adhérence est $\overline{Gx} = \mathrm{supp}(\mu)$. On a donc $\mathrm{supp}(\mu) \subset \overline{\Omega}$. Si $\mu(\Omega) = 0$, comme Ω est localement fermée, on aurait $\mathrm{supp}(\mu) \subset \overline{\Omega} \smallsetminus \Omega$, ce qui contredirait le fait que x est dans $\mathrm{supp}(\mu)$. Par ergodicité, on a donc $\mu(\Omega) = 1$. □

Remarque Ce corollaire est utile lorsque G est un sous-groupe d'un groupe $\mathbf{H}_{\mathbb{R}}$ où $\mathbf{H}$ est un $\mathbb{R}$-groupe agissant de façon algébrique sur une $\mathbb{R}$-variété $\mathbf{X}$: comme les $\mathbf{H}_{\mathbb{R}}$-orbites dans $\mathbf{X}_{\mathbb{R}}$ sont localement fermées, les mesures G-ergodiques sur $\mathbf{X}_{\mathbb{R}}$ sont alors portées par des $\mathbf{H}_{\mathbb{R}}$-orbites.

8.3 Théorème ergodique

Le théorème ergodique de Birkhoff exprime de façon précise une idée intuitive pour une transformation ergodique : pour toute partie mesurable A, la proportion de temps passé dans A par presque toutes les orbites est égale à la mesure de A.

Théorème 8.6 (Birkhoff) *Soit $(X, \mathcal{B}, \mu, f)$ un système dynamique probabilisé. Pour tout $\varphi \in L^1(X, \mu)$, on note $\varphi_n(x) = \sum_{0 \leq i < n} \varphi(f^i(x))$.*
a) La limite $\widetilde{\varphi}(x) := \lim_{n\to\infty} \frac{1}{n}\varphi_n(x)$ existe μ-presque partout.
b) On a $\widetilde{\varphi} \circ f = \widetilde{\varphi}$ μ-presque partout.
c) On a $\|\widetilde{\varphi}\|_{L^1} \leq \|\varphi\|_{L^1}$.
d) La convergence a lieu dans L^1, i.e. $\lim_{n\to\infty} \|\frac{1}{n}\varphi_n - \widetilde{\varphi}\|_{L^1} = 0$.
e) Pour toute partie f-invariante A de X, on a $\int_A \widetilde{\varphi}\, d\mu = \int_A \varphi\, d\mu$.
f) En particulier, si μ est ergodique, on a $\widetilde{\varphi}(x) = \int_X \varphi\, d\mu$ μ-presque partout.

Remarques - La somme $\varphi_n(x)$ s'appelle *somme orbitale* ou *somme de Birkhoff* de φ. L'intégrale $\int_X \varphi\, d\mu$ s'appelle la *moyenne spatiale* de φ. Le théorème de Birkhoff affirme donc, dans le cas ergodique, que les moyennes orbitales convergent presque partout vers la moyenne spatiale.

- L'assertion e) signifie que $\widetilde{\varphi}$ est *l'espérance conditionnelle* de φ relativement à la σ-algèbre $\mathcal{B}^f$ des parties f-invariantes : $\widetilde{\varphi} = E(\varphi|\mathcal{B}^f)$.

Lemme 8.7 (inégalité maximale) *Soient $\varphi_n \in L^1_{\mathbb{R}}(X, \mu)$ une suite sous-additive i.e. telle que, pour tout $m, n \geq 1$, on a $\varphi_{m+n} \leq \varphi_m \circ f^n + \varphi_n$. On note $\varphi = \varphi_1$ et $\varphi^* = \sup_{n\geq 1} \varphi_n$. Alors, on a $\int_{\{\varphi^* > 0\}} \varphi\, d\mu \geq 0$.*

Démonstration Soient $\psi_n = \max\{0, \varphi, \varphi_2, \ldots, \varphi_n\}$ et $E_n = \{x \in X \mid \psi_n(x) > 0\}$. Sur E_n, on a $\psi_n \leq \varphi + \psi_{n-1} \circ f$ tandis que sur le complémentaire E_n^c, on a $\psi_n = 0$ et $\psi_{n-1} \circ f \geq 0$. On a donc

$$\int_{E_n} \varphi \geq \int_{E_n} \psi_n - \int_{E_n} \psi_{n-1} \circ f \geq \int_X \psi_n - \int_X \psi_{n-1} \circ f \geq \int_X \psi_n - \psi_{n-1} \geq 0.$$

Or $\{\varphi^* > 0\} = \cup E_n$. On a donc $\int_{\{\varphi^* > 0\}} \varphi\, d\mu \geq 0$. □

Démonstration du théorème 8.6 a) Pour démontrer l'existence de la limite, il suffit de voir que, pour tous rationnels $\alpha < \beta$, l'ensemble

$$E_{\alpha,\beta} := \{x \in X \mid \liminf_{n\to\infty} \tfrac{1}{n}\varphi_n(x) < \alpha < \beta < \limsup_{n\to\infty} \tfrac{1}{n}\varphi_n(x)\}$$

est de mesure nulle. Remarquons que

$$\lim_{n\to\infty} \tfrac{1}{n}(\varphi_{n+1}(x) - \varphi_n(f(x))) = \lim_{n\to\infty} \tfrac{1}{n}\varphi(x) = 0$$

et donc que $f^{-1}(E_{\alpha,\beta}) = E_{\alpha,\beta}$. On peut donc appliquer l'inégalité maximale sur la partie $E_{\alpha,\beta}$ aux fonctions $\varphi - \beta$ et $\alpha - \varphi$. On obtient

$$\int_{E_{\alpha,\beta}} (\varphi - \beta) \geq 0 \ \text{ et } \ \int_{E_{\alpha,\beta}} (\alpha - \varphi) \geq 0.$$

On en déduit $\int_{E_{\alpha,\beta}} (\alpha - \beta) \geq 0$ et donc $\mu(E_{\alpha,\beta}) = 0$.

b) C'est clair car $\frac{1}{n}(\varphi_{n+1}(x) - \varphi_n(f(x)))$ converge vers 0.

c) On peut supposer que φ est positive. Cela résulte alors du lemme de Fatou :

$$\int_X \widetilde{\varphi} = \int_X \lim_{n\to\infty} \tfrac{1}{n}\varphi_n(x) \leq \lim_{n\to\infty} \tfrac{1}{n} \int_X \varphi_n(x) = \int_X \varphi.$$

d) Lorsque φ est bornée, cela résulte du théorème de convergence dominée. Le cas général s'en déduit par densité. En effet, pour tout $\varepsilon > 0$, on peut trouver ψ bornée telle que $\|\varphi - \psi\|_{L^1} \leq \varepsilon/3$. On a donc, pour tout $n \geq 1$, $\|\frac{1}{n}\varphi_n - \frac{1}{n}\psi_n\| \leq \varepsilon/3$ et, par c), $\|\widetilde{\varphi} - \widetilde{\psi}\|_{L^1} \leq \varepsilon/3$. Pour n grand, on a alors $\|\frac{1}{n}\psi_n - \widetilde{\psi}\| \leq \varepsilon/3$ et donc $\|\frac{1}{n}\varphi_n - \widetilde{\varphi}\| \leq \varepsilon$. C'est ce que l'on voulait.

e) Cela résulte de d) car $\int_A \varphi = \int_A \frac{1}{n}\varphi_n$.

f) Par b), la fonction $\widetilde{\varphi}$ est constante presque partout. □

La proposition suivante due à Egorov permet de remplacer dans le théorème de Birkhoff la convergence presque sure par une convergence uniforme en dehors d'un ensemble de mesure arbitrairement petite.

Proposition 8.8 *Soit $(X, \mathcal{B}, \mu)$ un espace probabilisé et f_n une suite de fonctions mesurables sur X qui converge μ-presque sûrement vers une fonction f.*

Alors pour tout $\varepsilon > 0$, il existe une partie mesurable $Z \subset X$ tel que $\mu(Z^c) \leq \varepsilon$ et la convergence $f_n(x) \to f(x)$ est uniforme pour $x \in Z$.

Démonstration Posons $Z_{m,n} := \{x \in X \mid |f_i(x) - f_j(x)| \leq \frac{1}{m} \text{ , pour } i, j \geq n\}$. Choisissons une suite n_m telle que $\mu(Z_{m,n_m}) \geq 1 - \varepsilon/2^p$ et posons $Z = \cup_{m\geq 1} Z_{m,n_m}$. Par construction, la convergence $f_n(x) \to f(x)$ est uniforme pour $x \in Z$ et on a $\mu(Z) \geq 1 - \varepsilon$. □

8.4 Martingales

Le théorème des martingales est avec le théorème de Birkhoff l'un des piliers de la théorie des probabilités.

Soit $(X, \mathcal{B}, \mu)$ un espace probabilisé et $\mathcal{B}_n$ une suite croissante de sous-σ-algèbres.

Définition 8.9 *Soit f_n une suite de fonctions intégrables et $\mathcal{B}_n$-mesurables.*
La suite f_n est une martingale si $f_n = E(f_{n+1}|\mathcal{B}_n)$.
La suite f_n est une sousmartingale si $f_n \leq E(f_{n+1}|\mathcal{B}_n)$.
La suite f_n est une surmartingale si $f_n \geq E(f_{n+1}|\mathcal{B}_n)$.

Pour $t \in \mathbb{R}$, on note $t^+ = \max(t, 0)$.

Remarques - Une martingale peut être vue comme un objet dont les f_n ne sont que des approximations. Un peu comme la donnée d'un réel par son développement décimal.

- Seules les martingales nous seront utiles par la suite. Nous n'utiliserons les sousmartingales et surmartingales. que pour démontrer le théorème de convergence des martingales. Elles sont utiles car si une suite f_n est une sousmartingale, les suites f_n^+ et $|f_n|$ sont encore des sousmartingales.

Exemple Soient $X = \{0,1\}^{\mathbb{N}^*}$ muni de la probabilité de Bernoulli $\mu = \alpha^{\otimes\mathbb{N}}$ avec $\alpha = \frac{1}{2}(\delta_0 + \delta_1)$, $p_n : X \to \{0,1\}^n$ l'application donnée par $p_n(x_1, x_2, \ldots) = (x_1, \ldots, x_n)$ et $\mathcal{B}_n$ la σ-algèbre formée des parties $p_n^{-1}(E)$ pour $E \subset \{0,1\}^n$. Dans ce cas la donnée d'une martingale f_n équivaut à la donnée d'une mesure bornée ν sur X. Le lien entre les deux est donné par $f_n(x) = 2^{-n}\nu(F_n(x))$, pour $x \in X$, où $F_n(x)$ est la fibre de p_n contenant x. Le fait que ces deux données soient équivalentes est dû au théorème de Carathéodory.

Comme dans l'exemple ci-dessus, dans la plupart des applications, l'espace X est muni d'une famille de surjections mesurables $p_n : (X, \mathcal{B}) \to (Y_n, \mathcal{C}_n)$ telles que $\mathcal{B}_n = p_n^{-1}(\mathcal{C}_n)$. Ces surjections sont de plus en plus fines de sorte que la suite $\mathcal{B}_n$ est croissante. La martingale est donc un objet sur X dont les fonctions f_n ne sont que ses "moyennes sur les fibres de p_n" .

Voici le théorème de convergence ps des martingales

Théorème 8.10 (Doob) *Soit f_n une sous-martingale sur $(X, \mathcal{B}, \mu)$ telle que $\sup_{n\geq 0} \|f_n\|_{L^1} < \infty$. Alors la limite $f_\infty(x) = \lim_{n\to\infty} f_n(x)$ existe μ-presque sûrement..*

Nous dirons que f_n est L^1-bornée si $\sup_{n\geq 0} \|f_n\|_{L^1} < \infty$.

Exemple Reprenons l'exemple ci-dessus et écrivons grâce au théorème de décomposition des mesures $\nu = f\mu + \nu_s$ avec ν_s étrangère à μ. On a alors l'égalité $f_\infty = f$. La limite presque sûre ne donne donc aucun renseignement sur la partie singulière ν_s.

Remarque En général la limite presque sûre f_∞ d'une martingale ne permet pas de reconstituer la martingale. C'est le cas si et seulement si la convergence de f_n vers f_∞ est une convergence L^1. On a alors $f_n = E(f_\infty|\mathcal{B}_n)$. Une condition

suffisante qui l'assure est $\sup_{n\geq 0} \|f_n\|_{L\log L} < \infty$ où cette norme est la norme L^1 de la fonction $|f_n| \log^+ |f_n|$.

Démonstration du théorème de Doob Elle résulte des trois lemmes 8.11, 8.12 et 8.13 suivants. □

Le premier lemme est la décomposition de Kricheberg.

Lemme 8.11 *Toute sousmartingale L^1-bornée f_n s'écrit $f_n = m_n - s_n$ où m_n est une martingale positive L^1-bornée et s_n une surmartingale positive L^1-bornée.*

Démonstration La suite f_n^+ est une sousmartingale positive et on a, pour $k \geq n$

$$E(f_k^+|\mathcal{B}_n) \leq E(f_{k+1}^+|\mathcal{B}_n).$$

Notons $m_n = \lim_{k\to\infty} E(f_k^+|\mathcal{B}_n)$. C'est une martingale positive telle que $E(m_n) \leq \sup_{n\geq 0} E(f_n^+) < \infty$ car l'espérance conditionnelle commute à la limite croissante. Donc m_n est L^1-bornée et $s_n = m_n - f_n$ est une surmartingale L^1-bornée. □

Le deuxième lemme affirme qu'une surmartingale est un jeu défavorable quelle que soit la stratégie : plus on arrête tard la surmartingale plus l'espérance de gain est faible.

On appelle temps d'arrêt une application $\mathcal{B}$-mesurable $\sigma : X \to \mathbb{N} \cup \{\infty\}$ telle que, pour tout $n \geq 0$, l'ensemble $\sigma^{-1}(n)$ est $\mathcal{B}_n$-mesurable.

On note alors $s_\tau : \omega \to s_{\tau(\omega)}(\omega)$ avec la convention $s_\infty = 0$.

Lemme 8.12 *Soit s_n une surmartingale positive et σ, τ deux temps d'arrêt avec $\sigma \leq \tau$. Alors $\int_X s_\sigma \, d\mu \geq \int_X s_\tau \, d\mu$.*

Démonstration Pour $m \leq n$, on a

$$\int_{\{\sigma=m\,,\,\tau>n\}} s_n \geq \int_{\{\sigma=m\,,\,\tau>n\}} s_{n+1}$$

car τ et σ sont des temps d'arrêt et s_n est une surmartingale. On en déduit, en notant $\tau \wedge n := \inf(\tau, n)$,

$$\int_{\{\sigma=m\}} s_{\tau\wedge n} \geq \int_{\{\sigma=m\}} s_{\tau\wedge(n+1)}$$

et donc en mettant bout à bout ces inégalités pour $n \geq m$, en se souvenant que $\tau \geq \sigma$, et en utilisant Fatou

$$\int_{\{\sigma=m\}} s_m \geq \cdots \geq \int_{\{\sigma=m\}} s_{\tau\wedge n} \geq \cdots \geq \int_{\{\sigma=m\}} s_\tau$$

d'où, en sommant sur m, $\int_X s_\sigma \geq \int_X s_\tau$. □

Lemme 8.13 *Toute surmartingale positive s_n converge μ-presque sûrement.*

Démonstration Pour démontrer l'existence de la limite de s_n, il suffit de voir que, pour tous rationnels $\alpha < \beta$, l'ensemble

$$E_{\alpha,\beta} := \{x \in X \mid \liminf_{n\to\infty} s_n(\omega) < \alpha < \beta < \limsup_{n\to\infty} s_n(\omega)\}$$

est de mesure nulle pour μ-presque tout ω. Pour cela, on introduit par récurrence des temps d'arrêt τ_i par $\tau_0 = 0$ et, pour $i \geq 1$,

$$\begin{aligned} \tau_{2i+1} &= \inf\{n > \tau_{2i} \mid s_n > \beta\} \\ \tau_{2i} &= \inf\{n > \tau_{2i-1} \mid s_n < \alpha\}. \end{aligned}$$

On a alors, en notant $p_i := \mu(\{\tau_i < \infty\})$, et en utilisant le lemme 8.12

$$\beta\, p_{2i+1} \leq \int_X s_{\tau_{2i+1}} \leq \int_X s_{\tau_{2i}} \leq \alpha p_{2i} \leq \alpha p_{2i-1}.$$

Donc $\mu(E_{\alpha,\beta}) \leq p_{2i+1} \leq (\frac{\alpha}{\beta})^i p_1$ pour tout $i \geq 1$ et $\mu(E_{\alpha,\beta}) = 0$. □

9 Mesures stationnaires

Les mesures stationnaires sont des mesures qui décrivent le comportement asymptotique des marches aléatoires.

Nous montrons dans ce chapitre comment les utiliser pour montrer des théorèmes d'existence et d'unicité pour des "applications mesurables équivariantes entre les bords".

9.1 Existence d'une mesure limite

Soit G un groupe localement compact séparable, μ une probabilité borélienne sur G et X un espace localement compact métrisable muni d'une action continue de G. On note $\mathcal{P}(X)$ l'espace des probabilités boréliennes sur X.

Pour toute probabilité (borélienne) ν sur X, on note $\mu * \nu$ la convolée

$$\mu * \nu := \int_G g_* \nu \, d\mu(g).$$

On note μ^{*n} la probabilité $\mu * \ldots * \mu$ convolée de n probabilités toutes égales à μ.

Définition 9.1 *Une probabilité borélienne ν sur X est dite μ-harmonique ou μ-stationnaire si on a $\mu * \nu = \nu$.*

Remarque Le terme *harmonique* vient de ce que ν coincide avec la moyenne de ses translatées. Le terme *stationnaire* exprime le fait que ν est une loi asymptotique possible pour une "marche aléatoire sur X dont les lois de transitions sont indépendantes et données par μ".

