Enseign. Math. (2) (Online first)
DOI 10.4171/LEM/1078
© 2024 Fondation L'Enseignement Mathématique
Published by EMS Press

Trou spectral dans les groupes simples

Weikun He and Nicolas de Saxcé

Résumé. Nous montrons la propriété du trou spectral pour la famille des graphes de Cayley obtenus par réduction modulo q d'un sous-groupe de $\mathrm{SL}_d(\mathbb{Z})$ dont l'adhérence de Zariski est un groupe algébrique absolument simple.

Mathematics Subject Classification (2020). Primary 20G30; Secondary 11B75, 11L07, 37A44.

Keywords. Arithmetic groups, expander graphs, strong approximation, random walks.

1. Introduction

Dans $\mathrm{SL}_d(\mathbb{Z})$, on considère un sous-groupe Γ, dont on note Ω l'adhérence dans le groupe profini $\mathrm{SL}_d(\widehat{\mathbb{Z}})$ des matrices de déterminant 1 à coefficients dans l'anneau profini $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/q\mathbb{Z}$. Le groupe Ω est un groupe topologique compact, que l'on munit naturellement de sa probabilité de Haar, notée m_Ω. On s'intéresse à l'action de Γ sur l'espace $L^2(\Omega)$ définie par

$$\forall g \in \Gamma,\ \forall f \in L^2(\Omega),\ \forall x \in \Omega, \quad T_g f(x) = f(g^{-1}x). \tag{1.1}$$

Comme Γ est dense dans Ω, toute fonction Γ-invariante dans $L^2(\Omega)$ est constante ; on dit que l'action $\Gamma \curvearrowright \Omega$ est *ergodique*. De manière équivalente, dans l'espace

$$L^2_0(\Omega) = \left\{ \xi \in L^2(\Omega) \mid \int_\Omega \xi \, \mathrm{d}m_\Omega = 0 \right\},$$

le groupe Γ n'a pas de vecteur invariant non nul. Nous dirons que l'action $\Gamma \curvearrowright \Omega$ a un *trou spectral* si Γ n'a pas de vecteur *presque invariant* dans $L^2_0(\Omega)$, i.e., s'il existe une constante $\varepsilon > 0$ et une partie finie $S \subset \Gamma$ tels que

$$\forall f \in L^2_0(\Omega),\ \exists g \in S, \quad \|T_g f - f\|_2 \geq \varepsilon \|f\|_2.$$

Cette propriété implique bien sûr l'ergodicité de l'action, mais est en fait strictement plus forte. Le but principal de cet article est de relier la propriété *analytique* du trou

spectral aux propriétés *algébriques* de l'adhérence de Zariski de Γ dans SL_d. Dans la suite, nous dirons qu'un groupe algébrique G est *simple* si sa composante neutre G^0 est non commutative et ne contient aucun sous-groupe algébrique distingué connexe non trivial ; cela équivaut à dire que l'action adjointe de G^0 sur son algèbre de Lie est non triviale et irréductible sur $\mathbb{C}$. Nous démontrerons le théorème suivant.

Théorème 1 (Propriété du trou spectral). *Soit Γ un sous-groupe de $\mathrm{SL}_d(\mathbb{Z})$ et Ω son adhérence dans $\mathrm{SL}_d(\widehat{\mathbb{Z}})$. Supposons que l'adhérence de Zariski de Γ soit un groupe algébrique simple, alors l'action de Γ sur Ω admet un trou spectral.*

De façon plus concrète, on peut comprendre cet énoncé en termes des graphes de Cayley des projections de Γ modulo q, où q est un entier naturel non nul. Pour cela, rappelons qu' une famille de graphes finis $(\mathcal{G}_q)_{q\in\mathbb{N}^*}$ est dite *famille d'expanseurs* s'il existe une constante $c > 0$ tels que pour tout $q \in \mathbb{N}^*$, pour toute partie $X \subset \mathcal{G}_q$ telle que $|X| \leq |\mathcal{G}_q|/2$, on ait

$$|\partial X| \geq c|X|$$

où $\partial X = \{y \in \mathcal{G}_q \setminus X \mid \exists x \in X, x \leftrightarrow y\}$ est la frontière de X dans le graphe $\mathcal{G}_q$. On renvoie au livre de Lubotzky [28] pour une introduction à la théorie des graphes expanseurs. Ci-dessous, on note $\pi_q \colon \mathrm{SL}_d(\mathbb{Z}) \to \mathrm{SL}_d(\mathbb{Z}/q\mathbb{Z})$ la réduction modulo q. Le théorème 1 est équivalent à l'énoncé suivant.

Théorème 2 (Graphes de Cayley expanseurs). *Soit S une partie symétrique finie de $\mathrm{SL}_d(\mathbb{Z})$ et Γ le sous-groupe engendré par S. On suppose que l'adhérence de Zariski de Γ dans SL_d est un groupe simple. Alors, la famille de graphes de Cayley $\mathcal{G}(\pi_q(\Gamma), \pi_q(S))_{q\in\mathbb{N}^*}$ forme une famille d'expanseurs.*

Un corollaire notable de ce théorème est une borne logarithmique sur le diamètre de ces graphes de Cayley.

Corollaire 3 (Diamètre des graphes de Cayley). *Sous les hypothèses du théorème 2, il existe une constante $C \geq 0$ telle que pour tout $q \in \mathbb{N}^*$,*

$$\operatorname{diam} \mathcal{G}(\pi_q(\Gamma), \pi_q(S)) \leq C \log q.$$

On peut enfin voir le théorème 1 comme une propriété forte d'équidistribution des marches aléatoires sur Ω engendrées par des éléments de Γ. Soit μ une probabilité dont le support engendre le groupe Γ. On s'intéresse à la marche aléatoire $(x_n)_{n\geq 1}$ sur Ω définie par

$$\forall n \geq 1, \quad x_n = g_n \dots g_1,$$

où $(g_n)_{n\geq 1}$ est une suite de variables aléatoires indépendantes identiquement distribuées de loi μ sur Γ. Si μ est symétrique cette marche aléatoire $(x_n)_{n\geq 1}$ converge en

loi vers la mesure de Haar sur Ω :

$$\forall f \in C(\Omega), \quad \lim_{n\to\infty} \mathbb{E}[f(x_n)] = \int_\Omega f(x)\, \mathrm{d}m_\Omega(x).$$

Remarque. On dit qu'une mesure dont le support engendre un sous-groupe dense de Ω est *adaptée*. L'hypothèse de symétrie n'est pas vraiment nécessaire pour obtenir la convergence ci-dessus, il suffit en fait de supposer que μ est *apériodique* sur Ω, i.e., que son support n'est pas inclus dans une classe à gauche d'un sous-groupe fermé distingué dans Ω. Si $\check{\mu}$ est l'image de μ par l'application $g \mapsto g^{-1}$, alors μ est apériodique si et seulement si le support de $\check{\mu} * \mu$ engendre Ω topologiquement.

Pour $g \in \Omega$, l'opérateur T_g sur l'espace $L^2(\Omega)$ a été défini en (1.1) ci-dessus. Plus généralement, on définit *l'opérateur de convolution* associé à la probabilité μ par la formule

$$T_\mu = \int_\Omega T_g \, \mathrm{d}\mu(g),$$

et on note T_μ^0 sa restriction au sous-espace $L_0^2(\Omega)$ des fonctions de moyenne nulle. Le résultat d'équidistribution mentionné ci-dessus montre que la suite d'opérateurs $((T_\mu^0)^n)_{n\geq 1}$ converge simplement vers 0. Dire que l'action $\Gamma \curvearrowright \Omega$ admet un trou spectral revient à dire que cette convergence a lieu à vitesse exponentielle.

Théorème 4 (Rayon spectral des marches aléatoires). *Soit μ une probabilité symétrique sur $\mathrm{SL}_d(\mathbb{Z})$, Γ le sous-groupe engendré par le support de μ, et Ω l'adhérence de Γ dans $\mathrm{SL}_d(\widehat{\mathbb{Z}})$. Si l'adhérence de Zariski de Γ dans SL_d est simple, alors*

$$\|T_\mu^0\|_{\mathrm{op}} < 1.$$

Remarque. Si le support de $\check{\mu} * \mu$ n'engendre pas un sous-groupe dense dans Ω, le rayon spectral de T_μ^0 n'est pas strictement inférieur à 1. Et cela peut arriver. Pour s'en convaincre, notons $p \geq 2$ un nombre premier quelconque, $g_0 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, et prenons une mesure μ supportée par

$$g_0 U_p = \{g \in \mathrm{SL}_2(\mathbb{Z}) \mid g \equiv g_0 \bmod p\}.$$

Comme g_0^{-1} Supp μ contient le premier sous-groupe de congruence U_p, le sous-groupe engendré par μ est Zariski dense. Mais les puissances de convolution μ^n ne s'équidistribuent pas vers la mesure de Haar sur Ω, car à chaque étape n, la mesure μ^n est supportée par $g_0^n U_p$. En fait, $\Gamma/\Gamma_p \simeq \mathbb{Z}/p\mathbb{Z}$ et la marche aléatoire induite par μ sur ce quotient est cyclique.

Il n'est pas difficile de montrer que les trois théorèmes énoncés ci-dessus sont équivalents. Le but du présent article est de donner une démonstration de ces théorèmes.

Nous commencerons par montrer le théorème 4, avant d'en déduire les théorèmes 1 et 2.

Pour la démonstration, nous suivrons la stratégie proposée par Bourgain et Varjú [16] dans le cas où l'adhérence de Zariski de Γ est égale à SL_d tout entier. Cette approche se fonde d'ailleurs sur la méthode développée par Bourgain et Gamburd dans la série d'articles [10–14] pour montrer la propriété du trou spectral dans certains groupes compacts simples. La méthode de Bourgain et Gamburd consiste à ramener la propriété du trou spectral à une propriété d'expansion combinatoire dans les groupes. Dans leur premier article [12] sur le sujet, dédié à l'étude des familles de graphes de Cayley de $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ obtenus par projection modulo un nombre premier p d'un système de générateurs fixé dans $\mathrm{SL}_2(\mathbb{Z})$, cette propriété combinatoire provenait des travaux de Helfgott [24]. Pour nous, le résultat prend la forme de la proposition suivante. Ci-dessous, étant donné un ensemble A constitué de matrices à coefficients dans $\widehat{\mathbb{Z}}$ et un entier $q \in \mathbb{N}^*$, on note $N(A,q)$ le cardinal de la projection de A modulo q.

Proposition 5. *Soit μ une probabilité symétrique à support fini sur $\mathrm{SL}_d(\mathbb{Z})$. On suppose que l'adhérence de Zariski du sous-groupe Γ engendré par le support de μ est simple, connexe, et simplement connexe. Alors, pour tout $\tau > 0$, il existe deux constantes $\varepsilon > 0$ et $C \geq 1$ telles que pour tout $q \in \mathbb{N}^*$ suffisamment grand, pour tout $n \geq C \log q$, et toute partie symétrique $A \subset \Omega$, si $\mu^{*n}(A) \geq q^{-\varepsilon}$, alors l'ensemble produit $\Pi_C A = \{a_1 \dots a_C \mid a_1, \dots, a_C \in A\}$ vérifie*

$$N(\Pi_C A, q) \geq q^{-\tau} N(\Omega, q).$$

Cette proposition constitue le cœur de l'article. Sa démonstration suit la stratégie introduite par Bourgain et Varjú [16], et utilise les résultats d'équidistribution quantitative des marches aléatoires linéaires sur le tore dûs à Bourgain, Furman, Lindenstrauss et Mozes [9], que nous avons généralisés récemment dans [23]. Donnons-en brièvement l'idée générale, sans tenir compte des subtilités techniques. Notons G l'adhérence de Zariski de Γ, et $\mathfrak{g}$ son algèbre de Lie, sur laquelle G agit naturellement par l'action adjointe. Comme Γ est inclus dans les points entiers de G, il préserve un réseau rationnel $\mathfrak{g}(\mathbb{Z})$ dans $\mathfrak{g}(\mathbb{R})$, et agit donc par automorphismes linéaires sur le tore $\mathfrak{g}(\mathbb{R})/\mathfrak{g}(\mathbb{Z})$. La première étape de notre démonstration, détaillée dans la partie 4, consiste à appliquer l'équidistribution quantitative d'une marche aléatoire associée à μ sur le tore $\mathfrak{g}(\mathbb{R})/\mathfrak{g}(\mathbb{Z})$. On en déduit que sous les hypothèses de la proposition, si X est un élément quelconque de $\mathfrak{g}(\mathbb{Z})$ et D le plus grand diviseur commun à toutes les coordonnées de X, alors

$$N\big(\Sigma_C(\mathrm{Ad}\, A)X, q\big) \geq q^{-O(\varepsilon)} \Big(\frac{q}{D}\Big)^{\dim G},$$

où $\Sigma_C(\mathrm{Ad}\, A)X$ désigne l'ensemble des éléments qui s'écrivent comme somme d'au plus C éléments de $(\mathrm{Ad}\, A)X$, et $C \geq 0$ est une constante dépendant de μ. Ensuite, on utilise l'application exponentielle et la formule de Campbell–Hausdorff pour déduire de cela que si $g = e^X$, alors l'ensemble produit $\Pi_C \iota(A) \cdot g$, où $\iota(a) \cdot g = aga^{-1}$, vérifie

$$N\left(\Pi_C \iota(A) \cdot g, q\right) \geq \frac{q^{-\varepsilon}}{D^{\dim G}} \cdot N(\Omega, q).$$

Pour exploiter cette inégalité, on construira dans la partie 5 un élément $g = e^X$ dans un ensemble produit A^C dont le plus grand commun diviseur D est aussi petit que possible. Malheureusement, l'exponentielle modulo q n'est pas définie sur $\mathfrak{g}(\mathbb{Z}/q\mathbb{Z})$ mais seulement sur les vecteurs divisibles par $2r$, où r désigne le radical de q, produit des diviseurs premiers de q, donc on ne peut appliquer l'inégalité ci-dessus qu'à un élément $g = e^X$ qui appartient au sous-groupe de congruence Ω_{2r} des éléments g dans Ω tels que $g - 1$ est divisible par $2r$. Par suite, cette méthode permet seulement d'engendrer le sous-groupe Ω_{2r}. Pour obtenir le groupe Ω tout entier, il faut exploiter les travaux de Salehi Golsefidy et Varjú [21] sur l'expansion modulo les entiers sans facteurs carrés. Les conséquences importantes de leurs résultats sont expliquées dans la partie 3, et la combinaison précise de ces théorèmes avec les observations ci-dessus basées sur l'exponentielle est donnée à la partie 5.

L'article est divisé en quatre parties. Dans la première, nous rappelons à grands traits l'argument de Bourgain et Gamburd pour déduire les théorèmes 1, 2 et 4 de la proposition 5. La deuxième partie est consacrée aux résultats de Salehi Golsefidy et Varjú [21] et à certaines de leurs conséquences, nécessaires pour la suite de la démonstration. Dans la troisième partie, nous énonçons le théorème d'équidistribution quantitative des marches aléatoires linéaires sur le tore, et l'appliquons à l'étude du phénomène d'expansion dans le groupe Ω. La quatrième et dernière partie termine la démonstration de la proposition 5 ; il s'agit de combiner astucieusement les résultats des deux parties précédentes pour construire à partir de produits d'éléments de A un élément qui satisfasse de bonnes propriétés de congruence.

Pour rendre l'article plus accessible, nous avons ajouté trois appendices. Le premier résume certains résultats importants dûs à Matthews, Vaserstein et Weisfeiler [29] et à Nori [30] concernant l'approximation par des points entiers dans les groupes algébriques simples. Le second donne les propriétés élémentaires de l'application exponentielle modulo un entier $q \in \mathbb{N}^*$. Dans le dernier appendice, nous démontrons une borne inférieure sur la dimension d'une représentation unitaire irréductible du groupe profini Ω, essentielle pour déduire la propriété du trou spectral de la proposition 5.

Résumé des notations.

- $\mathbb{Z}$ anneau des entiers relatifs, $\mathbb{Q}$ corps des nombres rationnels.
- $\mathbb{Z}_p$, $\mathbb{Q}_p$ complétions respectives de $\mathbb{Z}$ et $\mathbb{Q}$ pour la valeur absolue p-adique.
- $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/q\mathbb{Z} \simeq \prod_p \mathbb{Z}_p$ complétion profinie de $\mathbb{Z}$.
- μ probabilité symétrique (à support fini) sur $\mathrm{SL}_d(\mathbb{Z})$.
- Γ sous-groupe de $\mathrm{SL}_d(\mathbb{Z})$ engendré par le support de μ.
- G adhérence de Zariski de Γ dans SL_d.
- Ω adhérence de Γ dans le groupe profini $\mathrm{SL}_d(\widehat{\mathbb{Z}})$.
- $\mathfrak{gl}_d(R)$ anneau des matrices carrées $d \times d$ à coefficients dans l'anneau $R = \mathbb{Z}$, $\mathbb{Z}_p$, $\widehat{\mathbb{Z}}$, etc.
- $q \in \mathbb{N}^*$, $\pi_q : \mathfrak{gl}_d(\widehat{\mathbb{Z}}) \to \mathfrak{gl}_d(\mathbb{Z}/q\mathbb{Z})$ projection modulo $q \in \mathbb{N}^*$.
- $\Omega_q = \{g \in \Omega \mid \pi_q(g) = 1\}$.
- $A \subset \mathfrak{gl}_d(\widehat{\mathbb{Z}})$, $N(A, q) = \operatorname{card} \pi_q(A)$.
- $A, B \subset \mathfrak{gl}_d(\widehat{\mathbb{Z}})$,

$$A + B = \{a + b \mid a \in A,\, b \in B\},$$
$$AB = \{ab \mid a \in A,\, b \in B\}.$$

- $A \subset \mathfrak{gl}_d(\widehat{\mathbb{Z}})$, $k \in \mathbb{N}^*$,

$$\Sigma_k A = \underbrace{A + \cdots + A}_{k \text{ fois}} = \{a_1 + \cdots + a_k \mid \forall i,\, a_i \in A\},$$
$$\Pi_k A = \underbrace{A \cdots A}_{k \text{ fois}} = \{a_1 \dots a_k \mid \forall i,\, a_i \in A\}.$$

- $\delta_2(p) = \begin{cases} 1 & \text{si } p = 2, \\ 0 & \text{sinon,} \end{cases}$ symbole de Kronecker.
- $x \in \mathfrak{gl}_d(\widehat{\mathbb{Z}})$, p premier, $v_p(x)$ valuation p-adique de x dans $\mathfrak{gl}_d(\widehat{\mathbb{Z}})$.
- $q = \prod_p p^{m_p}$, de radical $r = \prod_{p|q} p$.
- I ensemble de nombres premiers, $q_I = \prod_{p \in I} p^{m_p}$ et $r_I = \prod_{p \in I} p$.
- $\delta \in]0, 1[$, $q_\delta = \prod_p p^{\lfloor \delta m_p \rfloor}$.
- $\mathrm{Hom}(H, S^1)$ ensemble des caractères unitaires d'un groupe H.