Lemme 9.2 *Lorsque X est compact, il existe toujours des mesures stationnaires.*

Démonstration Comme X est compact, l'espace $\mathcal{P}(X)$ est un convexe compact dans le Fréchet $\mathcal{M}(X)$ des mesures bornées muni de la topologie faible. L'argument de Kakutani prouve l'existence d'un point fixe par l'opérateur de convolution par μ : on part de n'importe quelle probabilité $\nu_0 \in \mathcal{P}(X)$ et on prend pour ν une valeur d'adhérence de la suite $\nu_n := \frac{1}{n}(\nu_0 + \mu * \nu_0 + \cdots + \mu^{*n} * \nu_0) \in \mathcal{P}(X)$. Comme $\nu_n - \mu * \nu_n$ tend vers 0, la probabilité ν est μ-stationnaire. □

On note Ω l'espace produit $\Omega = G^{\mathbb{N}}$, $\mathcal{B}$ sa tribu borélienne et $\overline{\mu}$ la probabilité produit sur $(X, \mathcal{B})$. C'est l'unique probabilité dont l'image dans chaque G^n est la probabilité produit $\mu^{\otimes n}$. Par le théorème de Carathéodory, cette probabilité $\overline{\mu}$ existe et est unique. On note $g_i : \Omega \to G; \omega \to g_i(\omega)$ les fonctions coordonnées.

Lemme 9.3 *a) La limite*

$$\nu_\omega := \lim_{n \to \infty} g_0(\omega)_* \cdots g_n(\omega)_* \nu \in \mathcal{P}(X)$$

existe pour $\overline{\mu}$-presque tout ω.
b) Pour tout $k \geq 1$, on a l'égalité, pour μ^{*k}-presque tout g et $\overline{\mu}$-presque tout ω,

$$\lim_{n\to\infty} g_0(\omega)_* \cdots g_n(\omega)_* g_*\nu = \nu_\omega.$$

c) On a l'égalité $\nu = \int_\Omega \nu_\omega \, d\overline{\mu}(\omega)$.

Démonstration Nous ne donnerons la preuve que pour X compact.

a) Notons $\mathcal{B}_n = \langle g_0, \ldots, g_n \rangle$ la σ-algèbre engendrée par les fonctions $g_0, \ldots, g_n$. Pour $\varphi \in C(X)$, on note $\Phi \in C(G)$ la fonction

$$g \mapsto \Phi(g) = (g_*\nu)(\varphi) = \int_X \varphi(gx) d\nu(x).$$

Le fait que ν soit μ-stationaire se traduit par l'égalité, pour tout $g \in G$,

$$\Phi(g) = \int_G \Phi(gh) d\mu(h).$$

La suite de fonction $f_n \in L^\infty(\Omega)$

$$f_n : \omega \mapsto \Phi(g_0(\omega) \cdots g_n(\omega))$$

est une martingale pour $\mathcal{B}_n$. En effet, on a l'égalité, pour tout $n \geq 1$,

$$\begin{aligned} E(f_{n+1}|\mathcal{B}_n)(\omega) &= \int_G \Phi(g_0(\omega) \cdots g_n(\omega) g) d\mu(g) \\ &= \Phi(g_0(\omega) \cdots g_n(\omega)) = f_n(\omega). \end{aligned}$$

Comme cette martingale est bornée par $\|\varphi\|_\infty$, le théorème 8.10 de Doob prouve qu'elle converge $\overline{\mu}$-ps. En utilisant une famille dénombrable dense de fonctions $\varphi \in C(X)$, la limite $\nu_\omega = \lim_{n\to\infty} g_0(\omega)_* \cdots g_n(\omega)_* \nu$ existe pour $\overline{\mu}$-presque tout ω.

b) En plus des fonctions Φ et f_n ci-dessus, introduisons les fonctions $f_n^g \in L^\infty(\Omega)$ pour $g \in G$ données par

$$f_n^g : \omega \mapsto \Phi(g_0(\omega) \cdots g_n(\omega) g)$$

et calculons les intégrales

$$\begin{aligned} I_n &= \int_\Omega \int_G |f_n(\omega) - f_n^g(\omega)|^2 \, d\mu^{*k}(g) \, d\overline{\mu}(\omega) \\ &= \int_G \int_G |\Phi(h) - \Phi(hg)|^2 \, d\mu^{*k}(g) \, d\mu^{*(n+1)}(h) \\ &= \int_\Omega |f_n(\omega) - f_{n+k}(\omega)|^2 \, d\overline{\mu}(\omega) \\ &= \|f_{n+k}\|_{L^2}^2 - \|f_n\|_{L^2}^2. \end{aligned}$$

Dans ce calcul, on a utilisé le fait que f_n est une martingale à travers l'égalité

$$\int_\Omega \overline{f}_n f_{n+k}\, d\overline{\mu} = \int_\Omega |f_n|^2\, d\overline{\mu}.$$

On déduit de ce calcul que

$$\sum_0^\infty I_n \leq k\|\varphi\|_\infty^2.$$

On en déduit que la fonction suivante est intégrable

$$\sum_0^\infty |f_n(\omega) - f_n^g(\omega)|^2 \in L^1(\Omega \times G, \overline{\mu} \otimes \mu^{*k}).$$

En particulier, pour μ^{*k}-presque tout g et $\overline{\mu}$-presque tout ω, la suite $f_n(\omega) - f_n^g(\omega)$ converge vers 0.

c) Par le théorème de convergence dominée et le point a), on a

$$\begin{aligned}\int_\Omega \lim_{n\to\infty} g_0(\omega)_* \cdots g_n(\omega)_*\nu\, d\overline{\mu}(\omega) &= \lim_{n\to\infty} \int_\Omega g_0(\omega)_* \cdots g_n(\omega)_*\nu\, d\overline{\mu}(\omega) \\ &= \lim_{n\to\infty} \mu^{*n} * \nu \;=\; \nu\end{aligned}$$

D'où $\int_\Omega \nu_\omega\, d\overline{\mu}(\omega) = \nu$. □

9.2 Contraction et proximalité

Dans cette section, on montre qu'une marche aléatoire linéaire contracte presque sûrement autant que son support peut le permettre.

Soit $k = \mathbb{R}$, $\mathbb{C}$ ou une extension finie de $\mathbb{Q}_p$. Dans cette partie μ est une probabilité sur le groupe $G = \mathrm{GL}(d, k)$. Ce groupe G agit sur $V = k^d$ ainsi que sur l'espace projectif $X = \mathbb{P}(V)$.

On note Γ_μ le plus petit sousgroupe fermé de G qui contient le support de μ.

Définition 9.4 *On dit qu'un sous-groupe $\Gamma \subset G$ est fortement irréductible (sur V) si Γ ne laisse invariant aucune union finie de sous-espaces propres de V.*

Il est équivalent de dire que la composante connexe de l'adhérence de Zariski de Γ agit de façon irréductible sur V.

On note $p = p_\Gamma$ le plus petit entier non nul pour lequel il existe une matrice $\pi \in \mathcal{M}(d, k)$ de rang p telle que $\pi = \lim_{n\to\infty} \lambda_n\gamma_n$ avec $\lambda_n \in k$ et $\gamma_n \in \Gamma$.

Définition 9.5 *On dit que Γ est proximal si $p_\Gamma = 1$.*

La proposition suivante donne les premières propriétés des marches aléatoires linéaires.

Proposition 9.6 *Soit μ une probabilité borélienne sur $G = \mathrm{GL}(d,k)$ telle que Γ_μ est fortement irréductible. On note $p = p_{\Gamma_\mu}$.*
a) Il existe une application mesurable $J : \Omega \to \mathrm{Gr}_p(V); \omega \mapsto J_\omega$ de $\Omega = G^{\mathbb{N}}$ dans la Grassmannienne des p-plans de V telle que, pour $\overline{\mu}$-presque tout $\omega \in \Omega$, toute valeur d'adhérence non nulle M d'une suite $\lambda_n\, g_0(\omega) \cdots g_n(\omega)$, avec $\lambda_n \in k$, a pour image $\mathrm{Im}(M) = J_\omega$.
b) Pour tout hyperplan $W \subset V$, on a $\overline{\mu}(\{\omega \in \Omega \mid J_\omega \subset W\}) = 0$.

La démonstration repose sur l'étude des probabilités μ-stationnaires sur $\mathbb{P}(V)$. On sait par le lemme 9.2 qu'il en existe toujours.

Lemme 9.7 *Soit μ une probabilité borélienne sur $G = \mathrm{GL}(d,k)$ telle que Γ_μ est fortement irréductible. Soit ν une probabilité μ-stationnaire sur $\mathbb{P}(V)$.*
Pour tout hyperplan $W \subset V$, on a $\nu(\mathbb{P}(W)) = 0$.

Démonstration du lemme 9.7 Soit r la plus petite dimension d'un espace $W \subset V$ tel que $\nu(\mathbb{P}(W)) \neq 0$. On a, pour tous sous-espaces $W_1 \neq W_2$ de dimension r,

$$\nu(\mathbb{P}(W_1) \cup \mathbb{P}(W_2)) = \nu(\mathbb{P}(W_1)) + \nu(\mathbb{P}(W_2)).$$

De sorte que, pour tout $\alpha > 0$, il n'existe qu'un nombre fini de sous-espaces W de dimension r tels que $\nu(\mathbb{P}(W)) \geq \alpha$. Notons

$$\alpha_0 = \max\{\nu(\mathbb{P}(W)) \mid \dim W = r\},$$

$$F = \{W \mid \dim W = r \text{ et } \nu(\mathbb{P}(W)) = \alpha_0\}.$$

Cet ensemble F est fini. Comme ν est μ-stationnaire, on a l'égalité

$$\nu(\mathbb{P}(W)) = \int_G \nu(\mathbb{P}(gW))\, d\mu(g).$$

On en déduit que F est Γ_μ-invariant. Ceci contredit la forte irréductibilité de Γ_μ.

Démonstration de la proposition 9.6 Par définition, la valeur d'adhérence M est de rang $\geq p$.

Soit ν une probabilité μ-stationnaire sur $\mathbb{P}(V)$. Notons J_ω le plus petit sous-espace vectoriel de V tel que $\mathbb{P}(J_\omega)$ contient le support de ν_ω. Par le lemme 9.7, on a $\nu(\mathbb{P}(\mathrm{Ker}M)) = 0$. La probabilité $M_*\nu$ a donc un sens et on a, par le lemme 9.3.a, l'égalité

$$M_*\nu = \nu_\omega.$$

En conséquence, par le même lemme 9.7, l'image $\mathrm{Im}M$ est le plus petit sous-espace W tel que $\mathbb{P}(W)$ contient le support de ν_ω. On a donc $\mathrm{Im}M = J_\omega$.

Ceci prouve simultanément que l'image $\mathrm{Im}M$ ne dépend pas du choix de la valeur d'adhérence M, que J_ω ne dépend pas du choix de la probabilité stationnaire ν et que $\dim J_\omega \geq p$.

Il reste à montrer que $\dim J_\omega = p$. Le même raisonnement avec le lemme 9.3.b prouve que, pour μ^{*k}-presque tout g, on a

$$M_* g_* \nu = \nu_\omega.$$

Par continuité, cette égalité est encore vraie, pour tout $g \in \Gamma_\mu$. Choisissons une limite non nulle π de rang p d'une suite $\lambda_n g_n$ avec $\lambda_n \in k$ et $g_n \in \Gamma_\mu$. On peut supposer, par irréductibilité de Γ_μ que $\mathrm{Im}\pi \not\subset \mathrm{Ker}M$. On a encore

$$M_* \pi_* \nu = \nu_\omega.$$

Donc $\mathrm{Im}(M \circ \pi) = J_\omega$ et $\dim J_\omega \leq p$. On a bien $\dim J_\omega = p$.

9.3 Proximalité

Dans cette section, on montre que dans une situation proximale, la probabilité stationnaire ν est unique.

On en déduit des résultats d'existence et d'unicité d'applications mesurables équivariantes entre les bords qui joueront un rôle central dans la démonstration du théorème de superrigidité.

Proposition 9.8 *Soit μ une probabilité borélienne sur $G = \mathrm{GL}(d,k)$ telle que Γ_μ est proximal et fortement irréductible.*
a) Il existe une unique probabilité μ-stationnaire $\nu \in \mathcal{P}(\mathbb{P}(V))$.
b) Il existe une unique probabilité μ-stationnaire $\sigma \in \mathcal{P}(\mathcal{P}(\mathbb{P}(V)))$. Son support est inclus dans l'ensemble $\delta_{\mathbb{P}(V)}$ des masses de Dirac sur $\mathbb{P}(V)$.

Démonstration L'existence de ν et de σ résulte du lemme 9.2.

a) On note $j : \Omega \to \mathbb{P}(k^d); \omega \mapsto j_\omega$ l'application donnée par la proposition 9.6 de sorte que $\nu_\omega = \delta_{j_\omega}$. D'après le lemme 9.3, la probabilité ν est donc donnée par $\nu = \int_\Omega \delta_{j_\omega}\, d\overline{\mu}(\omega)$.

b) Notons ν_σ le centre de gravité de σ,

$$\nu_\sigma = \int_{\mathcal{P}(\mathbb{P}(V))} \lambda \, d\sigma(\lambda) \in \mathcal{P}(\mathbb{P}(V)).$$

Cette probabilité ν_σ est aussi μ-stationnaire. Par le lemme 9.3, pour $\overline{\mu}$-presque tout ω, on a

$$\lim_{n\to\infty} g_0(\omega)_* \cdots g_n(\omega)_* \nu_\sigma = \delta_{j_\omega}$$

On en déduit que, pour $\overline{\mu}$-presque tout ω, pour tout $\varepsilon > 0$, pour toute fonction $\varphi \in C(\mathbb{P}(V))$,

$$\lim_{n\to\infty} \sigma(\{\lambda \mid (g_0(\omega)_* \cdots g_n(\omega)_* \lambda)(\varphi) - \varphi(j_\omega) \geq \varepsilon\}) = 0$$

et donc, en notant d une distance compatible sur l'espace métrisable compact $\mathcal{P}(\mathbb{P}(V))$,

$$\lim_{n\to\infty} \sigma(\{\lambda \mid d(g_0(\omega)_* \cdots g_n(\omega)_*\lambda, \delta_{\mathbb{P}(V)}) \geq \varepsilon\}) = 0.$$

Par le théorème de convergence dominée, on a donc

$$\lim_{n\to\infty} \sigma \otimes \overline{\mu}(\{(\lambda,\omega) \mid d(g_0(\omega)_* \cdots g_n(\omega)_*\lambda, \delta_{\mathbb{P}(V)}) \geq \varepsilon\}) = 0.$$

Comme σ est μ-stationnaire, cette suite est constante égale à

$$\sigma(\{\lambda \mid d(\lambda, \delta_{\mathbb{P}(V)}) \geq \varepsilon\}) = 0.$$

Donc σ est portée par le fermé $\delta_{\mathbb{P}(V)} \subset \mathcal{P}(\mathbb{P}(V))$ des masses de Dirac sur $\mathbb{P}(V)$. Elle peut donc être vue comme une probabilité sur $\mathbb{P}(V)$. Cette probabilité est μ-stationnaire, elle est donc égale à ν. □

Proposition 9.9 *Soient Γ un groupe localement compact métrisable séparable, $\mu \in \mathcal{P}(\Gamma)$ une probabilité telle que $\Gamma_\mu = \Gamma$. Soient X_0 un espace compact métrisable sur lequel Γ agit continument et $\nu_0 \in \mathcal{P}(X_0)$ une probabilité μ-stationnaire.*

On se donne aussi une représentation proximale et fortement irréductible de Γ dans un espace vectoriel V.
a) Toute application mesurable Γ-équivariante $\varphi : X_0 \to \mathcal{P}(\mathbb{P}(V))$ prend ν_0-presque sûrement ses valeurs dans l'ensemble $\delta_{\mathbb{P}(V)}$ des masses de Dirac.
b) Il existe au plus une application ν_0-mesurable Γ-équivariante $\Phi : X_0 \to \mathbb{P}(V)$.

Le point a) permettra, dans la section 10.3, de construire des applications ν_0-mesurable Γ-équivariante $\varphi : X_0 \to \mathbb{P}(V)$.

Démonstration a) La probabilité $\sigma = \varphi_*(\nu_0) \in \mathcal{P}(\mathcal{P}(\mathbb{P}(V)))$ est μ-stationnaire. D'après la proposition 9.8, elle est portée par des masses de Dirac.

b) Soient $\Phi_1, \Phi_2 : X_0 \to \mathbb{P}(V)$ deux applications ν_0-mesurables Γ-équivariantes. D'après le point *a*), l'application $\varphi : X_0 \to \mathcal{P}(\mathcal{P}(\mathbb{P}(V)))$; $\xi \mapsto \frac{1}{2}(\delta_{\Phi_1(\xi)} + \delta_{\Phi_2(\xi)})$ prend ses valeurs dans l'espace des masses de Dirac. Donc, pour ν_0-presque tout $\xi \in X_0$, on a $\Phi_1(\xi) = \Phi_2(\xi)$. □

9.4 Mesures stationnaires K-invariantes

> Pour tout réseau Γ d'un groupe de Lie semisimple réel G, on construit une probabilité μ de support Γ dont l'unique mesure stationnaire ν_0 sur G/P est K-invariante. On pourra alors appliquer dans la section 10.3 la proposition 9.9 à cette probabilité K-invariante.

Soient $k = \mathbb{R}$, $\mathbf{G}$ un k-groupe semisimple et $G = \mathbf{G}_k$. Soient P un sous-groupe parabolique de G et K un sous-groupe compact de G tel que $G = KP$ (voir théorème 3.14) et ν_0 la probabilité K-invariante sur la variété drapeau $X_0 = G/P$.

Proposition 9.10 *Pour tout réseau $\Gamma \subset G$, il existe une probabilité $\mu \in \mathcal{P}(\Gamma)$ de support Γ et telle que $\mu * \nu_0 = \nu_0$.*

Remarques - Comme l'action de K sur G/P est transitive, il y a une unique probabilité K-invariante ν_0 sur G/P. En particulier, pour toute mesure K-invariante $\mu_0 \in \mathcal{P}(G)$, on a l'égalité $\mu_0 * \nu_0 = \nu_0$.