2. La stratégie de Bourgain–Gamburd

Dans cette partie, nous rappelons la stratégie mise au point par Bourgain et Gamburd pour démontrer la propriété du trou spectral. Cette méthode est robuste et s'applique aussi bien aux groupes profinis [10,12,13,21,31,32] qu'aux groupes de Lie compacts [4, 11, 14]. Pour plus de simplicité, nous restreindrons notre attention au cadre présenté dans l'introduction, et qui est celui du théorème 4, que nous voulons démontrer. Ainsi, dans toute la suite, μ désigne une probabilité symétrique sur $\mathrm{SL}_d(\mathbb{Z})$, Γ le sous-groupe engendré par le support de μ, et Ω l'adhérence de Γ dans $\mathrm{SL}_d(\widehat{\mathbb{Z}})$. Nous supposerons en outre pour commencer que le support de μ est fini, et ne lèverons cette hypothèse qu'au paragraphe 2.3.

2.1. Aplanissement et trou spectral. La première étape de la démonstration du théorème 4 consiste à montrer un lemme d'aplanissement pour les puissances de convolution de la mesure μ. Soit m_Ω la probabilité de Haar sur Ω et $L^2(\Omega)$ l'espace L^2 associé sur Ω. La norme usuelle sur $L^2(\Omega)$ est notée $\|\cdot\|_2$. Pour chaque $q \in \mathbb{N}^*$, on considère le sous-groupe de congruence

$$\Omega_q = \{g \in \Omega \mid g \equiv 1 \bmod q\}$$

et on note $P_q = \mathbb{1}_{\Omega_q}/m_\Omega(\Omega_q)$ la suite d'unités approchées obtenue à partir de la famille $(\Omega_q)_{q\in\mathbb{N}^*}$.

Lemme 6 (Lemme d'aplanissement). *Il existe une constante $C \geq 1$ dépendant de μ telle que pour tout $\tau > 0$, il existe $\delta > 0$ tel que pour tout $n \geq C \log q$,*

$$\|\mu^{*n} * P_q\|_2 \geq q^{\tau},$$

alors

$$\|\mu^{*2n} * P_q\|_2 \leq q^{-\delta}\|\mu^{*n} * P_q\|_2.$$

Démonstration. Rappelons qu'étant donné un paramètre $K \geq 1$, une partie A d'un groupe fini H est un *sous-groupe K-approximatif* si A est symétrique, contient l'élément neutre et s'il existe un ensemble $X \subset H$ fini de cardinal $\leq K$ tel que $AA \subset AX$. En particulier, si A est un sous-groupe K-approximatif alors

$$\forall k \geq 1, \quad |\Pi_k A| \leq K^{k-1}|A|.$$

Grâce à une version non commutative du lemme de Balog–Szemerédi–Gowers [35, Corollary 2.46], les sous-groupes approximatifs d'un groupe fini sont reliés aux convolutions de mesures via le lemme suivant, qui apparaît déjà implicitement dans l'article de Bourgain et Gamburd [12].

Lemme 7. *Soit $K \geq 2$ un paramètre. Soient ν et ν' des mesures de probabilité sur un groupe fini H. On suppose que*

$$\|\nu * \nu'\|_2 \geq K^{-1} \|\nu\|_2^{\frac{1}{2}} \|\nu'\|_2^{\frac{1}{2}}.$$

Alors il existe un sous-groupe $K^{O(1)}$-approximatif $A \subset H$ tel que

- $K^{-O(1)} \|\nu\|_2^{-2} \leq |A| \leq K^{O(1)} \|\nu\|_2^{-2}$,
- *il existe $h \in H$ tel que $\nu(hA) \geq K^{-O(1)}$,*
- *il existe $h' \in H$ tel que $\nu'(Ah') \geq K^{-O(1)}$.*

Pour démontrer le lemme 6, on raisonne par l'absurde en supposant que

$$\|\mu^{*2n} * P_q\|_2 > q^{-\delta} \|\mu^{*n} * P_q\|_2,$$

pour $\delta > 0$ arbitrairement petit. D'après le lemme 7 ci-dessus, appliqué dans le groupe fini Ω/Ω_q à la mesure image de μ^{*n} par π_q, il existe une partie symétrique $A \subset \Omega$ telle que $\pi_q(A)$ soit un sous-groupe $q^{O(\delta)}$-approximatif et que

$$\mu^{*2n}(AA) \geq q^{-O(\delta)}$$

et

$$N(A, q) \leq q^{-2\tau + O(\delta)} N(\Omega, q).$$

Rappelons que $N(A, q)$ désigne le nombre de recouvrement de A par des classes de Ω_q ; autrement dit, $N(A, q)$ est le cardinal de la projection de A dans Ω/Ω_q. Soient $\varepsilon > 0$ et $C \geq 1$ les constantes données par la proposition 5, de sorte que si $\delta > 0$ est choisi suffisamment petit par rapport à ε, alors

$$N(\Pi_{2C} A, q) \geq N(\Omega, q)^{1-\tau}.$$

Mais par ailleurs, comme A est un sous-groupe $q^{O(\delta)}$-approximatif,

$$N(\Pi_{2C} A, q) \leq q^{O(C\delta)} N(A, q) \leq q^{-2\tau + O(C\delta)} N(\Omega, q).$$

Si δ est suffisamment petit par rapport à τ/C, cela donne la contradiction recherchée. ∎

Une application itérée du lemme d'aplanissement permet alors d'obtenir la proposition suivante.

Proposition 8. *Soit μ une probabilité à support fini sur $\mathrm{SL}_d(\mathbb{Z})$. On suppose que l'adhérence de Zariski du sous-groupe Γ engendré par $\mathrm{Supp}\,\mu$ est simple, connexe et simplement connexe. Alors, pour tout $\tau > 0$ il existe $C \geq 1$ tel que pour tout $n \geq C \log q$,*

$$\|\mu^{*n} * P_q\|_2 \leq q^{\tau}.$$

2.2. Multiplicité des représentations et trou spectral. À partir de la proposition 8, la démonstration du théorème 4 se fait par un argument d'analyse de Fourier sur le groupe compact Ω. On notera $\widehat{\Omega}$ le dual unitaire de Ω, i.e., l'ensemble des représentations unitaires irréductibles de Ω, à équivalence près. Comme Ω est un groupe compact, $\widehat{\Omega}$ est constitué de représentations de dimension finie.

L'ingrédient essentiel de la démonstration est la proposition 9 ci-dessous, qui tire son origine des observations de Frobenius sur les représentations du groupe $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, lorsque p est un nombre premier arbitraire. Lorsque le groupe Γ est dense dans SL_d au sens de la topologie de Zariski, sa démonstration est plus facile, et apparaît déjà dans [16, Proof of Theorem 1]. Le résultat général est sans doute bien connu des spécialistes, mais les différents cas à étudier dans la démonstration sont éparpillés dans la littérature sur le sujet [17, 26, 31]. Nous en donnerons donc une démonstration complète dans l'appendice C.

Proposition 9 (Propriété quasi-aléatoire). *Soit Γ un sous-groupe de $\mathrm{SL}_d(\mathbb{Z})$ et Ω l'adhérence de Γ dans $\mathrm{SL}_d(\widehat{\mathbb{Z}})$. On suppose que l'adhérence de Zariski de Γ dans SL_d est semi-simple, connexe et simplement connexe. Alors, il existe $\kappa > 0$ tel que pour tout $(\rho, V_\rho) \in \widehat{\Omega}$, il existe $q \in \mathbb{N}^*$ tel que*

$$\Omega_q \subset \ker \rho \quad \text{et} \quad \dim V_\rho \geq \kappa q^\kappa.$$

Pour le reste, la démonstration est basée sur la formule de Parseval dans le groupe compact Ω. Si (ρ, V_ρ) est une représentation unitaire de Ω et μ une mesure borélienne finie sur Ω, on définit un élément $\rho(\mu) \in \mathrm{End}(V_\rho)$ par la formule

$$\rho(\mu) = \int_\Omega \rho(g)\,\mathrm{d}\mu(g).$$

De façon similaire, si $f \in L^1(\Omega)$, on définit

$$\rho(f) = \int_\Omega \rho(g) f(g)\,\mathrm{d}m_\Omega(g).$$

Démonstration du théorème 4, cas particulier. Pour pouvoir appliquer la proposition 9, on se restreint ici au cas particulier où μ est à support fini et où l'adhérence de Zariski de Γ est un groupe algébrique simple, connexe et simplement connexe. Pour $n \geq 1$, la formule de Parseval [18, §5.3, équation (5.16)] appliquée à la fonction $\mu^{*n} * P_q$ sur Ω s'écrit

$$\|\mu^{*n} * P_q\|_2^2 = \sum_{\rho \in \widehat{\Omega}} (\dim V_\rho) \|\rho(\mu)^n \rho(P_q)\|_{\mathrm{HS}}^2,$$

où l'on note $\|\varphi\|_{\mathrm{HS}} = \sqrt{\mathrm{Tr}(\varphi^*\varphi)}$ la norme de Hilbert–Schmidt d'un endomorphisme φ d'un espace de Hilbert. D'après la proposition 9, il existe $\kappa > 0$ tel que pour tout $\rho \in \widehat{\Omega}$,

il existe $q \in \mathbb{N}^*$ tel que

$$\Omega_q \subset \ker \rho \quad \text{et} \quad \dim V_\rho \geq \kappa q^\kappa.$$

L'inclusion $\Omega_q \subset \ker \rho$ implique en particulier $\rho(P_q) = \mathrm{Id}_{V_\rho}$.