- Autrement dit, en dépit du caractère discret de Γ, les trajectoires sur G/P de la marche aléatoire indépendante sur Γ de loi μ s'équirépartissent sur le bord G/P selon la probabilité K-invariante ν_0.

Démonstration de la proposition 9.10 Soit μ_0 une probabilité K-invariante sur G à support compact et ayant une densité non nulle par rapport à la mesure de Haar sur un ouvert U de G dont les puisances U^n recouvrent G.

Posons

$$\tau(g) = \inf\{t \in [0,1] \mid g_*\nu_0 = (1-t)\mu' * \nu_0 + t\mu'' * \nu_0 \ , \ \mu', \mu'' \in \mathcal{P}(G) \ , \ \mathrm{supp}\mu' = \Gamma\}.$$

On espère bien sûr que cette fonction est constante égale à 0.

a) Montrons tout d'abord que, pour tout $g \in G$, on a $\tau(g) < 1$. Remarquons que pour tout $\gamma \in \Gamma$, on peut trouver $n_\gamma \geq 1$ et $\varepsilon_\gamma > 0$ tels que

$$g_*\mu_0^{*n_\gamma} > \varepsilon_\gamma \gamma_* \mu_0.$$

Donc

$$g_*\nu_0 = \varepsilon_\gamma \gamma_* \nu_0 + \mu''_\gamma * \nu_0$$

avec $\mu''_\gamma = g_*\mu_0^{*n_\gamma} - \varepsilon\gamma_*\mu_0$. On choisit alors une famille $a_\gamma > 0$ telle que $\sum_{\gamma\in\Gamma} a_\gamma = 1$. Une somme de ces égalités pondérées par a_γ donne

$$\tau(g) \leq 1 - \sum_{\gamma\in\Gamma} a_\gamma \varepsilon_\gamma < 1.$$

b) Montrons maintenant que $\tau(g)$ est une fonction constante. Cela va résulter de l'ergodicité de l'opérateur de convolution par μ_0 dans $L^2(X, \lambda_X)$ où $X = \Gamma\backslash G$ et λ_X est la probabilité G-invariante sur X. Plus précisément, remarquons que d'une part, pour tout $\gamma \in \Gamma$, on a $\tau(\gamma g) = \tau(g)$, et, d'autre part, comme ν_0 est μ_0-harmonique $\tau(g) \leq \int_G \tau(gh)\, d\mu_0(h)$. On note encore $\tau : X \to [0,1]$ la fonction induite sur X. Elle vérifie donc

$$\tau(x) \leq \int_G \tau(xh)\, d\mu_0(h).$$

C'est une fonction μ_0-sous-harmonique bornée. Elle est donc constante. En effet, dans le calcul suivant basé sur l'inégalité de Cauchy-Schwartz et sur Fubini

$$\int_X \tau(x)^2 d\lambda_X(x) \leq \int_X \int_G \tau(xh)^2\, d\lambda_X(x)\, d\mu_0(h) \leq \int_X \tau(x)^2\, d\lambda_X(x),$$

on doit avoir égalité dans ces inégalités et donc la fonction $h \to \tau(xh)$ est μ_0-presque sûrement constante. Donc τ est constante.

c) Il résulte de ces arguments qu'il existe $\ell < 1$ tel que $\tau(g) < \ell$, pour tout $g \in G$. En particulier, on peut écrire, pour tout $\mu_1 \in \mathcal{P}(G)$,

$$\begin{aligned} \mu_1 * \nu_0 &= (1-\ell)\mu_1' * \nu_0 + \ell\mu_2 * \nu_0 \\ &= (1-\ell)\mu_1' * \nu_0 + (1-\ell)\ell\mu_2' * \nu_0 + \ell^2\mu_3 * \nu_0 \\ &= (1-\ell)\mu_1' * \nu_0 + (1-\ell)\ell\mu_2' * \nu_0 + (1-\ell)\ell^2\mu_3' * \nu_0 + \cdots \end{aligned}$$

avec $\mu_i \in \mathcal{P}(G)$ et $\mu_i' \in \mathcal{P}(\Gamma)$. Si on part de $\mu_1 = \delta_e$, on obtient donc l'égalité $\nu_0 = \mu * \nu_0$ avec $\mu = (1-\ell)\sum_{i\geq 1} \ell^{i-1}\mu_i' \in \mathcal{P}(\Gamma)$. □

10 Superrigidité

Le but de ce chapitre est de montrer le théorème de superrigidité de Margulis.

10.1 Superrigidité

Le théorème de superrigidité permet de décrire toutes les représentations des réseaux d'un groupe de Lie semisimple réel G.

Pour pouvoir utiliser ce théorème de superrigidité pour montrer le théorème d'arithméticité, on doit considérer non seulement des représentations dans des espaces vectoriels réels mais aussi dans des espaces vectoriels p-adiques.

Nous verrons en outre que ces théorèmes s'étendent à des groupes G produit de groupes semisimples réels et p-adiques.

Théorème 10.1 (Margulis) *Soient $\ell = \mathbb{R}$, $G = \mathbf{G}_\ell$ le groupe des ℓ-points d'un ℓ-groupe semisimple $\mathbf{G}$ connexe. On suppose G sans facteur compact et $\mathrm{rang}_\ell(G) \geq 2$. Soit Γ un réseau irréductible de G.*

Soit $k = \mathbb{R}$, $\mathbb{C}$ ou une extension finie de $\mathbb{Q}_p$, $H = \mathbf{H}_k$ le groupe des k-points d'un k-groupe simple $\mathbf{H}$. Soit $\pi : \Gamma \to H$ un morphisme dont l'image $\pi(\Gamma)$ est Zariski dense et non bornée.

Alors π s'étend en un morphisme continu de G dans H.

Remarque Lorsque k est un corps p-adique, il n'existe pas de morphisme continu non constant de G dans H. La conclusion du théorème dans ce cas est donc qu'un tel morphisme $\pi : \Gamma \to H$ ne peut pas exister.

La démonstration occupe l'ensemble de ce chapitre.

Commençons par quelques commentaires sur les hypothèses de ce théorème.

L'hypothèse *G sans facteur compact* n'est pas très contraignante, on s'y ramène en remplaçant Γ par un sous-groupe fini sans torsion puis en considérant le réseau image de Γ dans le quotient de G par son sous-groupe distingué compact maximal. De même, l'hypothèse *$\pi(\Gamma)$ Zariski dense* n'est pas très restrictive. On peut souvent s'y ramener.

Exemple A Vérifions que l'hypothèse *$\pi(\Gamma)$ non bornée* est indispensable.

Notons q la forme quadratique sur $\mathbb{R}^5$, $q(x) = x_1^2 + x_2^2 + x_3^2 - \sqrt{2}x_4^2 - \sqrt{2}x_5^2$. Le groupe $\Gamma = \mathrm{SL}(5, \mathbb{Z}[\sqrt{2}]) \cap \mathrm{SO}(q, \mathbb{R})$ est un réseau de $\mathrm{SO}(q, \mathbb{R})$.

En effet, notons σ l'automorphisme non trivial du corps $\mathbb{Q}[\sqrt{2}]$ et q^σ l'image de q par σ. Le groupe $\{(g, g^\sigma) \mid g \in \mathrm{SL}(5, \mathbb{Z}[\sqrt{2}]) \cap \mathrm{SO}(q, \mathbb{R})\}$, est un sous-groupe arithmétique du $\mathbb{Q}$-groupe dont les points réels sont le produit $\mathrm{SO}(q, \mathbb{R}) \times \mathrm{SO}(q^\sigma, \mathbb{R})$. Comme le groupe $\mathrm{SO}(q^\sigma, \mathbb{R})$ est compact, Γ est bien un réseau.

Remarquons que le morphisme $\pi : \Gamma \to \mathrm{SO}(q^\sigma, \mathbb{R})$ donné par $\pi(g) = g^\sigma$ ne se prolonge pas à G. Dans ce cas, le groupe image est borné.

Exemple B Voici un deuxième exemple avec image p-adique qui met en valeur l'hypothèse $\pi(\Gamma)$ *non bornée*.

Le réseau $\Gamma = \mathrm{SL}(d, \mathbb{Z})$ du groupe $G = \mathrm{SL}(d, \mathbb{R})$ s'injecte dans le groupe p-adique $H = \mathrm{SL}(d, \mathbb{Q}_p)$. Cette injection ne se prolonge pas en un morphisme de G dans H. Dans ce cas aussi, le groupe image est borné.

Exemple C L'hypothèse de rang sur G est aussi importante : il n'existe pas de tels phénomènes de superrigidité pour les groupes $G = \mathrm{SO}(n, 1)$ qui sont de rang réel 1. Par exemple, pour $n = 2$, G contient des réseaux Γ qui sont des groupes libres non abéliens ou des π_1 de surface compacte. Il existe alors de nombreux morphismes $\pi : \Gamma \to G$ qui sont d'image dense, ceux-ci ne se prolongent pas en des morphismes de G dans G.

Exemple D L'hypothèse d'irréductibilité est aussi importante : le produit de deux réseaux $\Gamma_1 \times \Gamma_2 \subset G \times G$ avec $G = \mathrm{SO}(2, 1)$ fournit aisément des contre-exemples.

Exemple E L'hypothèse de simplicité sur $\mathbf{H}$ est aussi utile même si on s'y ramène facilement en composant π par la projection sur les facteurs simples de $\mathbf{H}$.

Par exemple, si Γ est le réseau du groupe $G = \mathrm{SL}(d, \mathbb{R})$ donné par $\Gamma = \{g \in \mathrm{SL}(d, \mathbb{Z}) \mid g \equiv Id \bmod 2\}$. Comme le groupe dérivé $[\Gamma, \Gamma]$ est formé de matrices congrues à l'identité modulo 4, il existe des morphismes non triviaux $\varepsilon : \Gamma \to \{\pm 1\}$. Mais alors le morphisme $\pi : \Gamma \to H = \mathrm{SL}(d, \mathbb{R})$, donné par $\pi(\gamma) = \varepsilon(\gamma)\gamma$, ne se prolonge pas en un morphisme de G dans H.

De même, si Γ est l'image dans $G = \mathrm{PGL}(d, \mathbb{R})$ du groupe $\Gamma_0 = \{g \in \mathrm{SL}(d, \mathbb{Z}) \mid g \equiv Id \bmod 3\}$. Le relèvement $\pi : \Gamma \to \Gamma_0 \subset H = \mathrm{SL}(d, \mathbb{R})$ ne se prolonge pas en un morphisme de G dans H.

Exemple F Lorsque $\mathbf{G}$ est simplement connexe et $k = \mathbb{R}$, le morphisme π s'étend alors en une $\mathbb{R}$-représentation de $\mathbf{G}$ dans $\mathbf{H}$.

L'hypothèse de simple connexité sur $\mathbf{G}$ est utile pour cela. Par exemple, les $\mathbb{R}$-groupes $\mathbf{G} = \mathbf{PGL}(3)$ et $\mathbf{H} = \mathbf{SL}(3)$ ont des points réels isomorphes $\mathbf{G}_\mathbb{R} \simeq \mathbf{H}_\mathbb{R}$ sans être $\mathbb{R}$-isomorphe.

- Le théorème de superrigidité et sa démonstration sont valables dans un cadre beaucoup plus large : non seulement, on peut remplacer le corps $\ell = \mathbb{R}$ par un corps p-adique, mais, plus généralement, on peut prendre pour G un groupe sans facteur compact qui est un produit fini $G = \prod G_p$, avec p premier ou ∞ et avec G_p le groupe des $\mathbb{Q}_p$-points d'un $\mathbb{Q}_p$-groupe semisimple simplement connexe sous l'hypothèse $\sum_p \mathrm{rang}_{\mathbb{Q}_p} G_p \geq 2$.

Stratégie de la démonstration du théorème 10.1

Soit P un sous-groupe parabolique minimal de G, K un sous-groupe compact maximal de G, $\mathbf{V}$ une k-représentation de $\mathbf{H}$. Le groupe $H := \mathbf{H}_k$ agit donc dans $V := \mathbf{V}_k$. On note ν_0 la probabilité K-invariante sur la variété des drapeaux G/P.

Dans la section 7.4, on a montré qu'il existe une application ν_0-mesurable Γ-équivariante

$$\varphi : G/P \to \mathcal{P}(\mathbb{P}(V))$$

de la variété des drapeaux G/P muni d'une probabilité K-invariante ν_0 dans l'espace des probabilités sur l'espace projectif $\mathbb{P}(V)$. On vérifie tout d'abord en 10.2 que l'on peut choisir la représentation de $\mathbf{H}$ dans $\mathbf{V}$ de sorte que $\pi(\Gamma)$ soit proximal.

La deuxième étape en 10.3 consiste à remplacer l'espace d'arrivée par l'espace projectif $\mathbb{P}(V)$ lui-même en montrant que l'image de φ est formée de masses de Dirac. Pour cela, on utilise la probabilité sur Γ dont la mesure stationnaire correspondante sur G/P est ν_0, probabilité que nous avons construit dans la section 9.4. On obtient ainsi une application mesurable Γ-équivariante

$$\Phi : G/P \to \mathbb{P}(V).$$

En utilisant aussi la représentation duale, on pourra remplacer cet espace projectif par un espace vectoriel W. Le prix à payer sera de perdre une partie de la P-invariance : on obtiendra une application mesurable Γ-équivariante

$$\Theta : G \to W$$

qui est seulement invariante à droite par un sous-espace de Cartan A de G.

La troisième étape en 10.4 consiste à montrer que l'espace vectoriel E engendré par les translatés à droite de Θ par les éléments de G est de dimension finie. C'est dans cette étape que l'on utilise l'hypothèse de rang au moins 2 via l'ergodicité des sous-groupes A' de codimension 1 dans A.

La dernière étape en 10.5 consiste à remarquer que la représentation de G dans E est mesurable et donc continue, par suite que l'application Θ est aussi continue. C'est grâce à l'application $\delta : E \to W$ d'évaluation en e que l'on construira alors le morphisme de G dans H qui prolonge π.

10.2 Valeurs propres de même module

Dans cette section, on montre que, comme $\pi(\Gamma)$ n'est pas borné, on peut remplacer la k-représentation irréductible de $\mathbf{H}$ dans $\mathbf{V}$ par une dans laquelle $\pi(\Gamma)$ est proximal (c.f. définition 9.5).

Pour cela, on appliquera le lemme suivant au groupe $\Delta := \pi(\Gamma)$.

Lemme 10.2 *Soit $k = \mathbb{R}$, $\mathbb{C}$ ou une extension finie de $\mathbb{Q}_p$. Soient $V = k^d$ et $\Delta \subset \mathrm{End}(V)$ un sous-groupe tel que V est irréductible et tel que tout élément de Δ a toutes ses valeurs propres de module 1. Alors Δ est borné.*

Remarque L'hypothèse "V irréductible" est utile, comme le prouve le groupe des matrices unipotentes triangulaires supérieures.

Démonstration du lemme 10.2 Le sous-espace vectoriel A de $\mathrm{End}(V)$ engendré par Δ est une algèbre.

Vérifions tout d'abord que *la forme bilinéaire symétrique sur A donnée par $(a,b) \to \mathrm{tr}(ab)$ est non dégénérée.* Soit I le noyau de cette forme bilinéaire, c'est un idéal de A. Pour tout $a \in I$, on a $\mathrm{tr}(a) = \mathrm{tr}(a^2) = \cdots = \mathrm{tr}(a^d) = 0$. Donc a est nilpotent. Le théorème 2.3 d'Engel assure que le sous-espace $V' := \cap_{a\in I}\mathrm{Ker}(a)$ est non nul. Ce sous-espace est A-invariant. Il est donc égal à V. Mais alors $I = 0$. C'est ce que l'on voulait

Montrons maintenant que Δ *est borné.* Choisissons une famille (δ_i) d'éléments de Δ qui forment une base de l'espace vectoriel A et notons (e_i) la base de A duale. On a l'égalité, pour tout g dans Δ : $g = \sum_i \mathrm{Tr}(g\delta_i)e_i$. Les éléments $g\delta_i$ sont dans Δ. L'hypothèse sur les valeurs propres des éléments de Δ assure que, pour tout i, $|\mathrm{Tr}(g\delta_i)| \leq d$. Donc Δ est borné. □

Proposition 10.3 *Sous les hypothèses du théorème 10.1, il existe une k-représentation irréductible de $\mathbf{H}$ dans un espace vectoriel $\mathbf{V}$ telle que $\pi(\Gamma)$ est proximal.*

Démonstration D'après le lemme 10.2, il existe au moins un élément $\delta_0 \in \pi(\Gamma)$ qui admet une valeur propre de module différent de 1. Notons $\mathbf{V}_0$ le sous-espace de $\mathbf{V}$ somme des sous-espaces caractéristiques de δ_0 associés aux valeurs propres de module maximum. Comme $\mathbf{H}$ est simple, il agit sur $\mathbf{V}$ par des matrices de déterminant 1 et l'entier $d_0 := \dim \mathbf{V}_0$ est inférieur à d. Comme $\mathbf{H}$ est simple, on peut décomposer la représentation de $\mathbf{H}$ dans $\Lambda^{d_0}\mathbf{V}$ en représentations irréductibles (proposition 4.12). Notons $\mathbf{V}'$ la sous-représentation irréductible $\Lambda^{d_0}\mathbf{V}$ dans laquelle apparait l'unique valeur propre de module maximum de $\Lambda^{d_0}\delta_0$. L'action de $\pi(\Gamma)$ sur $\mathbb{P}(V')$ est proximale, car, par construction, la suite $n \mapsto \Lambda^{d_0}\delta_0^n$ convenablement renormalisée converge vers un opérateur de rang 1. □

10.3 Construction de Θ

Dans cette section, on utilise tous les préparatifs du chapitre 9 pour construire l'application aux bord $\Phi : G/P \to \mathbb{P}(V)$ ainsi que l'application Θ.