Alors, d'après la proposition 8 appliquée avec $\tau = \kappa/5$, il existe une constante $C \geq 1$ telle que, pour $n = C \log q$,

$$\kappa q^\kappa \, \|\rho(\mu)^n\|_{\mathrm{HS}}^2 \leq \|\mu^{*n} * P_q\|_2^2 \leq q^{2\tau}.$$

Comme la norme de Hilbert–Schmidt majore la norme d'opérateur sur $\mathrm{End}\, V_\rho$, cela implique, avec le fait que $\rho(\mu)$ est un opérateur symétrique, pour q suffisamment grand,

$$\|\rho(\mu)\|_{\mathrm{op}} = \|\rho(\mu)^n\|_{\mathrm{op}}^{\frac{1}{n}} \leq \|\rho(\mu)^n\|_{\mathrm{HS}}^{\frac{1}{n}} \leq \kappa^{-\frac{1}{2n}} q^{\frac{-\kappa+2\tau}{2n}} = \kappa^{-\frac{1}{2n}} e^{\frac{-3\tau}{2C}} \leq e^{-\frac{\tau}{C}} < 1.$$

On en déduit qu'il existe des constantes $c > 0$ et $Q > 1$ telle pour tout $\rho \in \widehat{\Omega}$,

(1) ou bien $\|\rho(\mu)\|_{\mathrm{op}} \leq 1 - c$,

(2) ou bien il existe $q \leq Q$ et $\Omega_q \subset \ker \rho$.

La deuxième option n'est possible que pour un nombre fini de $\rho \in \widehat{\Omega}$, pour lesquelles on doit avoir $\|\rho(\mu)\|_{\mathrm{op}} < 1$ si ρ est non triviale. Comme

$$\|T_\mu^0\|_{\mathrm{op}} = \sup\{\|\rho(\mu)\|_{\mathrm{op}} \mid \rho \in \widehat{\Omega}, \rho \neq 1\}$$

le théorème est démontré lorsque l'adhérence de Zariski de Γ est simplement connexe.

∎

2.3. La propriété du trou spectral. Nous expliquons maintenant comment déduire le cas général du théorème 4 du cas particulier démontré au paragraphe précédent. Comme le reste de cette partie, l'argument présenté n'est pas nouveau, et apparaît déjà par exemple dans Salehi Golsefidy [31, §2.3].

Afin de démontrer le théorème 4 sans l'hypothèse de simple connexité, il est commode de passer par l'énoncé équivalent du théorème 1. Pour cela, nous ferons usage du lemme suivant, tiré du livre de Bekka, de la Harpe et Valette [3, Proposition G.4.2].

Lemme 10. *Soit Γ un groupe dénombrable, ρ une représentation unitaire de Γ et μ une probabilité symétrique sur Γ.*

(1) *Si $\|\rho(\mu)\|_{\mathrm{op}} < 1$, alors ρ n'a pas de vecteur presque invariant.*

(2) *Si ρ n'a pas de vecteur presque invariant et si le support de μ engendre Γ, alors $\|\rho(\mu)\|_{\mathrm{op}} < 1$.*

Par ailleurs, nous aurons besoin d'un lemme pour passer du groupe Γ à un sous-groupe d'indice fini, et réciproquement. L'énoncé ci-dessous est tiré de l'article [1, Lemma 3.3].

Lemme 11. *Soit Γ un sous-groupe de $\mathrm{SL}_d(\mathbb{Z})$ et Ω son adhérence dans $\mathrm{SL}_d(\widehat{\mathbb{Z}})$. Soit Γ' un sous-groupe d'indice fini de Γ et Ω' l'adhérence de Γ' dans Ω. L'action $\Gamma' \curvearrowright \Omega'$ admet un trou spectral, si et seulement si $\Gamma \curvearrowright \Omega$ admet un trou spectral.*

Nous pouvons maintenant démontrer le théorème 1 en toute généralité.

Démonstration du théorème 1. Notons G l'adhérence de Zariski de Γ dans SL_d. Par hypothèse, G est simple. Si G est connexe et simplement connexe, le cas particulier du théorème 4 démontré au paragraphe précédent montre que $\|T_\mu^0\|_{\mathrm{op}} < 1$ pour toute probabilité symétrique μ dont le support est fini et engendre Γ. Avec le lemme 10, cela montre que $\Gamma \curvearrowright \Omega$ admet un trou spectral.

Si G n'est pas connexe, notons G^0 la composante neutre de G, $\Gamma^0 = \Gamma \cap G^0$ et Ω^0 l'adhérence de Γ^0 dans Ω. Le groupe Γ^0 est un sous-groupe distingué d'indice fini dans Γ dont l'adhérence de Zariski est G^0. Si G^0 est simplement connexe, ce qui précède montre que $\Gamma^0 \curvearrowright \Omega^0$ admet un trou spectral. Le lemme 11 permet d'en déduire que $\Gamma \curvearrowright \Omega$ admet un trou spectral. Cela démontre le théorème lorsque G est simplement connexe.

Enfin, dans le cas général, soit $\pi\colon \widetilde{G} \to G$ le revêtement simplement connexe de G. Rappelons que π est une isogénie. Fixons une $\mathbb{Q}$-représentation fidèle $\widetilde{G} \hookrightarrow \mathrm{SL}_{\widetilde{d}}$ dans un groupe linéaire, pour un certain $\widetilde{d} \geq 2$, et notons

$$\widetilde{G}(\mathbb{Z}) = \widetilde{G} \cap \mathrm{SL}_{\widetilde{d}}(\mathbb{Z}).$$

D'après Borel [5, théorème 8.9], les groupes $\pi(\widetilde{G}(\mathbb{Z}))$ et $G(\mathbb{Z})$ sont commensurables. Posons

$$\widetilde{\Gamma} = \widetilde{G}(\mathbb{Z}) \cap \pi^{-1}(\Gamma).$$

L'adhérence de Zariski de $\widetilde{\Gamma}$ dans $\mathrm{SL}_{\widetilde{d}}$ est égale au groupe simplement connexe $\widetilde{G}$, et donc, d'après ce qui précède, l'action de $\widetilde{\Gamma}$ sur son adhérence $\widetilde{\Omega}$ dans $\mathrm{SL}_{\widetilde{d}}(\widehat{\mathbb{Z}})$ admet un trou spectral. En d'autres termes, si l'on note

$$\widetilde{\Gamma}_q = \{g \in \widetilde{\Gamma} \mid g \equiv 1 \bmod q\}, \quad q \in \mathbb{N}^*$$

alors $\widetilde{\Gamma}$ a la propriété (τ) par rapport à la famille $(\widetilde{\Gamma}_q)_{q\in\mathbb{N}^*}$: il existe une partie finie $\widetilde{S} \subset \widetilde{\Gamma}$ et $\varepsilon > 0$ tels que

$$\forall q \in \mathbb{N}^*,\ \forall v \in L^2_0(\widetilde{\Gamma}/\widetilde{\Gamma}_q),\ \exists g \in \widetilde{S}, \quad \|\rho(g)v - v\| \geq \varepsilon\|v\|.$$

Comme π est un morphisme de $\mathbb{Q}$-groupes, pour $g \in \widetilde{G}$, les coefficients de $\pi(g)$ sont donnés par des polynômes rationnels en les coefficients de g. Il existe donc $k \in \mathbb{N}^*$ tel que pour tout $q \in \mathbb{N}^*$, on ait

$$\pi(\widetilde{\Gamma}_{kq}) \subset \pi(\widetilde{\Gamma})_q = \{g \in \pi(\widetilde{\Gamma}) \mid g \equiv 1 \bmod q\}.$$

Par suite, toute représentation de $\pi(\widetilde{\Gamma})/\pi(\widetilde{\Gamma})_q$ se relève en une représentation de $\widetilde{\Gamma}/\widetilde{\Gamma}_{kq}$, et $\pi(\widetilde{\Gamma})$ a la propriété (τ) par rapport à la famille de ses sous-groupes de congruence $(\pi(\widetilde{\Gamma})_q)_{q\in\mathbb{N}^*}$: il existe une partie finie $S \subset \pi(\widetilde{\Gamma})$ et $\varepsilon > 0$ tels que

$$\forall q \in \mathbb{N}^*,\ \forall v \in L^2_0(\pi(\widetilde{\Gamma})/\pi(\widetilde{\Gamma})_q),\ \exists g \in S, \quad \|\rho(g)v - v\| \geq \varepsilon\|v\|.$$

Cela est équivalent à dire que l'action de $\pi(\widetilde{\Gamma})$ sur son adhérence dans $\mathrm{SL}_d(\widehat{\mathbb{Z}})$ admet un trou spectral. Comme $\pi(\widetilde{\Gamma})$ est d'indice fini dans Γ, le lemme 11 permet de conclure que l'action de Γ sur Ω admet un trou spectral. ∎

3. Expansion modulo les nombres sans facteur carré

Nous rappelons maintenant la propriété du trou spectral modulo les entiers sans facteur carré, due à Salehi Golsefidy et Varjú [21], et certaines de ses conséquences, dont nous aurons besoin plus tard.

3.1. Trou spectral et expansion modulo r. Le théorème suivant est tiré des travaux de Salehi Golsefidy et Varjú sur l'expansion dans les groupes parfaits [21, Theorem 1].

Théorème 12 (Trou spectral modulo les entiers sans facteur carré). *Soit μ une probabilité sur $\mathrm{SL}_d(\mathbb{Z})$, Γ le semi-groupe engendré par μ, et Ω l'adhérence de Γ dans $\mathrm{SL}_d(\widehat{\mathbb{Z}})$. On suppose que l'adhérence de Zariski de Γ est parfaite. Alors l'action du groupe Γ sur $\varprojlim \Omega/\Omega_r$, r parcourant l'ensemble des entiers naturels sans facteur carré, admet un trou spectral.*

Cette propriété d'expansion nous sera utile sous la forme de la proposition suivante, que nous associerons ensuite aux résultats de la partie 4 pour obtenir le théorème de trou spectral annoncé dans l'introduction. Pour pouvoir utiliser les résultats de l'approximation forte rappelés dans l'appendice A, nous supposerons toujours dans la suite que l'adhérence de Zariski de Γ est simple, connexe et simplement connexe.

Proposition 13. *Soit μ une probabilité sur $\mathrm{SL}_d(\mathbb{Z})$ et Γ le semi-groupe engendré par μ. On suppose que l'adhérence de Zariski de Γ est simple, connexe et simplement connexe. Étant donné $\varepsilon_0 > 0$, il existe $\varepsilon > 0$ et $C \geq 0$ tels que l'énoncé suivant soit*

vérifié pour tout entier sans facteur carré r suffisamment grand et tout $q \geq r$. Soit $A \subset \Gamma$ tel que $\mu^{*n}(A) \geq q^{-\varepsilon}$, où $n \geq C \log q$. Il existe un entier $r'|r$ tel que $r' \geq q^{-\varepsilon_0} r$ et

$$\pi_{r'}(\Pi_C A) = \Omega/\Omega_{r'}.$$

Nous reprenons essentiellement la démonstration de Bourgain et Varjú [16, Proposition 3]. Commençons par un lemme qui est une conséquence facile de la propriété du trou spectral.

Lemme 14. *Sous les hypothèses de la proposition 13, il existe une constante C telle que pour tout $n \geq C \log r$ et toute partie A satisfaisant $\mu^{*n}(A) \geq q^{-\varepsilon}$, on a*

$$|\pi_r(A)| \gg q^{-\varepsilon}[\Omega : \Omega_r].$$

Démonstration. D'après le théorème 12 et la caractérisation du trou spectral 10, il existe $c > 0$ tel que

$$\left\| (\pi_r)_*(\mu^{*n}) - \frac{\mathbf{1}_{\Omega/\Omega_r}}{[\Omega : \Omega_r]} \right\|_\infty \leq \left\| (\pi_r)_*(\mu^{*n}) - \frac{\mathbf{1}_{\Omega/\Omega_r}}{[\Omega : \Omega_r]} \right\|_2 \leq e^{-cn}.$$

Le lemme est alors immédiat avec $C = 1/c$. ∎

Pour la démonstration de la proposition 13, nous aurons aussi besoin d'un résultat de Gowers [22]. Étant donné un groupe fini H, nous notons $m(H)$ le degré minimal d'une représentation linéaire complexe non triviale.

Lemme 15. *Soient A_1, A_2, A_3 trois parties d'un groupe fini H. Si $|A_1||A_2||A_3| > |H|^3/m(H)$, alors $A_1A_2A_3 = H$.*

Nous admettons ce lemme. Sa démonstration est une simple application de la formule de Plancherel pour le groupe fini H ; le lecteur est renvoyé à Gowers [22, Theorem 3.3] pour plus de détails.

Démonstration de la proposition 13. Écrivons $r = \prod_{i=1}^m p_i$. Par le lemme chinois, le groupe $\pi_r(\mathrm{SL}_d(\hat{\mathbb{Z}})) = \mathrm{SL}_d(\mathbb{Z}/r\mathbb{Z})$ s'identifie à $\prod_{i=1}^m \mathrm{SL}_d(\mathbb{Z}/p_i\mathbb{Z})$. Nous verrons donc $\pi_r(\Omega)$ comme une partie de ce produit, et écrirons un élément $g \in \pi_r(\Omega)$ en coordonnées

$$g = (g_1, \ldots, g_m), \quad g_i \in \Omega/\Omega_{p_i}.$$

Le procédé de régularisation expliqué dans Bourgain–Gamburd–Sarnak [15, Lemma 5.2] permet de construire une partie $A' \subset \pi_r(A)$ et des constantes $K_i, i = 1, \ldots, m$ telles que pour chaque i, pour tout $g \in A'$,

$$|\{x \in \Omega/\Omega_{p_i} \mid (g_1, \ldots, g_{i-1}, x) \in \pi_{p_1 \ldots p_i}(A')\}| = K_i$$

et

$$|A'| = \prod_{i=1}^{m} K_i \geq \frac{|\pi_r(A)|}{\prod_{i=1}^{m} 2\log[\Omega : \Omega_{p_i}]}.$$

Cela se fait par induction rétrograde. Tout d'abord, par le principe des tiroirs, on choisit $1 \leq K_m \leq [\Omega : \Omega_{p_m}]$ et $A_m \subset \pi_r(A)$ tel que $|A_m| \geq |\pi_r(A)|/\log[\Omega : \Omega_{p_m}]$ en restreignant les $m-1$ premières coordonnées de sorte que pour tout $g = (g_1, \dots, g_m)$ dans A_m

$$K_m \leq |\{x \in \Omega/\Omega_{p_m} \mid (g_1, \dots, g_{m-1}, x) \in \pi_r(A)\}| \leq 2K_m.$$

Donc on peut choisir une sous-partie $A'_m \subset A_m$ avec $|A'_m| \geq |A_m|/2$ pour que toutes les fibres de la dernière coordonnée aient le même cardinal : pour tout $g = (g_1, \dots, g_m) \in A'_m$,

$$|\{x \in \Omega/\Omega_{p_m} \mid (g_1, \dots, g_{m-1}, x) \in A'_m\}| = K_m.$$

De même, on choisit K_{m-1} et $A_{m-1} \subset A'_m$ tel que $|A_{m-1}| \geq |A'_m|/\log[\Omega : \Omega_{p_{m-1}}]$ et pour tout $g = (g_1, \dots, g_m)$ dans A_{m-1},

$$K_{m-1} \leq |\{x \in \Omega/\Omega_{p_{m-1}} \mid (g_1, \dots, g_{m-2}, x) \in \pi_{p_1 \dots p_{m-1}}(A'_m)\}| \leq 2K_{m-1},$$

puis $A'_{m-1} \subset A_{m-1}$ tel que pour tout $g = (g_1, \dots, g_m) \in A'_{m-1}$,

$$|\{x \in \Omega/\Omega_{p_{m-1}} \mid (g_1, \dots, g_{m-2}, x) \in \pi_{p_1 \dots p_{m-1}}(A'_{m-1})\}| = K_{m-1}.$$

Après m étapes, ce procédé nous permet d'obtenir un ensemble $A' = A'_1$ qui satisfait les conditions requises. Au vu du lemme 14 et du lemme A.4, si r est assez grand,

$$\prod_{i=1}^{m} K_i \geq r^{-\varepsilon} q^{-\varepsilon} [\Omega : \Omega_r] \geq q^{-3\varepsilon} \prod_{i=1}^{m} [\Omega : \Omega_{p_i}].$$

La proposition 9 donne l'existence de $\kappa > 0$ tel que pour tout nombre premier p suffisamment grand, $m(\Omega/\Omega_p) \geq p^{\kappa}$. Posons

$$I = \{i \in \{1, \dots, m\} \mid K_i > p_i^{-\frac{\kappa}{3}} [\Omega : \Omega_{p_i}]\}$$

et

$$r' = \prod_{i \in I} p_i.$$

Pour $i \notin I$, on majore $K_i \leq p_i^{-\frac{\kappa}{3}} [\Omega : \Omega_{p_i}]$, tandis que pour $i \in I$, on a toujours $K_i \leq [\Omega : \Omega_{p_i}]$, et par conséquent :

$$q^{-3\varepsilon} \prod_{i=1}^{m} [\Omega : \Omega_{p_i}] \leq \prod_{i=1}^{m} K_i \leq \left(\frac{r}{r'}\right)^{-\frac{\kappa}{3}} \prod_{i=1}^{m} [\Omega : \Omega_{p_i}].$$

Ainsi, pourvu que $\varepsilon < \kappa\varepsilon_0/9$,

$$\frac{r}{r'} \leq q^{\frac{9\varepsilon}{\kappa}} \leq q^{\varepsilon_0}.$$

Pour $i \in \{0, \dots, m-1\}$, notons $r'_i = \prod_{j\in\{1,\dots,i\}\cap I} p_j$ et montrons par récurrence sur i que

$$\pi_{r'_i}(\Pi_3 A') = \Omega/\Omega_{r'_i}. \tag{3.1}$$

Le résultat est trivial pour $i = 0$. Supposons donc le résultat connu pour $i-1 \in \{0, \dots, m-1\}$. Si $i \notin I$, il n'y a rien à démontrer, car $r'_i = r'_{i-1}$. Sinon $r'_i = r'_{i-1}p_i$ et on dispose d'un morphisme injectif

$$(\pi_{r'_{i-1}}, \pi_{p_i})\colon \Omega/\Omega_{r'_i} \to \Omega/\Omega_{r'_{i-1}} \times \Omega/\Omega_{p_i}.$$

Il suffit de montrer que pour tout $h \in \Omega/\Omega_{r'_{i-1}}$,

$$\pi_{p_i}\left(\pi^{-1}_{r'_{i-1}}(\{h\}) \cap \Pi_3 A'\right) = \Omega/\Omega_{p_i}. \tag{3.2}$$