Rappelons que ν_0 est la probabilité K-invariante sur G/P.

Proposition 10.4 *Sous les hypothèses du théorème 10.1. Soit $\mathbf{V}$ une k-représentation irréductible de $\mathbf{H}$ dans laquelle $\pi(\Gamma)$ est proximal.*
a) Toute application ν_0-mesurable Γ-équivariante $\varphi : G/P \to \mathcal{P}(\mathbb{P}(V))$ prend ses valeurs dans l'ensemble $\delta_{\mathbb{P}(V)}$ des masses de Dirac.
b) Il existe une et une seule application ν_0-mesurable Γ-équivariante $\Phi : G/P \to \mathbb{P}(V)$.

Remarque Nous n'utiliserons pas l'unicité de Φ dans la suite du raisonnement. Il est néanmoins rassurant de savoir que cette application au bord Φ est unique.

Démonstration a) D'après la proposition 9.10, il existe une probabilité $\mu \in \mathcal{P}(\Gamma)$ de support Γ telle que ν_0 est μ-stationnaire. Le point a) résulte alors de la proposition 9.9.a.

b) L'existence d'une application φ résulte de la proposition 7.11 de Furstenberg. L'existence de l'application Φ s'en déduit par a). L'unicité de l'application Φ résulte de la proposition 9.9.b. □

Notre tache consiste maintenant à "remplacer" l'espace projectif $\mathbb{P}(V)$ par un k-espace vectoriel W. C'est ce que fait la proposition suivante. Notons A un sous-espace de Cartan de G.

Proposition 10.5 *Sous les hypothèses du théorème 10.1. Il existe une k-représentation ρ de $\mathbf{H}$ dans un espace vectoriel $\mathbf{W}$ et une application mesurable Γ-équivariante non constante $\Theta : G \to \mathbf{W}_k$, qui est A-invariante.*

De façon plus précise, notons $W = \mathbf{W}_k$, $F_\Gamma(G, W)$, le k-espace vectoriel des (classes de) fonctions mesurables Γ-équivariantes de G dans W, c'est-à-dire des fonctions $f : G \to W$ telles que $f(\gamma g) = \rho(\gamma) f(g)$, pour tout $\gamma \in \Gamma$, $g \in G$. Le groupe G agit sur $F_\Gamma(G, W)$ par, pour tous $g, x \in G$, $(T(g)f)(x) = f(gx)$. La proposition 10.5 affirme que l'espace $F_\Gamma(G, W)$ contient une fonction Θ non constante telle que $T(A)\Theta = \Theta$.

Démonstration de la proposition 10.5 On applique la proposition 10.4 à la représentation de $\mathbf{H}$ dans $\mathbf{V}$ donnée par la proposition 10.3 ainsi qu'à sa représentation duale. On obtient ainsi deux applications ν_0-mesurables et Γ-équivariantes $\varphi : G/P \to \mathbb{P}(V)$ et $\psi : G/P \to \mathbb{P}(V^*)$. On a donc une application $\nu_0 \otimes \nu_0$-mesurable et Γ-équivariante

$$\varphi \times \psi : G/P \times G/P \to \mathbb{P}(V) \times \mathbb{P}(V^*).$$

Vérifions tout d'abord que *le produit $G/P \times G/P$ s'identifie à un quotient de G/A*, à une partie $\nu_0 \otimes \nu_0$-négligeable près. Conformément aux notations de la section 3.5, fixons un sous-espace de Cartan A de G, une chambre de Weyl $A^+ \subset A$, une involution de Cartan θ de G telle que $\theta(A) = A$. On peut supposer que le parabolique minimal P est celui associé à A^+. On note P^- le parabolique opposé et on note K le sous-groupe compact maximal $K = G^\theta$. Par le même argument que dans la démonstration du théorème 3.13.b, on construit un élément $w_0 \in K$ tel que w_0 normalise A et tel que $w_0(A^+)$ est la chambre de Weyl opposée de sorte que $P^- = w_0 P w_0^{-1}$. Autrement dit, le stabilisateur dans G du point $w_0 P \in G/P$ est le groupe P^-.

Par le théorème 3.14.c, la P-orbite de cet élément $w_0 P \in G/P$ est ouverte de mesure pleine dans $G/P \simeq G/P^-$. Donc la G-orbite dans $G/P \times G/P$ du point $(P, w_0 P)$ est ouverte, de mesure pleine et de groupe d'isotropie $P \cap P^-$.

Vérifions maintenant que l'image de $\varphi \times \psi$ ne rencontre pas la quadrique $\mathbb{Q}(V) := \{(x, y) \in \mathbb{P}(V) \times \mathbb{P}(V^*) \mid y(x) = 0\}$. Cela résulte de ce que la mesure image $(\varphi \times \psi)_*(\nu_0 \otimes \nu_0)$ est une mesure produit et que, par le lemme 9.7, la probabilité μ-stationnaire $\varphi_*(\nu_0)$ ne masse pas les hyperplans.

On note W l'espace vectoriel $\mathrm{End}(V)$. Pour tout $(x, y) \in \mathbb{P}(V) \times \mathbb{P}(V^*) \smallsetminus \mathbb{Q}(V)$, on note $p_{x,y} \in W$ le projecteur sur x parallèlement à y. La formule

$$\Theta(g) = p_{\varphi(gP),\psi(gw_0P)}$$

donne alors l'application Θ cherchée. □

10.4 L'espace E des translatés de Θ

> Nous disposons enfin d'une application Γ-équivariante, A-invariante, non constante Θ de G dans un espace vectoriel W. On étudie dans cette section la représentation de G dans l'espace E des translatés de Θ.

Rappelons que ρ est la représentation de $\mathbf{H}$ dans $\mathbf{W}$ et que $F_\Gamma(G, W)$ est le k-espace vectoriel des fonctions mesurables Γ-équivariantes de G dans W. Géométriquement, ce sont les sections mesurables d'un fibré vectoriel sur $\Gamma\backslash G$ appelé le *fibré induit par* W. Rappelons aussi que nous avons noté T l'action mesurable du groupe G sur $F_\Gamma(G, W)$ Cette action est donnée par, pour tous $g, x \in G$,

$$(T(g)f)(x) = f(xg) \ .$$

Par construction la fonction Θ est un élément A-invariant de $F_\Gamma(G, W)$. Cette action T est mesurable si on munit $F_\Gamma(G, W)$ de la convergence en mesure.

Proposition 10.6 *Si* $\mathrm{rang}_{\mathbb{R}}(G) \geq 2$*, l'espace vectoriel* $E = \langle T(g)\Theta \mid g \in G\rangle$ *est de dimension finie.*

En outre, la fonction Θ *est continue.*

Remarque En particulier, comme Θ n'est pas constante, le corps k ne peut pas être totalement discontinu. On a donc que $k = \mathbb{R}$ ou $\mathbb{C}$.

Cette proposition 10.6 sera une conséquence des trois lemmes 10.7 et 10.8 ci-dessous.

Lemme 10.7 *Soit* $A' \subset A$ *un sous-groupe non trivial,* $Z(A')$*le centralisateur de* A' *dans* G *et* $I \subset F_\Gamma(G, W)$ *un sous-espace vectoriel* A*-invariant de dimension finie. Alors le sous-espace vectoriel* $I' = \langle T(g)f \mid g \in Z(A') \ , \ f \in I\rangle$ *est encore* A*-invariant et de dimension finie.*

Démonstration du lemme 10.7 Comme A normalise A', ce sous-espace vectoriel I' est bien A-invariant. Montrons que I' est de dimension finie. Regardons pour cela I comme un A'-module. Il suffit de montrer que le k-espace vectoriel $S = \mathrm{Hom}_{A'}(I, F_\Gamma(G, W))$ est de dimension finie, car chaque élément g de $Z(A')$ agit sur I via un élément de cet espace vectoriel S. Or on a une identification naturelle

$$S \simeq F_\Gamma(G, \mathrm{Hom}(I, W))^{A'}$$

de S avec l'ensemble des sections mesurables A'-invariantes du fibré sur $\Gamma\backslash G$ induit par $\mathrm{Hom}(I, W)$.

Comme $A' \neq 1$, le corollaire 7.7 affirme que l'action de A' sur $\Gamma\backslash G$ est ergodique. Nous allons en déduire que S est de dimension finie.

Plus précisément, pour toute famille $f_1, \ldots, f_i \in S$ et $g \in G$, on note,

$$m(g) := \dim(\langle f_j(g) \mid 1 \leq j \leq i \rangle).$$

La fonction mesurable $m : G \to \mathbb{N}$ vérifie, pour tout $\gamma \in \Gamma, a' \in A'$

$$m(\gamma g a') = m(g), \quad \text{pour presque tout } g.$$

Par ergodicité, la fonction m est donc constante égale à un entier m_0. Cet entier m_0 est majoré par $\dim(\mathrm{Hom}(I, W))$. On peut choisir la famille $f_1, \ldots, f_i$ de sorte que m_0 soit maximal. On peut aussi choisir cette famille de sorte que $i = m_0$. Soit $f \in S$. Par maximalité de m_0, on peut trouver des fonctions mesurables $c_j : G \to k$ telles que, pour presque tout $g \in G$, on ait

$$f(g) = \textstyle\sum_{1 \leq j \leq m_0} c_j(g) f_j(g).$$

L'indépendance des $f_j(g)$ et les propriétés de Γ-équivariance et de A'-équivariance des fonctions f et f_j prouvent que, pour tout $\gamma \in \Gamma, a' \in A'$

$$c_j(\gamma g a') = c_j(g), \quad \text{pour presque tout } g.$$

De nouveau, par ergodicité, les fonctions c_j sont constantes. L'espace vectoriel S est donc de dimension finie. □

Lemme 10.8 *Soient* $\mathbf{G}$ *un* $\mathbb{R}$*-groupe semisimple connexe,* $G = \mathbf{G}_\mathbb{R}$ *et* A *un sous-espace de Cartan de* G*. Si* $\mathrm{rang}_\mathbb{R}(G) \geq 2$*, il existe une suite* $A_1, \ldots, A_s$ *de sous-groupes non triviaux de* A *telle que, en notant* $Z(A_i)$ *le centralisateur de* A_i *dans* G*, la multiplication*

$$\begin{array}{ccc} Z(A_1) \times \cdots \times Z(A_s) & \longrightarrow & G \\ (z_1, \ldots, z_s) & \mapsto & z_1 \cdots z_s \end{array}$$

est surjective.

Démonstration Notons $\Sigma^+ = \{\lambda_1, \dots \lambda_t\}$ un système de racines positives de A dans G et $A_i \subset A$ le noyau de λ_i. Comme $\mathrm{rang}_{\mathbb{R}}(G) \geq 2$, ces groupe A_i sont non triviaux. L'ensemble $X = Z(A_1) \cdots Z(A_t)$ contient le parabolique minimal P associé à Σ^+ ainsi que le parabolique opposé P^-. Donc l'ensemble $Y = X\,X$ contient l'ouvert $U = P^-P$. D'après la démonstration du théorème 3.14.c, cet ouvert est dense dans G. Donc $G = Y\,Y$. C'est ce que l'on voulait. □

C'est le lemme 10.9.b ci-dessous qui nous fera passer du monde mesurable au monde continu.

Lemme 10.9 *Soient G_1 et G_2 deux groupes localement compacts séparables.*
a) Pour toute partie $W_1 \subset G_1$ de mesure positive pour la mesure de Haar de G_1, l'ensemble $W_1W_1^{-1}$ contient un voisinage de e.
b) Tout morphisme de groupes mesurable $\varphi : G_1 \to G_2$ est continu.

Démonstration a) On note μ_1 la mesure de Haar de G_1. Quitte à réduire W_1, on peut supposer que $\mu_1(W_1) < \infty$. Or si $\alpha, \beta \in L^2(G_1, \mu_1)$, la convolée $g \mapsto (\alpha * \beta)(g) = \int_G \alpha(gx)\beta(x^{-1})d\mu_1(x)$ est une fonction continue : on le vérifie d'abord pour α, β continues à support compact et on conclut par densité.

Donc la fonction $\mathbf{1}_{W_1} * \mathbf{1}_{W_1^{-1}}$ est une fonction continue qui vaut $\mu(W_1)$ en l'identité. Elle est donc strictement positive dans un voisinage de l'identité. Or elle est nulle en dehors de $W_1W_1^{-1}$. Donc $W_1W_1^{-1}$ contient un voisinage de e.

b) Soit $V_2 \subset G_2$ un voisinage de l'identité dans G_2. On veut montrer que $V_1 := \varphi^{-1}(V_2)$ est un voisinage de l'identité dans G_1. Choisissons un ouvert $W_2 \subset G_2$ tel que $W_2W_2^{-1} \subset V_2$. Comme G_2 est séparable, il existe une famille dénombrable d'éléments $g_p \in G_2$ tels que les translatés W_2g_p recouvrent G_2. Mais alors les images inverses $\varphi^{-1}(W_2g_p)$ recouvrent G_1. L'une d'elles $W_1 = \varphi^{-1}(W_2g_{p_0})$ est donc de mesure non nulle. Comme $W_1W_1^{-1} \subset V_1$, on conclut à l'aide du a). □

Démonstration de la proposition 10.6 Posons $I_0 := \langle \Theta \rangle$ et, pour $i = 1, \dots, s$, posons $I_i = \langle T(Z(A_i))I_{i-1} \rangle$. Par une application répétée du lemme 10.7, l'espace I_ℓ est de dimension finie. Par le lemme 10.8, il est égal à E.

Montrons maintenant la continuité de Θ. Plus généralement, on va montrer que toute fonction $f \in E$ est continue. Comme E est de dimension finie, le lemme 10.9 prouve que le morphisme mesurable $T : G \to \mathrm{GL}(E)$ est continu. Notons $f_1, \dots, f_i$ une base de E. On a donc des fonctions continues $c_j : G \to k$ telles que, pour tout g dans G, on a

$$T(g)f = \textstyle\sum_j c_j(g)f_j.$$

Par Fubini, pour presque tout $x_0 \in G$, on a l'égalité

$$f(gx_0) = \textstyle\sum_j c_j(g)f_j(x_0)$$

pour presque tout $g \in G$. Donc f est continue et Θ aussi. □

Remarque Comme Θ n'est pas constant, cela ne peut se produire que si $k = \mathbb{R}$ ou $\mathbb{C}$.

10.5 Prolongement de π à G

Nous pouvons maintenant construire le prolongement de π que nous cherchons grâce à la représentation de G dans E et grâce à l'évaluation en e qui relie E et W.

Notons $\delta : E \to W; f \mapsto f(e)$ l'évaluation en l'identité et rappelons que ρ est la représentation de H dans W.

Lemme 10.10 *a) L'application δ est Γ-équivariante, i.e. pour tout $\gamma \in \Gamma$, on a $\delta \circ T(\gamma) = \rho(\pi(\gamma)) \circ \delta$.*
b) L'application δ est injective.
c) Son image $\delta(E)$ est un sous-espace H-invariant de W.

Démonstration Comme $G = \mathbf{G}_{\mathbb{R}}$ est semisimple et connexe, la représentation T de G s'étend en une $\mathbb{R}$-représentation de $\mathbf{G}$ encore notée T. C'est vrai du moins si $\mathbf{G}$ est le quotient du $\mathbb{R}$-groupe algébrique simplement connexe $\widetilde{\mathbf{G}}$ dont l'algèbre de Lie est $Lie(G)_{\mathbb{C}}$ par le noyau Z du morphisme $(\widetilde{\mathbf{G}})_{\mathbb{R}} \to G$, ce que l'on peut supposer. Rappelons aussi que ρ est la restriction d'une $\mathbb{R}$-représentation ρ de $\mathbf{H}$.

a) On a les égalités, pour $f \in E$,

$$\delta \circ T(\gamma)\ (f) = f(\gamma) = \rho(\pi(\gamma))(f(e)) = \rho(\pi(\gamma)) \circ \delta\ (f).$$

b) Le noyau $\mathrm{Ker}(\delta)$ est un sous-espace Γ-invariant de E. Par le théorème 7.1 de densité de Borel, le réseau Γ est Zariski dense dans G, et donc le noyau $\mathrm{Ker}(\delta)$ est aussi G-invariant. Donc, si f est dans $\mathrm{Ker}(\delta)$, pour tout $g \in G$, on a, $f(g) = \delta(T(g)f) = 0$ et $f = 0$.

c) L' image $\delta(E)$ est $\pi(\Gamma)$-invariante. Par hypothèse $\pi(\Gamma)$ est Zariski dense dans H. Donc $\delta(E)$ est H-invariant. □

Fin de la démonstration du théorème 10.1 On sait déjà que $k = \mathbb{R}$ ou $\mathbb{C}$. Grace au lemme 10.10, on peut identifier E avec son image $\delta(E)$. On dispose donc dans E d'une représentation T de G et d'une représentation ρ de H telles que, pour tout $\gamma \in \Gamma$, on a

$$T(\gamma) = \rho(\pi(\gamma)).$$

Par le corollaire 4.5, l'image $\rho(\mathbf{H})$ est Zariski fermée. Par le théorème 7.1 de densité de Borel, le réseau Γ est Zariski dense dans G. Donc $T($**G** est inclus dans $\rho(\mathbf{H})$. Comme **H** est simple, ρ est injectif et est donc un $\mathbb{R}$-isomorphisme sur son image. Le $\mathbb{R}$-morphisme $\rho^{-1} \circ T : \mathbf{G} \longrightarrow \mathbf{H}$ prolonge π. □

11 Arithméticité

Nous avons montré dans le chapitre 5 le théorème de Borel Harish-Chandra qui affirme que "tout groupe arithmétique est un réseau". Le but de ce chapitre est de démontrer le théorème d'arithméticité de Margulis qui en est une réciproque en rang réel au moins 2.