Or, par hypothèse de récurrence il existe $g_1, g_2, g_3 \in A'$ tel que $h = \pi_{r'_{i-1}}(g_1g_2g_3)$. Par construction de A', les trois parties

$$B_j = \{g \in A' \mid \pi_{r'_{i-1}}(g) = \pi_{r'_{i-1}}(g_j)\}, \quad j = 1, 2, 3,$$

vérifient $|\pi_{p_i}(B_j)| \geq K_i$, et donc, vu le choix de I,

$$|\pi_{p_i}(B_1)||\pi_{p_i}(B_2)||\pi_{p_i}(B_3)| > \frac{[\Omega : \Omega_{p_i}]^3}{m(\Omega/\Omega_{p_i})}.$$

D'après le lemme 15, cela implique $\pi_{p_i}(B_1B_2B_3) = \Omega/\Omega_{p_i}$. Comme $\pi_{r'_{i-1}}(B_1B_2B_3) = h$, cela termine la démonstration de (3.2) et ainsi celle de (3.1). ∎

3.2. Points dans Ω_p/Ω_{p^2}. Nous réunissons ici plusieurs lemmes qui nous serviront plus tard à construire des éléments non triviaux dans les quotients Ω_p/Ω_{p^2}. Dans tout le paragraphe, Γ désigne un sous-groupe de $\mathrm{SL}_d(\mathbb{Z})$ dont l'adhérence de Zariski G dans SL_d est simple, connexe, et simplement connexe. On note encore Ω l'adhérence de Γ dans le groupe profini $\mathrm{SL}_d(\widehat{\mathbb{Z}})$, et pour tout $q \in \mathbb{N}^*$,

$$\Omega_q = \{g \in \Omega \mid g \equiv 1 \bmod q\}.$$

Enfin, la projection modulo q sera notée $\pi_q\colon \Omega \to \Omega/\Omega_q$.

Lemme 16. *Pour tout nombre premier p suffisamment grand, la suite exacte*

$$1 \to \Omega_p/\Omega_{p^2} \to \Omega/\Omega_{p^2} \to \Omega/\Omega_p \to 1$$

n'est pas scindée.

Démonstration. Supposons $p > 2d$ et montrons que pour tout $g \in \Omega$, si $\pi_p(g)$ est d'ordre p dans Ω/Ω_p alors $\pi_{p^2}(g)$ est d'ordre p^2 dans Ω/Ω_{p^2}.

En effet, si $\pi_p(g)$ est d'ordre p alors g s'écrit $g = 1 + u$ avec $u \in \mathfrak{gl}_d(\hat{\mathbb{Z}})$ vérifiant $u^p \equiv 0 \bmod p$. La matrice $\pi_p(u)$ est un élément nilpotent de $\mathfrak{gl}_d(\mathbb{Z}/p\mathbb{Z})$, donc $u^d \equiv 0 \bmod p$, et par suite, $u^{2d} \equiv 0 \bmod p^2$. Soit $k \geq 1$ minimal tel que $u^k \equiv 0 \bmod p$. Comme p divise $\binom{p}{\ell}$ pour $1 \leq \ell < p$ et qu'en outre $p > 2d \geq k$, la formule du binôme de Newton nous donne

$$g^p \equiv 1 + pu + \binom{p}{2}u^2 + \cdots + \binom{p}{k-1}u^{k-1} \bmod p^2.$$

Mais

$$\Big(u + \frac{1}{p}\binom{p}{2}u^2 + \cdots + \frac{1}{p}\binom{p}{k-1}u^{k-1}\Big)^{k-1} \equiv u^{k-1} \not\equiv 0 \bmod p.$$

Donc

$$u + \frac{1}{p}\binom{p}{2}u^2 + \cdots + \frac{1}{p}\binom{p}{k-1}u^{k-1} \not\equiv 0 \bmod p$$

et $g^p \not\equiv 1 \bmod p^2$. Par la formule du binôme à nouveau, $g^{p^2} \equiv 1 \bmod p^2$. Cela montre que $\pi_{p^2}(g)$ est d'ordre p^2 dans Ω/Ω_{p^2}.

Pour p suffisamment grand, on sait par le lemme A.5 que le groupe Ω/Ω_p contient des éléments d'ordre p. On en déduit que $\pi_p\colon \Omega/\Omega_{p^2} \to \Omega/\Omega_p$ n'admet pas de section dans la catégorie des groupes. ∎

Nous montrons maintenant une version quantitative de l'énoncé : si ψ est une section ensembliste de la suite exacte du lemme 16, alors on doit avoir $\psi(xy) \neq \psi(x)\psi(y)$ pour la plupart des couples (x, y) d'éléments de Ω/Ω_p.

Lemme 17. *Il existe $\sigma > 0$ dépendant seulement de Γ tel que l'assertion suivante soit vraie. Soit $r \in \mathbb{N}^*$ un entier sans facteur carré dont les facteurs premiers sont tous assez grands. Soit p un facteur premier de r. Si $\psi\colon \Omega/\Omega_r \to \Omega$ est une section ensembliste de π_r, i.e., $\pi_r \circ \psi = \mathrm{Id}_{\Omega/\Omega_r}$, alors l'événement*

$$\psi(xy) \equiv \psi(x)\psi(y) \bmod p^2$$

est de probabilité au plus $p^{-\sigma}$ lorsque x et y sont deux variables aléatoires indépendantes de loi uniforme sur Ω/Ω_r.

Démonstration. On suppose que tous les facteurs premiers de r sont suffisamment grands, si bien que $\Omega/\Omega_r = \prod_{p|r} \Omega/\Omega_p$ d'après le lemme A.3. Fixons un facteur premier p de r. Écrivons $r = ps$ et identifions Ω/Ω_r à $\Omega/\Omega_p \times \Omega/\Omega_s$. Pour chaque $x_2 \in \Omega/\Omega_s$, l'application $\psi_{x_2}\colon \Omega/\Omega_p \to \Omega/\Omega_{p^2}$ définie par $\psi_{x_2}(x_1) = \pi_{p^2} \circ \psi(x_1, x_2)$ est une section de la projection $\pi_p\colon \Omega/\Omega_{p^2} \to \Omega/\Omega_p$. Notons ν_{x_2} la mesure image de la probabilité uniforme sur Ω/Ω_p par l'application ψ_{x_2}.

Observons que pour tout $x_2 \in \Omega/\Omega_s$,

$$\|\nu_{x_2}\|_2 = [\Omega : \Omega_p]^{-\frac{1}{2}}. \tag{3.3}$$

Observons aussi que pour tout couple $(x_2, y_2) \in \Omega/\Omega_s \times \Omega/\Omega_s$,

$$\begin{aligned}\operatorname{card}\{(x_1, y_1) \in \Omega/\Omega_p \times \Omega/\Omega_p \mid \psi(x_1, x_2)\psi(y_1, y_2) &\equiv \psi(x_1y_1, x_2y_2) \bmod p^2\}\\ &= \operatorname{card}\{(x_1, y_1) \in \Omega/\Omega_p \times \Omega/\Omega_p \mid \psi_{x_2}(x_1)\psi_{y_2}(y_1) = \psi_{x_2y_2}(x_1y_1)\}\\ &= [\Omega : \Omega_p]^3 \langle \nu_{x_2} * \nu_{y_2}, \nu_{x_2y_2}\rangle\end{aligned}$$

de sorte que

$$\mathbb{P}[\psi(xy) \equiv \psi(x)\psi(y) \bmod p^2] = \frac{[\Omega : \Omega_p]}{[\Omega : \Omega_s]^2} \sum_{(x_2,y_2)\in\Omega/\Omega_s\times\Omega/\Omega_s} \langle \nu_{x_2} * \nu_{y_2}, \nu_{x_2y_2}\rangle.$$

Supposons par l'absurde que cette probabilité soit supérieure à $p^{-\sigma}$. Alors il existe $(x_2, y_2) \in \Omega/\Omega_s \times \Omega/\Omega_s$ tel que

$$p^{-\sigma} \leq [\Omega : \Omega_p]\langle \nu_{x_2} * \nu_{y_2}, \nu_{x_2y_2}\rangle.$$

Par l'inégalité de Cauchy–Schwarz et (3.3),

$$\|\nu_{x_2} * \nu_{y_2}\|_2 \geq p^{-\sigma}\|\nu_{x_2}\|_2^{\frac{1}{2}}\|\nu_{y_2}\|_2^{\frac{1}{2}}.$$

Avec le lemme 7, cela donne un sous-groupe $p^{O(\sigma)}$-approximatif $A \subset \Omega/\Omega_{p^2}$ et un élément $h \in \Omega/\Omega_{p^2}$ tel que $\nu_{x_2}(hA) \geq p^{-O(\sigma)}$ et

$$|A| \leq p^{O(\sigma)}\|\nu_{x_2}\|_2^{-2} = p^{O(\sigma)}[\Omega : \Omega_p]. \tag{3.4}$$

Il s'ensuit que

$$\frac{|\pi_p(A)|}{[\Omega : \Omega_p]} = ((\pi_p)_*\nu_{x_2})(\pi_p(hA)) = \nu_{x_2}(hA) \geq p^{-O(\sigma)}.$$