11.1 Groupes arithmétiques

Nous devons tout d'abord étendre légèrement la définition 5.1 de groupes arithmétiques

Définition 11.1 *Soit $G = \mathbf{G}_{\mathbb{R}}$ le groupe des $\mathbb{R}$-points d'un $\mathbb{R}$-groupe semisimple connexe à centre trivial. Un réseau $\Gamma \subset G$ est dit arithmétique si il existe un $\mathbb{Q}$-groupe semisimple $\mathbf{H}$ et un morphisme continu surjectif $p : \mathbf{H}_{\mathbb{R}} \to G$ de noyau compact tel que les réseaux $p(H_{\mathbb{Z}})$ et Γ sont commensurables.*

Théorème 11.2 (Margulis) *Soit $G = \mathbf{G}_{\mathbb{R}}$ le groupe des $\mathbb{R}$-points d'un $\mathbb{R}$-groupe semisimple. On suppose G sans facteur compact et $\mathrm{rang}_{\mathbb{R}}(G) \geq 2$.*

Alors tout réseau irréductible $\Gamma \subset G$ est arithmétique.

Exemple Reprenons l'exemple A de la section 10.1.

Pour la forme quadratique q sur $\mathbb{R}^5$, $q(x) = x_1^2 + x_2^2 + x_3^2 - \sqrt{2}x_4^2 - \sqrt{2}x_5^2$, le groupe $\Gamma = \mathrm{SL}(5, \mathbb{Z}[\sqrt{2}]) \cap \mathrm{SO}(q, \mathbb{R})$ est un sous-groupe arithmétique de $\mathrm{SO}(q, \mathbb{R})$.

En effet, le groupe $\mathbf{H}_{\mathbb{Z}} = \{(g, g^\sigma) \mid g \in \mathrm{SL}(5, \mathbb{Z}[\sqrt{2}]) \cap \mathrm{SO}(q, \mathbb{R})\}$ est un sous-groupe arithmétique d'un $\mathbb{Q}$-groupe noté $\mathbf{H} = \mathbf{R}_{\mathbb{Q}[\sqrt{2}]|\mathbb{Q}}(\mathbf{SO}(q))$ tel que $\mathbf{H}_{\mathbb{R}} = \mathrm{SO}(q, \mathbb{R}) \times \mathrm{SO}(q^\sigma, \mathbb{R})$. Comme le groupe $\mathrm{SO}(q^\sigma)$ est compact, Γ est bien un groupe arithmétique.

Stratégie de démonstration du théorème 11.2

On vérifie tout d'abord que Γ est un groupe de type fini de sorte que le corps K engendré par les traces des éléments de Γ est un corps de type fini.

On rappelle ensuite comment construire de nombreux plongements des corps de type fini dans les corps locaux.

On utilise ces plongements pour construire des représentations de Γ à coefficients dans les corps locaux, représentations auxquelles on applique le théorème de superrigidité pour montrer que le corps K est une extension finie de $\mathbb{Q}$.

Cela permet alors, grâce à la "restriction de Weil" de construire une représentation de Γ à coefficients dans $\mathbb{Q}$, représentation à laquelle on applique la superrigidité p-adique pour montrer que les dénominateurs qui apparaissent dans les coefficients matriciels sont uniformément bornés. On aura ainsi réalisé un sous-groupe d'indice fini Γ' de Γ comme un sous-groupe de $\mathrm{GL}(d, \mathbb{Z})$.

On verra que Γ' est d'indice fini dans le groupe des points entiers de son adhérence de Zariski. La superrigidité réelle sera utile pour cela.

11.2 Les réseaux sont de type fini

Nous admettrons dans cette section un point certes crucial mais pas très surprenant.

Proposition 11.3 *Un réseau Γ du groupe des $\mathbb{R}$-points $G = \mathbf{G}_{\mathbb{R}}$ d'un $\mathbb{R}$-groupe $\mathbf{G}$ est de type fini.*

Cette proposition s'étend aux réseaux des produits finis $G = \prod G_p$ de groupes réels et p-adiques.

Nous admettrons cette proposition 11.3 dans sa généralité. Néanmoins, il y a un cas où la démonstration est assez rapide :

1er cas : Si Γ est cocompact dans G.
Dans ce cas, Γ est le groupe fondamental d'une variété compacte. Il est donc de type fini, et même de présentation finie.

2ème cas : Si G ne contient pas de facteurs quasisimples G_i de rang réel 1.
Dans ce cas, la proposition est due à Kazhdan et la démonstration repose sur la propriété T de Kazhdan. Elle est détaillée dans le chapitre 3 de [4] dans un esprit très proche de ce cours. Je ne la recopie pas ici. Les grandes lignes sont : comme $\text{rang}_{\mathbb{R}}(G_i) \geq 2$, le groupe G a la propriété T de Kazhdan, donc le réseau Γ aussi et donc Γ est de type fini.

3ème cas : Si G contient un facteur quasisimple de rang réel 1.
Le fait que Γ soit de type fini est dû à Raghunathan, voir [21] corollaire 13.10.

11.3 Algébricité des valeurs propres

Dans cette section on utilise la superrigidité pour montrer l'algébricité des valeurs propres des éléments de $\text{Ad}\Gamma$.

Proposition 11.4 *Sous les hypothèses du théorème 11.2.*
Pour tout $\gamma \in \Gamma$, les valeurs propres de $\text{Ad}\gamma$ sont des nombres algébriques.

Pour montrer cette proposition, nous aurons besoin de construire des plongements des extensions de type fini de $\mathbb{Q}$.

Lemme 11.5 *Soit K une extension de type fini de $\mathbb{Q}$, λ un élément de K transcendant sur $\mathbb{Q}$. Alors il existe un corps local p-adique k et un morphisme de corps $\sigma : K \to k$ tel que $|\sigma(\lambda)| > 1$.*

Démonstration du lemme 11.5 Mettons λ dans une famille maximale $\lambda_1 = \lambda, \lambda_2, \ldots, \lambda_r$ d'éléments de K algébriquement indépendants sur $\mathbb{Q}$ et notons

$K' = \mathbb{Q}(\lambda_1, \ldots, \lambda_r) \subset K$. Il est facile de trouver un plongement $\sigma' : K' \to \mathbb{Q}_p$ tel que $|\sigma'(\lambda)| > 1$. On étend alors ce plongement en un morphisme de l'extension finie K de K' vers une extension finie k de $\mathbb{Q}_p$. □

Démonstration de la proposition 11.4 Décomposons l'algèbre de Lie $\mathfrak{g}$ de G en somme d'idéaux simples et fixons une base de ces idéaux. Soit K_0 le corps engendré par les coefficients matriciels d'une famille finie génératrice du groupe $\mathrm{Ad}\Gamma$. Ce corps est de type fini. Le groupe adjoint $\mathbf{G}'$ de $\mathbf{G}$ est donc un groupe semisimple défini sur K_0 tel que $\mathrm{Ad}\Gamma \subset \mathbf{G}'_{K_0}$.

Supposons que l'adjoint $\mathrm{Ad}\gamma$ d'un élément $\gamma \in \Gamma$ a une valeur propre λ transcendante sur $\mathbb{Q}$. Le lemme 11.4 permet de construire un morphisme de corps $K_0[\lambda] \to k$ dans un corps local p-adique tel que $|\sigma(\lambda)| > 1$.

Comme le groupe $\mathbf{G}'$ est un produit de groupes k-simples et que l'image de Γ est Zariski dense dans $\mathbf{G}'$, le théorème 10.1 de superrigidité affirme que l'image de Γ dans $\mathbf{G}'_k$ est bornée. Mais par construction, le groupe engendré par $\mathrm{Ad}\gamma$ n'est pas borné. Contradiction. □

Remarque On a basé la démonstration de la proposition 11.4 sur la superrigidité p-adique. On aurait pu aussi bien utiliser ici la superrigidité réelle.

11.4 Corps de définition de G

Nous déterminons dans cette section le plus petit corps de définition de Γ

Notons K le corps engendré par les traces $Tr(\mathrm{Ad}\gamma)$ pour $\gamma \in \Gamma$.

Proposition 11.6 *Sous les hypothèses du théorème 11.2.*
a) Le corps K est un corps de nombre i.e. une extension finie de $\mathbb{Q}$.
b) Il existe un $\mathbb{R}$-morphisme injectif $i : \mathbf{G} \to \mathbf{GL}(m)$ tel que $i(\Gamma) \subset \mathrm{SL}(m, K)$
c) Le groupe $i(\mathbf{G})$ est défini sur K.

Démonstration de la proposition 11.6

a) D'après la proposition 11.4, le corps K est une extension algébrique de $\mathbb{Q}$. Or ce corps K est une extension de type fini de $\mathbb{Q}$. C'est donc une extension finie de $\mathbb{Q}$.

b) Notons $\mathbb{R}[G]$ l'anneau des fonctions régulières et réelles sur G. Le groupe G agit sur $\mathbb{R}[G]$ par translation à droite. Pour tout $\varphi \in \mathbb{R}[G]$ et $g, x \in G$

$$(T(g)\varphi)(x) = \varphi(xg)$$

Soit φ_0 l'élément de $\mathbb{R}[G]$ donné par $\varphi_0(g) = \mathrm{Tr}(\mathrm{Ad}g)$ et $E := \langle T(G)\varphi_0 \rangle$ le $\mathbb{R}$-sous-espace vectoriel de dimension finie m engendré par les translatés de φ_0. Le morphisme $i = T|_E$ provient d'un $\mathbb{R}$-morphisme $i : \mathbf{G} \to \mathbf{GL}(m)$.

Montrons que i *est injectif.* Soit $g \in \mathbf{G}$ un élément du noyau de i. Pour tout $x \in \mathbf{G}$ on a donc

$$\mathrm{Tr}(\mathrm{Ad}x\mathrm{Ad}g) = \mathrm{Tr}(\mathrm{Ad}x).$$

On a donc pour tout $n \geq 0$

$$\mathrm{Tr}(\mathrm{Ad}g^n) = \mathrm{Tr}(\mathrm{Ad}g^{n-1}) = \cdots = \dim \mathfrak{g}.$$

L'élément g est donc unipotent. Le noyau de i est donc un sous-groupe semisimple de $\mathbf{G}$ dont tous les éléments sont unipotents. Il est donc trivial. Le morphisme i est bien injectif.

Montrons qu'*il existe une base* $\varphi_1, \ldots, \varphi_m$ *de* E *dans laquelle les éléments de* $i(\Gamma)$ *sont à coefficients dans* K. Par le théorème 7.1 de densité de Borel, Γ est Zariski dense dans G et il existe $\gamma_1, \ldots, \gamma_m \in \Gamma$ tels que les m translatés $\varphi_i = T(\gamma_i)\varphi_0$ forment une base de E. Ecrivons, pour $\gamma \in \Gamma$,

$$T(\gamma)\varphi_j = \sum_i a_{i,j}^{\gamma} \varphi_i \ .$$

De nouveau, comme Γ est Zariski dense dans G, les restrictions des fonctions φ_j sont encore linéairement indépendantes. On peut donc trouver $\gamma'_1, \ldots, \gamma'_m \in \Gamma$ tels que la matrice $(\varphi_i(\gamma'_k))$ est une matrice $m \times m$ inversible. Les égalités

$$\sum_i a_{i,j}^{\gamma} \, \varphi_i(\gamma'_k) = (T(\gamma)\varphi_j)(\gamma'_k) = \varphi_0(\gamma'_k \gamma \gamma_j) \in K$$

prouvent que les coefficients $a_{i,j}^{\gamma}$ sont dans K.

c) D'après le corollaire 4.5, le groupe $i(\mathbf{G})$ est algébrique. Le fait qu'il soit défini sur K résulte du théorème 7.1 de densité de Borel et du lemme 7.2. □

11.5 Restriction de K à $\mathbb{Q}$

La dernière étape consiste à remplacer le corps de nombre K par $\mathbb{Q}$ grâce au procédé de *restriction à la Weil.*

On utilise dans cette étape, à la fois la superrigidité réelle et la superrigidité p-adique.

Le théorème 11.2 d'arithméticité est une conséquence de la proposition suivante.

Proposition 11.7 *Sous les hypothèses du théorème 11.2.*
Il existe un $\mathbb{Q}$*-groupe semisimple* $\mathbf{H}$ *à centre trivial, un morphisme* $\varphi : \Gamma \to \mathbf{H}_{\mathbb{Q}}$ *et un morphisme continu* $p : \mathbf{H}_{\mathbb{R}} \to G$ *tels que*
a) $\pi = p \circ \varphi$.
b) Le sous-groupe $\Gamma' := \{\gamma \in \Gamma \mid \varphi(\Gamma) \in \mathbf{H}_{\mathbb{Z}}$ *est d'indice fini dans* Γ.
c) Le noyau $\mathrm{Ker}\, p$ *est compact.*
d) Les groupes Γ *et* $p(\mathbf{H}_{\mathbb{Z}})$ *sont commensurables.*

Démonstration de la proposition 11.7

D'après la proposition 11.6, on peut supposer que $\mathbf{G} \subset \mathbf{GL}(m)$ est défini sur un corps de nombre K et que $\Gamma \subset \mathbf{G}_K$.

a) Commençons par rappeler la construction et les propriétés de la "restriction de Weil" $\mathbf{H} = \mathbf{R}_{K|\mathbb{Q}}(\mathbf{G})$. Identifions K à un sous-corps de $\mathbb{R}$ et notons $\sigma_1, \ldots, \sigma_{r_1}$ les morphismes de K dans $\mathbb{R}$, avec $\sigma_1 = Id$, et $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+1}, \ldots, \overline{\sigma}_{r_1+r_2}$ les morphismes de K dans $\mathbb{C}$ de sorte que le morphisme σ

$$\begin{array}{ccc} \mathbb{R} \otimes_{\mathbb{Q}} K & \stackrel{\sigma}{\longrightarrow} & \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ k & \mapsto & (\sigma_1(k), \ldots, \sigma_{r_1+r_2}(k)) \end{array}$$

soit un isomorphisme d'algèbres. Regardons K comme un $\mathbb{Q}$-espace vectoriel de dimension ℓ. Notons

$$\varphi : \mathrm{GL}(m, K) \longrightarrow \mathrm{GL}(m\ell, \mathbb{Q})$$

le morphisme de groupes qui s'en déduit. Ce morphisme a son image dans

$$\mathrm{GL}(m, \mathbb{R} \otimes_{\mathbb{Q}} K) \simeq \mathrm{GL}(m, \mathbb{R})^{r_1} \times \mathrm{GL}(m, \mathbb{C})^{r_2} \subset \mathrm{GL}(m\ell, \mathbb{R}).$$

Notons

$$p : \mathrm{GL}(m, \mathbb{R} \otimes_{\mathbb{Q}} K) \longrightarrow \mathrm{GL}(m, \mathbb{R})$$

la projection sur le premier facteur.

Le groupe $\mathrm{GL}(m, K)$ s'identifie ainsi au groupe $\mathbf{R}_{\mathbb{Q}}$ des $\mathbb{Q}$-points d'un $\mathbb{Q}$-sous-groupe $\mathbf{R}$ de $\mathbf{GL}(m\ell)$, dont le groupe des $\mathbb{R}$-points s'identifie à $\mathbf{R}_{\mathbb{R}} \simeq \mathrm{GL}(m, \mathbb{R})^{r_1} \times \mathrm{GL}(m, \mathbb{C})^{r_2}$. Ce $\mathbb{Q}$-groupe est noté $\mathbf{R}_{K|\mathbb{Q}}(\mathbf{GL}(m))$ et est appelé la *restriction de K à $\mathbb{Q}$ de* $\mathbf{GL}(m)$.

Notons $\mathbf{H} = \mathbf{R}_{K|\mathbb{Q}}(\mathbf{G})$ l'adhérence de Zariski de $\varphi(\mathbf{G}_K)$. Comme $\varphi(\mathbf{G}_K)$ est inclus dans $\mathrm{GL}(m\ell, \mathbb{Q})$, le lemme 7.2 affirme que $\mathbf{H}$ est un $\mathbb{Q}$-groupe. En outre, par construction, on a, pour tout algèbre A contenant $\mathbb{Q}$, l'égalité $\mathbf{H}_A \simeq \mathbf{G}_{K \otimes_{\mathbb{Q}} A}$. En particulier, $\mathbf{H}$ est encore un $\mathbb{Q}$-groupe dont les $\mathbb{Q}$-points s'identifient aux K-points de $\mathbf{G}$. Le morphisme φ s'étend en un $\mathbb{Q}$-morphisme encore noté φ de $\mathbf{G}$ dans $\mathbf{H}$. Le groupe des points complexes $\mathbf{H}_{\mathbb{C}}$ s'identifie à $(\mathbf{G}_{\mathbb{C}})^{r_1+2r_2}$. On en déduit que le $\mathbb{Q}$-groupe $\mathbf{H}$ est donc semisimple. Par construction, on a $p(\mathbf{H}_{\mathbb{R}}) = G$ et $p(\varphi(\gamma)) = \gamma$, pour tout $\gamma \in \Gamma$.

b) Comme Γ est de type fini, il existe des nombres premiers $p_1, \ldots, p_r$ tels que

$$\varphi(\Gamma) \subset \mathbf{H}_{\mathbb{Z}[p_1^{-1}, \ldots, p_r^{-1}]}.$$

Soit φ_i la composée $\Gamma \to \mathbf{H}_{\mathbb{Q}} \subset \mathbf{H}_{\mathbb{Q}_{p_i}}$. D'après le théorème de superrigidité, l'image $\varphi_i(\Gamma)$ est relativement compacte dans $\mathbf{H}_{\mathbb{Q}_{p_i}}$. Notons $\mathbb{Z}_p$ l'anneau des entiers de $\mathbb{Q}_p$. Comme le sous-groupe $\mathbf{H}_{\mathbb{Z}_{p_i}}$ est ouvert dans $\mathbf{H}_{\mathbb{Q}_{p_i}}$, le sous groupe $\Gamma' := \cap_i \varphi_i^{-1}(\mathbf{H}_{\mathbb{Z}_{p_i}})$ est d'indice fini dans Γ et vérifie $\varphi(\Gamma') \subset \mathbf{H}_{\mathbb{Z}}$.

c) Montrons que le noyau $\mathrm{Ker}(p)$ est compact. Sinon, on pourrait décomposer $\mathbf{H}$ en produit de $\mathbb{R}$-groupes $\mathbf{H} = \mathbf{G} \times \mathbf{F} \times \mathbf{F}'$ où p est la projection sur le premier

facteur et où $\mathbf{F}$ est simple et $\mathbf{F}_{\mathbb{R}}$ non compact. Notons q la projection sur ce deuxième facteur. L'image $q \circ \varphi(\Gamma)$ est Zariski dense dans $\mathbf{F}$. En particulier, cette image n'est pas bornée. Le théorème 10.1 de superrigidité prouve que $q \circ \varphi$ se prolonge en un morphisme continu $\psi : G \to F$. L'image $\varphi(\Gamma)$ serait alors inclus dans le sous-groupe fermé Graphe$(\psi) \times F'$. Ce groupe n'est pas Zariski dense dans $\mathbf{H}$. Ceci contredit la Zariski densité de $\varphi(\Gamma)$ dans $\mathbf{H}$. Donc le noyau Ker(p) est compact.

d) D'après le c) $\varphi(\Gamma')$ est un réseau de $H_{\mathbb{R}}$. Donc $\varphi(\Gamma')$ est d'indice fini dans $\mathbf{H}_{\mathbb{Z}}$ et Γ et $p(\mathbf{H}_{\mathbb{Z}})$ sont commensurables. □

Remarques (voir [16].IX) - Comme pour le théorème de superrigidité, le théorème d'arithméticité et sa démonstration sont valables dans un cadre beaucoup plus large : on peut prendre pour G un produit fini $G = \prod G_p$, avec p premier ou ∞ et G_p le groupe des $\mathbb{Q}_p$-points d'un $\mathbb{Q}_p$-groupe semisimple sous l'hypothèse $\sum_p \text{rang}_{\mathbb{Q}_p} G_p \geq 2$.

- On peut en outre remplacer cette hypothèse de rang par

$$\Gamma \textit{ est d'indice infini dans son commensurateur } \text{Com}(\Gamma)$$

où $\text{Com}(\Gamma) := \{g \in G \mid g\Gamma g^{-1} \text{ et } \Gamma \text{ sont commensurables } \}$.

- Si $k = \mathbb{R}$ ou $\mathbb{C}$, le groupe $\mathbf{G}_k$ des k-points d'un k-groupe semisimple $\mathbf{G}$ contient toujours des réseaux cocompacts et des réseaux non cocompacts.

- Si k est un corps p-adique, le groupe $\mathbf{G}_k$ des k-points d'un k-groupe semisimple $\mathbf{G}$ contient toujours des réseaux et ceux-ci sont toujours cocompacts.

- Si k est un corps local de caractéristique non nulle, le groupe $\mathbf{G}_k$ des k-points d'un k-groupe semisimple $\mathbf{G}$ contient toujours des réseaux non cocompacts mais pas toujours des réseaux cocompacts.

12 Mesures invariantes

12.1 Mesures U-invariantes sur $\mathbf{SL(2,\mathbb{R})/\Gamma}$

Dans cette partie, nous montrons le théorème mesuré de Ratner pour $G = \mathrm{SL}(2,\mathbb{R})$. Il est dû à Dani dans ce cas.

Proposition 12.1 *Soit* $G = \mathrm{SL}(2,\mathbb{R})$, $U = \{u_s := \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \mid s \in \mathbb{R}\}$. *Soient* $\Gamma \subset G$ *un sous-groupe discret et* μ *une probabilité* U*-invariante* U*-ergodique sur le quotient* $X = G/\Gamma$.

Alors ou bien cette probabilité μ *est portée par une* U*-orbite périodique ou bien cette probabilité* μ *est* G*-invariante.*

Remarques - Lorsque Γ est cocompact, le premier cas est impossible car Γ ne contient pas d'élément unipotent non trivial. (voir la démonstration du corollaire 5.6.b)

- Lorsque Γ n'est pas un réseau, le deuxième cas est impossible car $\mu(X) = 1$.

Dans cette section on notera aussi $A = \{a_t := \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \mid t > 0\}$, B=AU, $U^- = \{u_s^- := \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} \mid s \in \mathbb{R}\}$ et $B^- = AU^-$.

Démonstration de la proposition 12.1 Elle résulte des lemmes suivants. □

Lemme 12.2 *Si* μ *n'est pas portée par une* U*-orbite périodique, alors* μ *est* A*-invariante.*

Lemme 12.3 *Si* μ *est* B*-invariante, alors* μ *est* G*-invariante.*

Démonstration du lemme 12.2 Expliquons tout d'abord la démarche que nous allons suivre. Soit

$$Z = \{x \in X \mid \lim_{t\to\infty} \frac{1}{t} \int_0^t \varphi(u_s x) ds = \int_X \varphi \, d\mu \text{ pour tout } \varphi \in C_c(X)\}.$$

Le théorème 8.6 de Birkhoff appliqué à une famille dénombrable dense de fonctions de $C_c(X)$ prouve que $\mu(Z) = 1$. L'idée est de prendre deux points proches x et gx dans Z et de comparer les moyennes orbitales de φ issues de x et de gx. On écrit

$$u_s g x = D(s) u_{d(s)} x$$

avec $D(s)$ dans B^-. La quantité $d(s)$ est la *dérive du paramétrage* et $D(s)$ la *dérive transverse*. On verra que, lorsque g n'est pas dans B, on peut trouver un

"long" intervalle de temps I pendant lequel $D(s)$ est presque égal à un élément non trivial a de A. On aura alors, en posant $\varphi^a(y) = \varphi(ay)$,

$$\int_X \varphi \, d\mu \simeq \frac{1}{\ell(I)} \int_I \varphi(u_s g x) ds \simeq \frac{1}{\ell(I)} \int_I \varphi^a(u_{d(s)} x) ds \simeq \int_X \varphi^a \, d\mu.$$

Ce qui implique que μ est A-invariant, à moins que g ne soit toujours dans B. Il reste à justifier ces $\simeq$. C'est l'objet de la démonstration que nous détaillons maintenant.

Pour tout $\varepsilon_0 > 0$, on peut trouver une partie compacte $Z_0 \subset Z$ de mesure $\mu(Z_0) \geq 1 - \varepsilon_0$ telle que, pour tout $\varphi \in C_c(X)$, la limite

$$\lim_{t \to \infty} \frac{1}{t} \int_0^t \varphi(u_s x) ds \quad = \quad \int_X \varphi \, d\mu \tag{3}$$

soit uniforme pour x dans Z_0.

En effet, la proposition 8.8 d'Egorov appliquée à une fonction f d'une partie dénombrable dense F de $C_c(X)$ permet de construire des parties compactes Z_φ de mesure $\mu(Z_\varphi) \geq 1 - \varepsilon_\varphi$ telles que la limite (3) soit uniforme pour $x \in Z_\varphi$. Il suffit de prendre $Z_0 = \cap_{\varphi \in F} Z_\varphi$ où les ε_φ sont choisis de sorte que $\sum_{\varphi \in F} \varepsilon_\varphi \leq \varepsilon_0$. En effet, l'ensemble des fonctions $\varphi \in C_c(X)$ pour lesquelles la limite (3) soit uniforme pour $x \in Z_0$ est un fermé de $C_c(X)$.

Distinguons deux cas.

1er cas : *Il existe une suite $g_n \in G$, $g_n \notin B$, $g_n \to e$ telle que $g_n Z_0 \cap Z_0 \neq \emptyset$.* Notons $g_n = \begin{pmatrix} \alpha_n & \beta_n \\ \gamma_n & \delta_n \end{pmatrix}$ et choisissons $x_n \in Z_0$ tel que $g_n x_n \in Z_0$. On peut supposer $\gamma_n > 0$. Un calcul matriciel avec $\lambda_n = \gamma_n^{-1} \to \infty$ donne

$$u_{\lambda_n s} g_n = D_n(s) u_{\lambda_n d_n(s)}$$

où

$$D_n(s) = \begin{pmatrix} \alpha_n + s & 0 \\ \gamma_n & \frac{1}{\alpha_n + s} \end{pmatrix} \longrightarrow D(s) := \begin{pmatrix} 1+s & 0 \\ 0 & \frac{1}{1+s} \end{pmatrix}$$

et

$$\alpha_n(s) = \frac{\beta_n \gamma_n + \delta_n s}{\alpha_n + s} \longrightarrow \alpha(s) := \frac{s}{1+s}.$$

Soient $\varphi \in C_c(X)$ et $a = \begin{pmatrix} 1+t_0 & 0 \\ 0 & \frac{1}{1+t_0} \end{pmatrix} \in A$. On va montrer que $\int_X \varphi \, d\mu = \int_X \varphi^a d\mu$, ce qui prouvera que μ est A-invariante. On peut supposer que $\|\varphi\|_\infty \leq 1$.

Par définition de Z_0, on a, pour tout $t_1 < t_2$, la convergence uniforme pour $x \in Z_0$,

$$\lim_{\lambda \to \infty} \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} \varphi(u_{\lambda s} x) ds = \int_X \varphi \, d\mu.$$

En effet, par simple soustraction pondérée de moyennes sur $[0, t_2]$ et $[0, t_1]$, on peut se ramener à de telles moyennes sur des portions d'orbites. En particulier, pour tout $t_1 < t_2$,

$$\lim_{n\to\infty} \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} \varphi(u_{\lambda_n s} g_n x_n) ds = \int_X \varphi \, d\mu. \tag{4}$$

De la même façon, pour $s_1 < s_2$, qu'on prend égal à $s_1 = d(t_1)$ et $s_2 = d(t_2)$, on a

$$\lim_{n\to\infty} \frac{1}{s_2 - s_1} \int_{s_1}^{s_2} \varphi^a(u_{\lambda_n \sigma} x_n) d\sigma = \int_X \varphi^a \, d\mu. \tag{5}$$

Expliquons tout d'abord dans quel ordre on choisit les paramètres. Soit $\varepsilon > 0$, on peut choisir $t_1 < t_2$ suffisamment proche de t_0 pour que, pour $s \in [t_1, t_2]$, on ait

$$\|\varphi^{D(s)} - \varphi^a\|_\infty \leq \varepsilon \tag{6}$$

et

$$\left| \frac{1}{d'(s)} \frac{s_2 - s_1}{t_2 - t_1} - 1 \right| \leq \varepsilon. \tag{7}$$

On choisit alors n_0 tel que, pour tout $n \geq n_0$ et $s \in [t_1, t_2]$, on ait

$$\|\varphi^{D_n(s)} - \varphi^{D(s)}\|_\infty \leq \varepsilon, \tag{8}$$

$$|t_i - d_n^{-1}(s_i)| \leq \varepsilon(t_2 - t_1) \tag{9}$$

pour $i = 1, 2$ et

$$\left| \frac{s_2 - s_1}{t_2 - t_1} \right| \left| \frac{1}{d_n'(s)} - \frac{1}{d'(s)} \right| \leq \varepsilon. \tag{10}$$

On a alors, pour $n \geq n_0$

$$\left| \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} \varphi(u_{\lambda_n s} g_n x_n) ds - \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} \varphi^a(u_{\lambda_n d_n(s)} x_n) ds \right| \leq 2\varepsilon$$

d'après (6) et (8)

$$\left| \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} \varphi^a(u_{\lambda_n d_n(s)} x_n) ds - \frac{1}{t_2 - t_1} \int_{s_1}^{s_2} \varphi^a(u_{\lambda_n \sigma} x_n) \frac{1}{|d_n'(s)|} d\sigma \right| \leq 2\varepsilon$$

d'après (9), où $\sigma = d_n(s)$

$$\left| \frac{1}{t_2 - t_1} \int_{s_1}^{s_2} \varphi^a(u_{\lambda_n \sigma} x_n) \frac{1}{|d_n'(s)|} d\sigma - \frac{1}{s_2 - s_1} \int_{s_1}^{s_2} \varphi^a(u_{\lambda_n \sigma} x_n) d\sigma \right| \leq 2\varepsilon$$

d'après (7) et (10).

Ces trois majorations avec (4) et (5) donnent

$$\left| \int_X \varphi \, d\mu - \int_X \varphi^a \, d\mu \right| \leq 6\varepsilon.$$

Comme ε est arbitraire, on a $\int_X \varphi \, d\mu = \int_X \varphi^a \, d\mu$.

2ème cas : *Il n'y a pas de suite $g_n \in G$, $g_n \notin B$, $g_n \to e$ avec $g_n Z_0 \cap Z_0 \neq \emptyset$.*

Montrons tout d'abord que μ est portée par une B-orbite. Pour cela, notons D un voisinage de e dans G tel que les éléments $g \in D$, $g \notin B$ vérifient $gZ_0 \cap Z_0 = \emptyset$. Il existe un point $x = g\Gamma \in Z_0$ tel que $\mu(Dx \cap Z_0) > 0$. Cette intersection $Dx \cap Z_0$ est incluse dans l'orbite Bx. Donc $\mu(Bx) > 0$ et par ergodicité, $\mu(Bx) = 1$.

Le groupe $\Delta := B \cap g\Gamma g^{-1}$ est un sous-groupe discret de B et μ est une probabilité U-invariante sur B/Δ. Il est facile de décrire tous les sous-groupes discrets de B. A conjugaison près, on a soit $\Delta \subset A$ ou $\Delta \subset U$. Dans les deux cas, toutes les orbites de U dans B/Δ sont fermées. Comme μ est ergodique, μ est portée par une U-orbite (cf. proposition 8.3). Ce qui termine la démonstration du lemme 12.2. □

Démonstration du lemme 12.3 Remarquons que μ est B-invariante et U-ergodique. On en déduit que μ est A-ergodique. En effet, un élément $\varphi \in L^2(X, \mu)$ qui est A-invariant est forcément U-invariant à cause du lemme 6.6 de Mautner et de l'égalité $\lim_{t \to 0} a_t u_s a_t^{-1} = e$.

Pour $x \in X$ et $\varphi \in C_c(X)$, on note

$$\widetilde{\varphi}(x) = \liminf_{t \to \infty} \frac{1}{t} \int_0^t \varphi(a_{e^s} x) \, ds \quad \text{et} \quad Y = \{x \in X \mid \widetilde{\varphi}(x) = \int_X \varphi \, d\mu\}.$$

D'après le théorème 8.6 de Birkhoff, on a $\mu(Y^c) = 0$. Soit λ une mesure G-invariante sur G/Γ. Montrons que $\lambda(Y^c) = 0$.

Remarquons que, par uniforme continuité de φ, pour tout $u_s^- \in U^-$

$$\lim_{t \to \infty} (\varphi(a_{e^t} u_s^- x) - \varphi(a_{e^t} x)) = \lim_{t \to \infty} (\varphi(u^-_{e^{-2t}s} a_{e^t} x) - \varphi(a_{e^t} x)) = 0.$$

Ce calcul traduit le fait que *les deux géodésiques issues de x et de $u_s^- x$ se rapprochent exponentiellement vite vers $+\infty$*. On dit qu'elles sont sur la même feuille stable du flot géodésique. On en déduit que $\widetilde{\varphi}(u_s^- x) = \widetilde{\varphi}(x)$ puis que $U^- Y = Y$.

Comme la probabilité μ est B-invariante, et que $\mu(Y) = 1$, le théorème de Fubini prouve que, pour μ-presque tout $x \in X$, l'ensemble $B_x = \{b \in B \mid bx \in Y\}$ est de complémentaire négligeable pour la mesure de Lebesgue de B.

La multiplication induit un difféomorphisme entre

$$U^- \times B \text{ et } \{g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G \mid \alpha \neq 0\}.$$

On déduit des trois paragraphes précédents que $\lambda(Y^c) = 0$. C'est-à-dire que $\widetilde{\varphi}(x) = \int_X \varphi \, d\mu$ pour λ-presque tout x.

Montrons que $\lambda(X) < \infty$. Pour cela choisissons $\varphi \geq 0$ tel que $\int_X \varphi \, d\mu = 1$. Le lemme de Fatou donne alors

$$\lambda(X) = \int_X \widetilde{\varphi} \, d\lambda \leq \liminf_{t\to\infty} \int_X \left(\frac{1}{t} \int_0^t \varphi(a_{e^s} x) \, ds \right) d\lambda = \int_X \varphi \, d\lambda < \infty.$$

On peut donc supposer que $\lambda(X) = 1$. Pour conclure, on peut soit reprendre le calcul précédent en remplaçant le lemme de Fatou par le théorème de convergence dominée et les limites inférieures par des limites. On peut aussi remarquer que λ est A-invariante et A-ergodique par le corollaire 6.4 de Howe-Moore. Donc, par le théorème 8.6 de Birkhoff, on a $\widetilde{\varphi}(x) = \int_X \varphi \, d\lambda$ pour λ-presque tout x. On en déduit que $\int_X \varphi \, d\lambda = \int_X \varphi \, d\mu$. C'est-à-dire $\mu = \lambda$. □

12.2 Petites valeurs des formes quadratiques

Dans cette section, on donne une démonstration directe et rapide de la conjecture d'Oppenheim qui fut la première des motivations des travaux de Ratner.

Proposition 12.4 *(Margulis) Soit Q une forme quadratique sur $\mathbb{R}^3$ de signature $(1,2)$ qui n'est pas multiple d'une forme quadratique entière. Alors Q prend des valeurs arbitrairement petites sur $\mathbb{Z}^3 \smallsetminus 0$.*

Cette proposition sera une conséquence de la version faible suivante du théorème topologique de Ratner.

Proposition 12.5 *Soient $G = \mathrm{SL}(3,\mathbb{R})$, $\Gamma = \mathrm{SL}(3,\mathbb{Z})$, $X = G/\Gamma$ et $H = \mathrm{SO}(2,1)$. Alors toute H-orbite bornée $Hx \subset X$ est compacte.*

Remarques - *Bornée* signifie *relativement compacte.*

- La démonstration directe que nous suivons ne se généralise pas pour décrire les adhérences de toutes les H-orbites. Son défaut principal est de ne faire appel a aucun argument de théorie ergodique. En contre-partie, elle est assez élémentaire.