Pour p assez grand, $\Omega/\Omega_p = G(\mathbb{Z}/p\mathbb{Z})$ par le théorème A.2. Donc, par le théorème C.5, $m(\Omega/\Omega_p) \geq (p-1)/2$. On peut alors choisir σ suffisamment petit pour pouvoir appliquer le lemme 15 à $\pi_p(A) \subset \Omega/\Omega_p$. On obtient

$$\pi_p(\Pi_3 A) = \Omega/\Omega_p.$$

Soit $\phi\colon \Omega/\Omega_p \to \Pi_3 A$ une section de π_p. D'après le lemme 16, il existe $x_1, y_1 \in \Omega/\Omega_p$ tels que $\phi(x_1y_1) \neq \phi(x_1)\phi(y_1)$, et l'élément

$$z = \phi(x_1y_1)\phi(y_1)^{-1}\phi(x_1)^{-1} \in \Pi_9 A$$

vérifie alors

$$z \in \Omega_p/\Omega_{p^2} \setminus \{1\}.$$

Considérons l'action de $\Pi_3 A$ sur Ω_p/Ω_{p^2} par conjugaison. D'après le lemme A.6, l'ensemble

$$B = \{aza^{-1} \mid a \in \Pi_3 A\}$$

est égal à l'orbite de z sous l'action de Ω/Ω_p et de plus z n'est pas un point fixe. Ainsi, le stabilisateur de z est un sous-groupe propre donc d'indice au moins $(p-1)/2$ d'après le corollaire C.6. On en déduit que $|B| \geq (p-1)/2$. En remarquant que $B \subset (\Pi_{15} A) \cap \ker \pi_p$, on obtient

$$|\Pi_{18} A| \geq |B(\Pi_3 A)| \geq |B||\pi_p(\Pi_3 A)| \geq \frac{p-1}{2}[\Omega : \Omega_p].$$

Si σ est choisi suffisamment petit, cela contredit (3.4) et le fait que A est un sous-groupe $p^{O(\sigma)}$-approximatif. ∎

Lemme 18. *Pour tout $\varepsilon > 0$, si r est un entier suffisamment grand sans facteur carré, et si A est une partie de Ω telle que $\pi_r(A) = \Omega/\Omega_r$, alors il existe $r_0 | r$ avec $r_0 \leq r^\varepsilon$ et $z \in (\Pi_3 A) \cap \Omega_r$ tel que pour tout facteur premier p de r/r_0, $z \notin \Omega_{p^2}$.*

Démonstration. On peut supposer que tous les facteurs premiers de r sont assez grands pour que le lemme 17 soit valable. Soient alors x et y deux variables aléatoires indépendantes de loi uniforme sur Ω/Ω_r, et $\psi\colon \Omega/\Omega_r \to A$ une section de la projection naturelle $\Omega \to \Omega/\Omega_r$. Par le lemme 17,

$$\begin{aligned}
&\mathbb{E}\left[\sum_{p|r} (\log p)\mathbb{1}_{\{\psi(xy)=\psi(x)\psi(y) \bmod p^2\}}\right] \\
&\quad = \sum_{p|r} (\log p)\mathbb{P}[\psi(xy) = \psi(x)\psi(y) \bmod p^2] \\
&\quad \leq \sum_{p|r} (\log p)p^{-\sigma} \leq \varepsilon \sum_{p|r} \log p = \varepsilon \log r,
\end{aligned}$$

et il doit exister x et y tels que

$$\sum_{p|r} (\log p)\mathbb{1}_{\{\psi(xy)\equiv\psi(x)\psi(y) \bmod p^2\}} \leq \varepsilon \log r.$$

L'élément $z = \psi(xy)\psi(y)^{-1}\psi(x)^{-1}$ et l'entier $r_0 = \prod_{p|r : z \in \Omega_{p^2}} p$ vérifient toutes les conditions requises. ∎

4. Expansion via la représentation adjointe

Outre les résultats de Salehi Golsefidy et Varjú [21] sur la propriété du trou spectral modulo un entier sans facteur carré, l'ingrédient principal dans la démonstration de la proposition 5 est un résultat d'équidistribution quantitative des marches aléatoires linéaires sur le tore. Il sera utilisé pour démontrer la proposition 19 ci-dessous, qui sera ensuite appliquée dans la représentation adjointe de G.

4.1. Représentations linéaires et répartition modulo q. Nous considérons une représentation irréductible V définie sur $\mathbb{Q}$ de l'adhérence de Zariski de Γ, et fixons un réseau rationnel $V(\mathbb{Z})$ dans V stable par Γ. Cela est possible, d'après Borel [5, Corollaire 7.13], car par hypothèse $\Gamma \subset G \cap \mathrm{SL}_d(\mathbb{Z})$ est inclus dans un sous-groupe arithmétique de G. Pour comprendre la répartition de la marche aléatoire induite sur V modulo un entier arbitraire, nous noterons, pour une partie $X \subset V(\mathbb{Z})$ et $q \in \mathbb{N}^*$,

$$N(X, q) = \operatorname{card} \pi_q(X),$$

où $\pi_q \colon V(\mathbb{Z}) \to V(\mathbb{Z})/qV(\mathbb{Z})$ est la projection naturelle. Nous utiliserons aussi les notations usuelles de combinatoire additive : pour un entier $C \geq 1$ et une partie $X \subset V(\mathbb{Z})$,

$$\sum_C X = X + \cdots + X = \{v_1 + \cdots + v_C \mid \forall i,\ v_i \in X\},$$

et pour $A \subset \Gamma$ et un vecteur $v \in V$,

$$A \cdot v = \{a \cdot v \mid a \in A\}.$$

Enfin, pour $q \in \mathbb{N}^*$ et $v \in V(\mathbb{Z})$ on note $\operatorname{pgcd}(q, v)$ le plus grand diviseur commun entre l'entier q et le vecteur v. (Un entier d est dit diviseur de $v \in V(\mathbb{Z})$ si $\frac{v}{d} \in V(\mathbb{Z})$.)

Proposition 19 (Action sur une représentation irréductible). *Soit μ une probabilité sur $\mathrm{SL}_d(\mathbb{Z})$, Γ le sous-groupe engendré par μ, G l'adhérence de Zariski de Γ, et V une $\mathbb{Q}$-représentation non triviale de G. On suppose que*

(1) $\exists \eta > 0 : \int \|g\|^\eta \mu(\mathrm{d}g) < +\infty$;

(2) *G est connexe pour la topologie de Zariski ;*

(3) *l'algèbre engendrée par $G(\mathbb{R})$ dans $\mathrm{End}(V(\mathbb{R}))$ est égale à $\mathrm{End}(V(\mathbb{R}))$.*

On note $V(\mathbb{Z})$ un réseau de $V(\mathbb{R})$ stable sous l'action de Γ. Il existe une constante $C > 0$ telle que pour tout $\varepsilon > 0$ suffisamment petit, l'énoncé suivant soit vérifié pour tout entier q suffisamment grand.

Soit $A \subset \Gamma$ un ensemble tel que

$$\mu^{*n}(A) \geq q^{-\varepsilon} \quad \textit{pour un certain } n \geq C \log q.$$

Pour tout vecteur non nul $v \in V(\mathbb{Z})$,

$$N\left(\sum_C A \cdot v, q\right) \geq q^{-C\varepsilon}\left(\frac{q}{\operatorname{pgcd}(q, v)}\right)^{\dim V}.$$

Remarque. L'hypothèse que $G(\mathbb{R})$ engendre $\mathrm{End}(V)$ implique en particulier que Γ agit irréductiblement sur $V(\mathbb{R})$. Cependant, la réciproque n'est pas vraie, comme le montre l'exemple de $\mathrm{SL}_{d/2}(\mathbb{Z}[i])$, qui agit irréductiblement sur $\mathbb{R}^d \simeq \mathbb{C}^{d/2}$. De plus, cette proposition est fausse en général si l'on suppose seulement que $V(\mathbb{R})$ est irréductible.

Pour la démonstration de cette proposition, nous aurons besoin du théorème d'équidistribution quantitative des marches aléatoires linéaires sur le tore, que nous rappelons ci-dessous. Avec une hypothèse supplémentaire de proximalité, ce résultat est dû à Bourgain, Furman, Lindenstrauss et Mozes [9] ; les modifications nécessaires à leur démonstration pour lever cette hypothèse sont détaillées dans [23], d'où est tiré l'énoncé ci-dessous. Dans la suite, étant donné un entier $d \geq 2$, on note $\mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$ le tore de dimension d. Si ν est une mesure borélienne finie sur $\mathbb{T}^d$, ses coefficients de Fourier sont indexés par $a \in \mathbb{Z}^d$, et donnés par la formule

$$\hat{\nu}(a) = \int_{\mathbb{T}^d} e^{2i\pi\langle a,x\rangle} \nu\,(\mathrm{d}x).$$

Théorème 20 (Équirépartition des marches aléatoires sur $\mathbb{T}^d$). *Soit μ une probabilité sur $\mathrm{SL}_d(\mathbb{Z})$, Γ le sous-groupe engendré par le support de μ, et λ_1 le premier exposant de Liapounoff de μ. On suppose que*

(1) $\exists \eta > 0 : \int \|g\|^\eta \mu\,(\mathrm{d}g) < +\infty$;

(2) *Γ agit irréductiblement sur $\mathbb{R}^d$;*

(3) *l'adhérence de Zariski de Γ est connexe.*

Pour tout $\lambda \in]0, \lambda_1[$, il existe une constante $C > 0$ telle que, pour tout $t \in]0, \frac{1}{2}[$ et tout $x \in \mathbb{T}^d$, s'il existe $a \in \mathbb{Z}^d \setminus \{0\}$ tel que

$$|\widehat{\mu^{*n} * \delta_x}(a)| \geq t \quad \textit{avec } n \geq C \log \frac{\|a\|}{t},$$

alors il existe $q \in \mathbb{N}$ et $x' \in (\frac{1}{q}\mathbb{Z}^d/\mathbb{Z}^d)$ tels que

$$q \leq \left(\frac{\|a\|}{t}\right)^C \quad \textit{et} \quad d(x, x') \leq e^{-\lambda n}.$$

Ce théorème implique une décroissance de Fourier pour les marches aléatoires dont le point de départ est rationnel, et c'est sous cette forme qu'il nous sera utile. Le corollaire suivant et sa démonstration sont tirés de l'article de Bourgain et Varjú [16, Lemma 7].