La stratégie de la preuve de la proposition 12.5 consiste à partir d'un fermé U-invariant minimal K de l'adhérence de l'orbite $F = \overline{Hx}$. Par un argument proche de l'argument de dérive de la section 12.1, on montre que K est A-invariant puis que l'image de K par un sous-semigroupe de G reste dans F, semigroupe trop gros pour avoir des orbites bornées dans X.

Démonstration de l'implication Proposition 12.5 $\Longrightarrow$ Proposition 12.4

L'argument qui suit, dû à Raghunathan, n'est pas propre à la dimension 3.

Supposons par l'absurde qu'il existe $\varepsilon > 0$ tel que $Q(\mathbb{Z}^3 \smallsetminus 0)$ ne rencontre pas $]-\varepsilon, \varepsilon[$. Notons x_0 le réseau $\mathbb{Z}^3$, $H = \mathrm{SO}(Q,\mathbb{R})$ et Hx_0 la H-orbite de x_0 dans X. La proposition 12.5 est bien sûr aussi valable pour ce groupe H. Le critère 1.8

de Mahler prouve que cette orbite est relativement compacte. En effet, l'ouvert $\Omega := Q^{-1}(]-\varepsilon,\varepsilon[)$ est un voisinage de 0 qui ne rencontre qu'en 0 les réseaux $\Lambda \in Hx_0$. La proposition 12.5 prouve alors que cette orbite Hx_0 est compacte.

Montrons que cela implique que Q est multiple d'une forme quadratique entière. Ecrivons $Q(x) = \sum a_{i,j}x_ix_j$ avec $a_{i,j} = a_{j,i}$.

On peut supposer que l'un des coefficients $a_{i,j}$ est égal à 1. Montrons que Q est alors à coefficients dans $\mathbb{Q}$. Soit $\sigma \in \mathrm{Gal}(\mathbb{C}|\mathbb{Q})$ et $Q^\sigma(x) = \sum a^\sigma_{i,j}x_ix_j$. Il suffit de montrer que $Q = Q^\sigma$. Remarquons que le groupe $\Gamma \cap H$ est un réseau cocompact de H. Par le théorème 7.1 de densité de Borel, il est donc Zariski dense dans H. Comme on a l'inclusion $\Gamma \cap H \subset \mathrm{SO}(Q^\sigma, \mathbb{C})$, on en déduit que $H \subset \mathrm{SO}(Q^\sigma, \mathbb{C})$. Soit $\mu \in \mathbb{C}$ tel que $Q^\sigma - \mu Q$ est dégénérée. Le groupe H préserve donc le noyau de $Q^\sigma - \mu Q$. L'irréductibilité de l'action de H sur $\mathbb{C}^3$ prouve que $Q^\sigma = Q$. Forcément $\mu = 1$ et $Q^\sigma = Q$. □

Le lemme suivant est basé sur l'aspect polynomial des flots unipotents. Cet argument nous est maintenant bien familier. Il jouera le rôle de l'argument de dérive de la section 12.1.

Lemme 12.6 *Soient E un $\mathbb{R}$-espace vectoriel de dimension $d < \infty$, $U = \{u_s \mid s \in \mathbb{R}\}$ un groupe à un paramètre de transformations unipotentes et F l'ensemble des points fixes de U dans E. Soient D une partie de $E \smallsetminus F$ et v_0 un point de $\overline{D} \cap F$. Alors $\overline{UD} \cap F$ contient un chemin polynomial non constant passant par v_0.*

Démonstration du lemme 12.6 Soient v_n une suite de points de D tels que $\lim_{n\to\infty} v_n = v_n$. On choisit $\lambda_n > 0$ tels que

$$\sup_{s\in[-1,1]} \|u_{\lambda_n s}v_n - v_n\| = 1.$$

C'est possible car l'application $s \mapsto u_s v_n$ est polynomiale non constante de degré borné par d.

En outre, on a $\lim_{n\to\infty} \lambda_n = \infty$ car v_0 est un point fixe de U. La suite des polynômes $\varphi_n : s \mapsto u_{\lambda_n s}v_n$ est bornée sur $[-1,1]$. Quitte à extraire, on peut supposer qu'elle converge uniformément sur $[-1,1]$ vers un polynôme φ. Ce polynôme est non constant car $\varphi(0) = 0$ et

$$\sup_{s\in[-1,1]} \|\varphi(s) - v_0\| = 1.$$

Par construction, on a $\varphi(\mathbb{R}) \subset \overline{UD}$. En outre, φ prend ses valeurs dans F car, pour $u_t \in U$, on a

$$u_t\varphi(s) = \lim_{n\to\infty} u_t\varphi_n(s) = \lim_{n\to\infty} \varphi_n(s + t/\lambda_n) = \varphi(s)$$

par uniforme convergence. □

Certains sous-groupes à un paramètre de G vont jouer un rôle important dans la démonstration. Fixons les notations : on peut supposer que la forme quadratique s'écrit, pour $v = (x_1, x_2, x_3) \in \mathbb{R}^3$, $Q(v) = x_2^2 - 2x_1x_3$. Le groupe H contient alors les deux groupes

$$A = \{a_t := \begin{pmatrix} e^t & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e^{-t} \end{pmatrix} \mid t \in \mathbb{R}\} \quad , \quad U = \{u_s := \begin{pmatrix} 1 & s & s^2/2 \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix} \mid s \in \mathbb{R}\}.$$

Notons $V = \{v_s := \begin{pmatrix} 1 & 0 & s \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid s \in \mathbb{R}\}$. Le groupe V n'est pas inclus dans H. On vérifie facilement que U et V commutent, que A normalise U et V, que les produits $B := AU$ et $W := UV$ sont des groupes et que le normalisateur de U est le groupe $N_G(U) = AUV$. On notera $V^{\pm} := \{v_s \in V \mid \pm s > 0\}$.

Les gros sous-semi groupes dont nous parlions ci-dessus sont $AUV^{\pm}$.

Lemme 12.7 *Pour tout $y \in X$, les orbites AUV^+y et AUV^-y ne sont pas bornées dans X.*

Démonstration Le point $y \in X$ est un réseau de $\mathbb{R}^3$. On peut choisir un point $p = (x_1, x_2, x_3)$ dans ce réseau tel que $x_3 \neq 0$ et $\pm(x_2^2 - 2x_1x_3) > 0$. On pose

$$g_t = a_t \, u_{-x_2/x_3} \, v_{(x_2^2 - 2x_1x_3)/2x_3^2} \in AUV^{\pm}$$

et on calcule $g_t p = (0, 0, e^{-t}x_3) \to 0$ quand $t \to \infty$. Le critère 1.8 de Mahler prouve donc que $AUV^{\pm}y$ n'est pas relativement compact. □

Démonstration de la proposition 12.5 Rappelons que, par un argument à la Zorn, tout compact U-invariant non vide de X contient un compact U-invariant minimal. Soit $F = \overline{Hx}$. On suppose par l'absurde que $F \neq Hx$.

On va appliquer deux fois le lemme 12.6. La première fois via le lemme 12.8. La deuxième fois via le lemme 12.9.

Soit K un compact U-invariant minimal de F. D'après le lemme 12.8, ce compact K est aussi AU-invariant. D'après le lemme 12.8, on a soit $AUV^+(K) \subset F$ ou $AUV^-(K) \subset F$. Mais, d'après le lemme 12.7, les ensembles $AUV^{\pm}(K)$ ne sont pas bornés dans X. Contradiction. □

Dans cette démonstration, on a utilisé les deux lemmes suivants.

Lemme 12.8 *Soit K un compact U-invariant minimal du compact $F = \overline{Hx}$. Alors K est AU-invariant.*

Démonstration du lemme 12.8 Remarquons tout d'abord que K n'est pas une U-orbite compacte. Sinon, on pourrait trouver y dans K et $s \neq 0$ tels que

$u_s y = y$. On aurait alors $u_{e^{-t}s} a_t y = a_t y$. Or les points de X ont un stabilisateur discret dans G et $\lim_{t\to\infty} u_{e^{-t}s} = e$. Donc $a_t y$ tend vers l'infini, ce qui contredit la compacité de F.

L'ensemble $M := \{g \in G \mid gK \cap K \neq \emptyset\}$ vérifie les trois propriétés suivantes.
M est U-invariant à droite et à gauche.
M est fermé.
Il existe une suite g_n dans $M \setminus U$ convergeant vers e.
Pour vérifier cette dernière affirmation, on choisit un point $y \in K$. Par minimalité de K, il existe une suite $u_{s_n} \in U$ avec $s_n \to \infty$ telle que $u_{s_n} y \to y$. On écrit alors $y = g_n u_{s_n} y$ avec $g_n \to e$.

Pour pouvoir appliquer le lemme 12.6 à l'image D de la suite g_n dans G/U, remarquons qu'il existe une représentation linéaire de G dans un espace vectoriel E de dimension finie et un point $v_0 \in E$ tel que $Gv_0 \simeq G/U$. Cela résulte du résultat général 4.7 de Chevalley. On peut être aussi très explicite en prenant

$$E = \{ \text{ formes quadratiques sur } \mathbb{R}^3\} \times \mathbb{R}^3 \text{ et } v_0 = (Q, (1,0,0)).$$

L'ensemble des points fixes de U dans G/U est égal à $N_G(U)/U \simeq AV$.

Le lemme 12.6 et les trois propriétés ci-dessus prouvent que l'on est dans l'un des deux cas suivants :
1$^{\text{er}}$ cas La suite g_n est dans AVU pour $n \gg 0$.
2$^{\text{ème}}$ cas Il existe une application continue non constante $\varphi : \mathbb{R} \to AV \cap M$.

Notons L la composante connexe du groupe engendré par $M \cap AV$. Dans les deux cas, c'est un sous-groupe de Lie connexe non trivial de AV. Montrons que K est L-invariant. Pour tout g dans dans $M \cap AV$, le fermé $gK \cap K$est U-invariant et non vide et, par minimalité de K, on a $gK = K$. Donc K est bien L-invariant.

Pour conclure, il reste à montrer que L contient A.

Supposons par l'absurde que ce ne soit pas vrai. On est alors dans l'un des deux cas suivants : $L = V$ ou $v_{s_0} A v_{-s_0}$ avec $s \neq 0$. Dans ce deuxième cas, on a $V^+ \subset AL$, car $a_t v_{s_0} a^{-t} v_{-s_0} = a_{(e^{2t}-1)s_0}$. Dans les deux cas, pour tout $y \in K$, on a donc $AUV^+ y \subset HLy \subset F$. Ce qui contredit le lemme 12.7. □

Lemme 12.9 *On suppose que l'orbite Hx n'est pas compacte. Soit K un compact AU-invariant minimal du compact $F = \overline{Hx}$.*

Alors on a soit $AUV^+(K) \subset F$ ou $AUV^-(K) \subset F$.

Démonstration du lemme 12.9 Le raisonnement est très proche de celui du lemme 12.8.

Comme H/AU est compact et que l'orbite Hx n'est pas compacte, K ne peut pas être inclus dans Hx.

L'ensemble $M := \{g \in G \mid gF \cap K \neq \emptyset\}$ vérifie alors les trois propriétés suivantes.
M est H-invariant à droite et AU-invariant à gauche.
M est fermé.
Il existe une suite g_n dans $M \setminus H$ convergeant vers e.

Pour vérifier cette dernière affirmation, on prend un point $y \in K$ hors de l'orbite Hx. On a alors une suite $h_n \in H$ telle que $h_n x \to y$. On écrit alors $y = g_n h_n x$ avec $g_n \to e$.

Pour appliquer le lemme 12.6 à l'image D de la suite g_n dans G/H, on remarque de nouveau à l'aide du corollaire 4.7 qu'il existe une représentation linéaire de G dans un espace vectoriel E de dimension finie et un point $v_0 \in E$ tel que $Gv_0 \simeq G/H$. On peut être aussi explicite que dans le lemme 12.8 en prenant

$$E = \{ \text{ formes quadratiques sur } \mathbb{R}^3 \} \text{ et } v_0 = Q.$$

Comme tous les sous-groupes unipotents de H sont conjugués, l'ensemble des points fixes de U dans G/U est égal à $N_G(U)H/H = VH/H \simeq V$.

Le lemme 12.6 et les trois propriétés ci-dessus prouvent que l'on est dans l'un des deux cas suivants :

1$^{\text{er}}$ cas La suite g_n est dans VH pour $n \gg 0$.

2$^{\text{ème}}$ cas Il existe une application continue non constante $\varphi : \mathbb{R} \to V \cap M$.

Dans les deux cas, on a $M \cap V \neq e$. Comme M est invariant par conjugaison par A, on en déduit que $V^+ \subset M$ ou $V^- \subset M$.

Supposons par exemple $V^- \subset M$. Pour tout $v \in V^-$, l'intersection $vF \cap K$ est non vide et U-invariante. Le lemme 12.8 assure que K est un fermé U-invariant minimal. On a donc $K \subset vF$, puis $V^+K \subset F$ et enfin $AUV^+K \subset AUF = F$. $\square$

13 Récurrence des groupes unipotents

Le but de ce chapitre est de montrer des propriétés de récurrence pour les flots unipotents sur les espaces homogènes X de volume fini.

A cause du théorème d'arithméticité de Margulis le cas crucial est celui où $X = SL(d,\mathbb{R})/SL(d,\mathbb{Z})$ est l'espace des réseaux de volume 1 dans $\mathbb{R}^d$. Ce que nous supposerons dans ce chapitre.

Notons alors $t \to u_t = e^{tN}$ un groupe à un paramètre d'éléments unipotents. Le but de cette section est le théorème suivant. On note $|I|$ la mesure de Lebesgue d'une partie I de $\mathbb{R}$.

Théorème 13.1 (Dani, Margulis) *Soit $X = SL(d,\mathbb{R})/SL(d,\mathbb{Z})$. Pour tout $\varepsilon > 0$, $x \in X$, il existe un compact $K = K_x \subset X$ tel que, pour tout $T \geq 0$*

$$|\{t \in [0,T] \mid u_t x \in K\}| \geq (1-\varepsilon)T.$$

On notera l'analogie entre ce théorème 13.1 et le lemme 1.4 de récurrence pour les marches aléatoires qui s'applique à X.

En outre, le compact K_x peut être choisi uniforme pour tout x dans un compact K' de X. Ce théorème affirme donc que les orbites du flot u_t sur X passent la plus grande partie de leur temps à distance finie.

13.1 Le cas $d = 2$

Dans le cas $d = 2$, la démonstration du théorème 13.1 est très courte :

On note b_ε la boule de rayon ε dans $\mathbb{R}^2$. Le critère de Mahler assure que l'ensemble des réseaux $\Delta \in X$ qui ne rencontrent b_ε qu'en 0 est un compact. Choisissons une boule b_α avec $\alpha \leq 1$ qui ne rencontre le réseau de départ $\Delta = x$ qu'en 0.

Pour chaque paire $\pm v \in \Delta$ de vecteurs primitifs, le vecteurs $u_t v$ se déplace à vitesse constante. Donc dans l'intervalle de temps I_v qu'il a passé dans b_α la proportion de temps qu'il a passé dans une boule beaucoup plus petite $b_{\alpha\varepsilon/2}$ est au plus ε.

Ces intervalles I_v sont disjoints car, comme $u_t\Delta$ est de volume 1, la boule b_α contient à chaque instant t au plus une paire de points $\pm u_t v$ avec $v \in \Delta$ primitif. Donc la proportion du temps entre 0 et T pendant lequel $u_t\Delta$ avait un point dans cette boule $b_{\alpha\varepsilon/2}$ est au plus ε. C'est ce que l'on voulait. □

13.2 Préliminaires sur les réseaux

Nous aurons besoin d'une version plus maniable du critère 1.8 de compacité de Mahler

Munissons $\mathbb{R}^d$ d'une norme euclidienne $\|.\|$. Rappelons que, pour Δ réseau de $\mathbb{R}^d$, un sous-espace Δ-rationnel $L \subset \mathbb{R}^d$ est un sous-espace tel que $\Delta \cap L$ est un réseau de L. On note alors

$$d_\Delta(L) := \mathrm{covol}_L(\Delta \cap L).$$

Par exemple $d_\Delta := d_\Delta(\mathbb{R}^d)$ est le covolume de Δ. Notons $S(\Delta)$ l'ensemble des sous-espaces Δ-rationnels. On appelle *drapeau Δ-rationnel de longueur ℓ*, un ensemble F de ℓ sous-espaces Δ-rationnels non triviaux qui est totalement ordonné. On pourrait noter un tel drapeau F sous la forme

$$F : \ 0 \subsetneq L_{i_1} \subsetneq \cdots \subsetneq L_{i_\ell} \subsetneq \mathbb{R}^d.$$

Nous ne le ferons pas car, au cours de la démonstration, les sous-espaces L_i n'apparaitrons pas forcément dans l'ordre croissant. On note alors $S_F = S_F(\Delta)$ l'ensemble des sous-espaces Δ-rationnels propres L tels que $F \cup \{L\}$ est un drapeau Δ-rationnel de longueur $k+1$. Autrement dit,

$$S_F := \{L \in S \ , \ 0 \subsetneq L \subsetneq \mathbb{R}^d \mid \text{pour tout } M \in F, \text{ on a } M \subsetneq L \text{ ou } L \subsetneq M \ \}.$$

On dit que le drapeau F est *complet* si $\ell = d-1$. Dans ce cas $S_F(\Delta)$ est vide.

Proposition 13.2 (Mahler) *Soient $X = SL(d,\mathbb{R})/SL(d,\mathbb{Z})$ et $Y \subset X$. Les assertions suivantes sont équivalentes.*
(i) Y est relativement compact.
(ii) Il existe $a > 0$ tel que, pour tout $\Delta \in Y$, $\inf_{v \in \Delta - 0} \|v\| \geq a$.
(iii) Il existe $b > 0$ tel que, pour tout $\Delta \in Y$, $\inf_{L \in S(\Delta)} d_\Delta(L) \geq b$.
(iv) Il existe $\beta > \alpha > 0$ tels que, pour tout $\Delta \in Y$, il existe un drapeau Δ-rationnel complet F tels que $\alpha \leq d_\Delta(L) \leq \beta$, pour tout $L \in F$.

Rappelons tout d'abord quelques affirmations que nous avons déjà utilisées dans la section 1.4. On note c_d la constante $c_d = 2(1/v_d)^{\frac{1}{d}}$ où $v_d = \frac{\pi^{\frac{d}{2}}}{\frac{d}{2}\Gamma(\frac{d}{2})}$ est le volume de la boule euclidienne dans $\mathbb{R}^d$. La valeur précise de cette constante ne jouera pas de rôle dans la démonstration. On remarque juste que $c_d \geq 1$ et que c_d croît avec d.

Lemme 13.3 *a) Tout réseau $\Delta \subset \mathbb{R}^d$ contient un vecteur v avec $0 < \|v\| \leq c_d\, d_\Delta^{\frac{1}{d}}$.*
b) Pour tout $C > 0$, l'ensemble $\{L \in S(\Delta) \mid d_\Delta(L) \leq C\}$ est fini.
c) L'application $X \to]0,\infty[\,; \Delta \mapsto \min_{L \in S(\Delta)} d_\Delta(L)$ est continue.

Démonstration C'est le lemme 1.10 de Minkowski et le lemme 1.12. □

Le lemme suivant permet de compléter les drapeaux Δ-rationnels incomplets en des drapeaux dont on contrôle les covolumes.

Lemme 13.4 *Soient $\beta \geq 1$, $\Delta \in X$ et F un drapeau Δ-rationnel incomplet tel que, pour tout $L \in F$, $d_\Delta(L) \leq \beta$.*

Alors il existe $M \in S_F(\Delta)$ tel que $d_\Delta(M) \leq c_d\beta$.

Démonstration Comme le drapeau F est incomplet, on peut trouver deux sous-espaces Δ-rationnels successifs $L_1 \subset L_2$ de dimension $d_1 < d_2$ avec $\delta := d_2 - d_1 \geq 2$ avec $L_i \in F \cup \{0, \mathbb{R}^d\}$. En appliquant le lemme 13.3.a de Minkowski à l'image de $L_2 \cap \Delta$ dans L_2/L_1, on peut trouver un vecteur $v \in L_2 \smallsetminus L_1$ dont l'image $\overline{v}$ dans L_2/L_1 est de norme au plus

$$\|\overline{v}\| \leq c_d(d_\Delta(L_2)/d_\Delta(L_1))^{\frac{1}{\delta}}.$$

Le sous-espace $M = L_1 \oplus \mathbb{R}v$ est alors dans $S_F(\Delta)$ et vérifie

$$d_\Delta(M) \leq \|\overline{v}\| d_\Delta(L_1) \leq c_d d_\Delta(L_1)^{1-\frac{1}{\delta}} d_\Delta(L_2)^{\frac{1}{\delta}} \leq c_d\beta.$$

C'est la majoration cherchée. □

Démonstration de la proposition 13.2 $(i) \iff (ii)$ C'est la proposition 1.8.

$(ii) \implies (iii)$ Cela résulte du lemme 13.3.c. En effet, une fonction continue strictement positive sur un compact est minorée par une constante strictement positive.

$(iii) \implies (iv)$ La minoration est claire. Pour la majoration, on peut prendre pour constante $\beta = (c_d)^d$. Pour cela, on construit le drapeau F par récurrence à l'aide du lemme 13.4. On perd au plus un facteur c_d à chaque étape.

$(iv) \implies (ii)$ On peut supposer $0 < \alpha < 1 < \beta$. Soit v un vecteur non nul dans un des réseaux $\Delta \in Y$. Notons $L_1 \subsetneq \cdots \subsetneq L_{d-1}$ le drapeau Δ-rationnel complet F donné par la condition (iv) et posons $L_0 = 0$ et $L_d = \mathbb{R}^d$. Soit i l'entier tel que $v \in L_i - L_{i-1}$. On a alors

$$\|v\| \geq d(L_i)/d(L_{i-1}) \geq \alpha/\beta.$$

C'est la minoration cherchée. □

13.3 Autres lemmes préliminaires

Voici deux lemmes élémentaires dont nous aurons besoin, l'un sur les polynômes en une variable, l'autre sur les recouvrements d'un intervalle.

Notons P^m l'espace des polynômes sur $\mathbb{R}$ de degré au plus m. Le lemme suivant exprime qu'un polynôme ne peut pas être petit trop longtemps et ce avec un contrôle uniforme qui ne dépend que du degré du polynôme.

Lemme 13.5 *Pour tout $\varepsilon > 0$, il existe $M_\varepsilon > 0$ tel que pour tout intervalle I et tout polynôme $p \in P^m$, on a* $\left|\{t \in I \mid |p(t)| \leq \frac{1}{M_\varepsilon} \sup_I |p| \}\right| \leq \varepsilon |I|$.

Démonstration Sinon il existerait $m \geq 0$, $\varepsilon > 0$ et une suite de polynômes $p_n \in P^m$ telle que $\sup_{[0,1]} |p_n| = 1$ et $\left|\{t \in [0,1] \mid |p_n(t)| \leq \frac{1}{n} \}\right| \leq \varepsilon$. Cet ensemble est une réunion d'au plus $2m$ intervalles. Par compacité de la sphère unité de P^m, cette suite p_n une valeur d'adhérence $p_\infty \in P^m$. Ce polynôme p_∞ est non nul, mais l'ensemble de ses racines est de mesure au moins ε. Contradiction. □

Lemme 13.6 *Soit $I = \cup_{\alpha \in A} I_\alpha$ un recouvrement d'un intervalle compact $I \subset \mathbb{R}$ par des intervalles I_α ouverts dans I. Alors, il existe un sous-recouvrement $I = \cup_{\alpha \in A'} I_\alpha$ de chevauchement au plus 2.*

Le *chevauchement* est le nombre maximum d'intervalles I_α dont l'intersection est d'intérieur non vide.

Démonstration On extrait tout d'abord un recouvrement fini. On prend alors un intervalle $I_{\alpha_0} = [x_0, y_0[$ contenant l'extrémité gauche de I avec y_0 maximum. Puis un intervalle $I_{\alpha_1} =]x_1, y_1[$ contenant y_0 avec y_1 maximum. Et on continue. □

Pour montrer le théorème 13.1 de récurrence, on partira d'un point $x = \Delta$ dans un compact $K' \subset X$, ce qui nous donne une constante b par le critère (iii) de Mahler. On veut contrôler, pour $L \in S(\Delta)$, le covolume dans L de $u_t(\Delta \cap L)$. On introduit donc le polynôme sur $\mathbb{R}$

$$p_L : t \to d_{u_t \Delta}(u_t L)^2.$$

C'est un polynôme de degré au plus $2d^2$ car on a l'égalité $p_L(t) = \|u_t e_1 \wedge \cdots \wedge u_t e_i\|$ où $e_1, \ldots, e_i$ est une base de $\Delta \cap L$.

13.4 La récurrence qui prouve la récurrence

> Pour décrire le compact K dans lequel $u_t \Delta$ passe plus de $1 - \varepsilon$ de son temps, on va utiliser le critère (iv) de Mahler. Il s'agira donc de construire à chaque instant t convenable un drapeau complet F de sous-espaces Δ-rationnels L_i dont on contrôlera les covolumes carrés $p_{L_i}(t)$.

On procèdera par récurrence, en ajoutant à chaque étape, pour tout temps t un nouveau sous-espace à un drapeau Δ-rationnel de longueur ℓ. Le nombre d'étape dans cette récurrence est donc $d - 1$. La proposition technique qui met en place cette récurrence est la suivante.

Proposition 13.7 *Soit $\beta > 1 > \alpha > 0$ et posons $\beta' = c_d\beta$ et $\alpha' = \alpha$. Soient I un intervalle compact et F un drapeau Δ-rationnel incomplet tel que*

$$\begin{array}{lrcll} (a) & \inf\limits_{L\in S_F}(\sup\limits_{t\in I} p_L(t)) & \geq & \alpha & \\ (b) & \sup\limits_{t\in I}(\inf\limits_{L\in S_F} p_L(t)) & < & \beta & \\ (c) & \sup\limits_{t\in I} p_L(t) & < & \beta & \forall L \in F. \end{array}$$

Il existe un recouvrement fini de chevauchement au plus 2 de I par des intervalles compacts I' tels que sur chaque I', il existe un drapeau $F' = F \cup \{L_0\}$ avec $L_0 \in S_F$ tel que

$$\begin{array}{lrcll} (a') & \inf\limits_{L\in S_{F'}}(\sup\limits_{t\in I'} p_L(t)) & \geq & \alpha' & \\ (b') & \sup\limits_{t\in I'}(\inf\limits_{L\in S_{F'}} p_L(t)) & < & \beta' & \\ (c') & \sup\limits_{t\in I'} p_L(t) & < & \beta' & \forall L \in F' \\ (d') & \sup\limits_{t\in I'} p_{L_0}(t) & \geq & \alpha'. & \end{array}$$

Remarque On ne peut pas en général réduire la taille des intervalles I' de sorte qu'ils soient d'intérieur disjoint sans perdre les conditions (a') et (d').

Démonstration de la proposition 13.7 Pour tout $t_0 \in I$, on doit fournir un intervalle I' contenant t_0 dans son intérieur et un sous-espace $L_0 \in S_F$ vérifiant (a'), (b'), (c') et (d'). On extraira alors le sous-recouvrement de chevauchement au plus 2 à l'aide du lemme 13.6. On distingue deux cas.

1er cas : Il existe $L \in S_F$ tel que $p_L(t_0) \leq \alpha$.

D'après le lemme 13.3, il n'y a qu'un nombre fini de tels sous-espace Δ rationnels L. On choisit donc un intervalle compact I' de longueur maximal dont l'intérieur contient t_0, pour lequel il existe $L_0 \in S_F$ tel que $\sup\limits_{t\in I'} p_{L_0}(t) \leq \alpha$.

Par la condition (a) et la maximalité de I', cette inégalité est une égalité $\sup\limits_{t\in I'} p_{L_0}(t) = \alpha$ et on a, $\sup\limits_{t\in I'} p_L(t) \geq \alpha$, pour tout $L \in S_F$.

La condition (a') est donc vérifiée dès que $\alpha' \leq \alpha$.

Par la condition (c) et le lemme 13.4, la condition (b') est vraie dès que $\beta' \geq c_d^2\beta$.

Par (c) et l'égalité $\sup\limits_{t\in I'} p_{L_0}(t) = \alpha$, la condition (c') est vraie dès que $\beta' \geq \beta$.

La même égalité prouve que la condition (d') est valide dès que $\alpha' \leq \alpha$.

2ème cas : Pour tout $L \in S_F$, on a $p_L(t_0) \geq \alpha$.

On choisit, grâce à la condition (b) un sous-espace $L_0 \in S_F$ tel que $p_{L_0}(t_0) < \beta$. On choisit alors un intervalle compact I' dont l'intérieur contient t_0 sur lequel on a encore $\sup\limits_{t\in I'} p_{L_0}(t) < \beta$

Dans ce cas, la condition (a') est automatique dès que $\alpha' \leq \alpha$.

Par la condition (c) et le lemme 13.4, la condition (b') est vraie dès que $\beta' \geq c_d^2\beta$. Par (c) et le choix ci-dessus, la condition (c') est aussi vérifiée dès que $\beta' \geq \beta$. La minoration $p_{L_0}(t_0) \geq \alpha$ garantit la condition (d') dès que $\alpha' \leq \alpha$. □

Démonstration du théorème 13.1 On applique $d-1$ fois la proposition 13.7.

On commence la première étape avec $I = [0,T]$ et $F = \emptyset$. Pour valider la condition (a), il suffit de la comprendre en $t = 0$. D'après la condition (iii) du critère 13.2 de Mahler, la condition (a) est vraie avec une constante $\alpha = \alpha_0 = b^2$ uniforme pour Δ dans un compact K' de X. Pour valider la condition (b), on applique le lemme 13.3 de Minkowski : chaque réseau $u_t\Delta$ contient un vecteur non nul de norme au plus c_d. La condition (b) est donc satisfaite avec $\beta = \beta_0 = c_d^2$. Noter qu'à ce stade, la condition (c) est vide.

On construit ensuite successivement $d-1$ couples de réels $\alpha_k = \alpha_{k-1}$ et $\beta_k = (c_d)^2\beta_{k-1}$ ainsi que $d-1$ recouvrement de $[0,T]$ par des intervalles compacts. Le premier ayant un chevauchement au plus 2, le deuxième un chevauchement au plus 4,... , le dernier un chevauchement au plus 2^{d-1}. Le chevauchement total est donc au plus 2^d. On a donc $\alpha_{d-1} = b^2$ et $\beta_{d-1} = (c_d)^{2d}$. Posons $\varepsilon_0 = 2^{-d}\varepsilon$. Par le lemme 13.5 et les conditions (d'), dans chacun des intervalles I', on a pour le sous-espace L_0 correspondant

$$|\{t \in I' \mid p_{L_0}(t) < \frac{\alpha_{d-1}}{M_{\varepsilon_0}}\}| \quad \leq \quad \varepsilon_0|I'|.$$

On retire de chacun de ces intervalles I' les points t tels que $p_{L_0}(t) < \frac{\alpha_{d-1}}{M_{\varepsilon_0}}$. L'ensemble J de tous ces points t est de mesure au plus

$$2^d\varepsilon_0 T = \varepsilon T.$$

Les réseaux $u_t\Delta$ correspondant aux temps t hors de J contiennent un drapeau complet de sous-espaces Δ-rationnel dont les covolumes carrés sont dans l'intervalle $[\frac{\alpha_{d-1}}{M_{\varepsilon_0}}, \beta_{d-1}]$. On applique la condition (iv) du critère 13.2 de Mahler avec les constantes $\alpha = b/M_{\varepsilon_0}^{\frac{1}{2}}$ et $\beta = (c_d)^d$. Ces réseaux $u_t\Delta$ pour $t \notin J$ sont donc dans un compact K qui ne dépend que de ε et de b. □

Références

[1] N.A'Campo, M.Burger - Réseaux arithmétiques et commensurateur d'après G. A. Margulis, Invent. Math. 116 (1994) p.1-25.

[2] R.Alperin - An elementary account of Selberg's lemma, Ens. Math.33 (1987) p.269-273.

[3] Y.Benoist - Pavages du plan, in Journées X-UPS 2001,Editions de l'Ecole Polytechnique.

[4] Y.Benoist - Five lectures on lattices in semisimple Lie groups, Un cours à l'école d'été de Grenoble 2004***.

[5] A.Borel - Compact Clifford-Klein forms of symmetric spaces, Topology 2 (1963) p.111-122.

[6] A.Borel - Introduction aux groupes arithmétiques, Hermann (1969).

[7] A.Borel - Linear algebraic groups, GTM 126 Springer (1991).

[8] A.Borel, G.Harder - Existence of discrete cocompact subgroups of reductive groups over local fields, J. Reine Angw. Math. 298 (1978) p.53-64.

[9] N.Bourbaki - Groupes et algèbres de Lie, Paris (1975).

[10] A.Eskin, G.Margulis - Recurrence properties of random walks on finite volume homogeneous spaces, ***

[11] M.Gromov, P.Pansu - Rigidity of lattices : an introduction, Lect. Notes in Math. 1504 (1991) p.39-137.

[12] P.de la Harpe, A.Valette - La propriété T de Kazhdan, Asterisque (1989).

[13] S.Helgason - Differential geometry, Lie groups and symmetric spaces, Acad. Press (1978).

[14] S.Helgason - Groups and geometric analysis, Acad. Press (1984).

[15] R.Howe, E.Tan - Non-abelian harmonic analysis, Universitext Springer (1992).

[16] G.Margulis - Discrete subgroups of semisimple Lie groups, Springer Ergebnisse (1991).

[17] G.Margulis - Random walks on the spaces of lattices and the finiteness of covolumes of arithmetic subgroups, in Algebraic groups and arithmetic, Tata Inst. Fund. Res. Stud. Math. 17 (2004) p.409-425.

[18] B.Maskit- Kleinian groups, Springer GTM (1988).

[19] G.Mostow - Quasiconformal mappings in n-space and the rigidity of hyperbolic space forms, Publ. Math. IHES 34 (1967) p.53-107.

[20] V.Platonov, A.Rapinchuk - Algebraic groups and number theory, Ac. Press (1994).

[21] M.Raghunathan - Discrete subgroups of Lie groups, Springer(1972).

[22] P.Samuel - Theorie algébrique des nombres, Hermann Paris (1971).

[23] A.Selberg - On discontinuous groups in higher dimensional symmetric spaces, in Contribution to function theory, Tata (1960) p.147-164.

[24] J-P. Serre - Cohomologie des groupes discrets, Ann. of Math. Studies 70,p.77-169.

[25] J.Tits - Sur la classification des groupes algébriques semi-simples, C. R. Acad. Sci. 249 (1959) p.1438-1440.

[26] J.Tits - Structure des groupes de Weyl, Séminaire Bourbaki 288 (1965).

[27] E.Vinberg, V.Gorbatsevich, O.Shvartsman - Discrete subgroups of Lie groups, in Encyclopedia of Math. Sc. 21 Springer (2000).

[28] A.Weil - Algebras with involutions and the classical groups, J. Indian Math. Soc. 24 (1961) p.589-623.

[29] A.Weil - Basic number theory, Springer (1973).

[30] D.Witte-Morris - Introduction to arithmetic groups, preprint (2003).

[31] R.Zimmer - Ergodic theory and semisimple groups, Birkhauser (1984).

Univ. Paris-Sud & CNRS yves.benoist@math.u-psud.fr www.dma.ens.fr/~benoist