Corollaire 21 (Décroissance de Fourier des marches rationnelles). *Soit μ une probabilité sur $\mathrm{SL}_d(\mathbb{Z})$ et Γ le sous-groupe engendré par μ. On suppose que*

(1) $\exists \eta > 0 : \int \|g\|^\eta \mu(\mathrm{d}g) < +\infty$;

(2) *la sous-algèbre engendrée par Γ est égale à $M_d(\mathbb{R})$;*

(3) *l'adhérence de Zariski de Γ est connexe.*

Il existe alors des constantes $C,\ \tau > 0$ telles que, pour tout $x_0 = \frac{p_0}{q_0} \in \mathbb{Q}^d/\mathbb{Z}^d$ avec $\mathrm{pgcd}(p_0, q_0) = 1$,

$$\forall n \geq C \log q_0,\ \forall b \in \mathbb{Z}^d, \quad |\widehat{\mu^{*n} * \delta_{x_0}}(b)| \leq \left(\frac{q_0}{\mathrm{pgcd}(q_0, b)}\right)^{-\tau}.$$

Démonstration. Si $q_0 = dq_1$ et $b = db'$ pour un certain entier d, alors, avec $x_1 = \frac{p_0}{q_1}$,

$$\widehat{\mu^{*n} * \delta_{x_0}}(b) = \widehat{\mu^{*n} * \delta_{x_1}}(b')$$

de sorte qu'il suffit de démontrer le théorème dans le cas où $\mathrm{pgcd}(q_0, b) = 1$, ce que nous supposerons dorénavant. Notons $E = M_d(\mathbb{R})$ et E^* l'espace des formes linéaires sur E. Dans E^*, nous considérons l'ensemble $E^*(\mathbb{Q})$ des formes linéaires à coefficients rationnels dans la base canonique, et le réseau $E^*(\mathbb{Z})$ constitué des formes linéaires $\phi \in E^*(\mathbb{R})$ telles que $\phi(M_d(\mathbb{Z})) \subset \mathbb{Z}$. Soit $\widetilde{x}_0$ un relevé de x_0 dans $\mathbb{R}^d$, et ϕ_0 l'image dans $E^*/E^*(\mathbb{Z})$ de la forme linéaire $g \in E \mapsto \langle b, g\widetilde{x}_0\rangle \in \mathbb{R}$ où $\langle \cdot, \cdot \rangle$ désigne le produit scalaire usuel sur $\mathbb{R}^d$.

Notons L (resp. R) l'application $E \to \mathrm{End}(E^*)$; $g \mapsto L_g$ définie par

$$\forall \phi \in E^*, \quad L_g(\phi)(u) = \phi(gu) \qquad (\text{resp. } R_g(\phi)(u) = \phi(ug))$$

et posons

$$\widetilde{\mu} = \frac{1}{2}(L_*\mu + R_*\mu).$$

Pour $g \in \mathrm{SL}_d(\mathbb{Z})$, L_g est inversible et préserve le réseau $E^*(\mathbb{Z})$ donc agit sur le tore $E^*/E^*(\mathbb{Z})$. Nous allons appliquer le théorème 20 à la marche aléatoire sur le tore $E^*/E^*(\mathbb{Z})$ associée à la loi de transition $\widetilde{\mu}$ et au point de départ ϕ_0. Les coefficients de Fourier sur $E^*/E^*(\mathbb{Z})$ sont naturellement indexés par $M_d(\mathbb{Z})$: pour une mesure ν sur $E^*/E^*(\mathbb{Z})$, et $a \in M_d(\mathbb{Z})$, on a

$$\widehat{\nu}(a) = \int_{E^*/E^*(\mathbb{Z})} e^{2\pi i \phi(a)}\, \mathrm{d}\nu(\phi).$$

Pour $n \geq 0$, le coefficient de Fourier en l'identité de la marche aléatoire est

$$\widehat{\widetilde{\mu}^{*n} * \delta_{\phi_0}}(I) = \widehat{\mu^{*n} * \delta_{x_0}}(b).$$

Remarquons que le groupe algébrique engendré par le support de $\widetilde{\mu}$, isomorphe à $G \times G$, est bien connexe, et que son action sur $E^*(\mathbb{R})$ est irréductible, car E est une algèbre simple engendrée par $G(\mathbb{R})$. L'hypothèse du moment exponentiel est aussi satisfaite pour $\widetilde{\mu}$, dès qu'elle l'est pour μ. Donc il existe une constante $C \geq 0$ telle que si pour $t \in]0, 1/2[$ et $n \geq C \log t$,

$$|\widehat{\widetilde{\mu}^{*n} * \delta_{\phi_0}}(I)| \geq t,$$

alors il existe un élément $\phi \in E^*(\mathbb{Q})/E^*(\mathbb{Z})$ de dénominateur au plus t^{-C} et tel que

$$\|\phi_0 - \phi\| < e^{-n\frac{\lambda_1}{2}}. \tag{4.1}$$

Posons $t = q_0^{-\frac{1}{2C}}$. Supposons $n \geq (4 \log q_0)/\lambda_1$ et donc $e^{-n\frac{\lambda_1}{2}} \leq q_0^{-2}$. Comme ϕ_0 admet un coefficient rationnel réduit de dénominateur q_0, il n'existe pas d'élément de $E^*(\mathbb{Q})$ de hauteur au plus $t^{-C} = q_0^{\frac{1}{2}}$ satisfaisant (4.1). Ainsi, si $n \geq (4 \log q_0)/\lambda_1$, on trouve bien

$$|\widehat{\mu^{*n} * \delta_{x_0}}(b)| = |\widehat{\widetilde{\mu}^{*n} * \delta_{\phi_0}}(I)| < t = q_0^{-\frac{1}{2C}}.$$

Quitte à remplacer C par $\max(C, 4/\lambda_1)$, cela montre le corollaire, avec $\tau = 1/2C$. ∎

Démonstration de la proposition 19. Fixons une $\mathbb{Z}$-base de $V(\mathbb{Z})$ qui permet d'identifier $V(\mathbb{Z})$ à $\mathbb{Z}^d$, et de définir un produit scalaire $\langle \cdot, \cdot \rangle$ sur V. Quitte à remplacer v par $v/\mathrm{pgcd}(q, v)$, on peut supposer que $\mathrm{pgcd}(q, v) = 1$. D'après le corollaire 21 appliqué à l'action de Γ sur $V(\mathbb{R})/V(\mathbb{Z})$ et au point

$$x_0 = \frac{v}{q} \bmod V(\mathbb{Z}) \in V(\mathbb{R})/V(\mathbb{Z}),$$

il existe deux constantes $C \geq 0$ et $\tau > 0$ telles que pour tout $n \geq C \log q$,

$$\forall b \in V(\mathbb{Z}), \quad |\widehat{\mu^{*n} * \delta_{x_0}}(b)| \leq \left(\frac{q}{\mathrm{pgcd}(q, b)}\right)^{-\tau}. \tag{4.2}$$

Remarquons que la mesure $\mu^{*n} * \delta_{x_0}$ est supportée par $\frac{1}{q}V(\mathbb{Z})/V(\mathbb{Z})$ qui est en bijection avec $V(\mathbb{Z})/qV(\mathbb{Z})$. Nous allons utiliser l'analyse de Fourier sur le groupe additif $V(\mathbb{Z})/qV(\mathbb{Z})$. L'application $b \mapsto (x \mapsto e^{2i\pi\frac{\langle b, x\rangle}{q}})$ identifie $V(\mathbb{Z})/qV(\mathbb{Z})$ avec son groupe dual. Notons ν l'image de μ^{*n} dans $V(\mathbb{Z})/qV(\mathbb{Z})$ par l'application

$$\begin{aligned} \Gamma &\to V(\mathbb{Z})/qV(\mathbb{Z}), \\ g &\mapsto g \cdot v \bmod qV(\mathbb{Z}). \end{aligned}$$

L'inégalité (4.2) est alors équivalente à

$$\forall b \in V(\mathbb{Z})/V(q\mathbb{Z}), \quad |\widehat{\nu}(b)| \leq \left(\frac{q}{\operatorname{pgcd}(q,b)}\right)^{-\tau}.$$

Quitte à augmenter C, nous pouvons supposer $C \geq (\dim V)/\tau$, et si $\nu^{(C)}$ désigne la C-ième convolution additive de ν, on a alors

$$\forall b \in V(\mathbb{Z})/qV(\mathbb{Z}), \quad |\widehat{\nu^{(C)}}(b)| \leq \left(\frac{q}{\operatorname{pgcd}(q,b)}\right)^{-\dim V},$$

et par la formule de Parseval dans le groupe $V(\mathbb{Z})/qV(\mathbb{Z})$,

$$\begin{aligned}\|\nu^{(C)}\|_2^2 &= \frac{1}{|V(\mathbb{Z})/qV(\mathbb{Z})|} \sum_{b \in V(\mathbb{Z}/q\mathbb{Z})} |\widehat{\nu^{(C)}}(b)|^2 \\ &\ll q^{-\dim V} \sum_{r|q} r^{\dim V} r^{-2\dim V} \ll q^{-\dim V}.\end{aligned}$$

Comme $\mu^{*n}(A) \geq q^{-\varepsilon}$, on a aussi $\nu^{(C)}(\Sigma_C A \cdot v) \geq q^{-O(\varepsilon)}$, et avec l'inégalité de Schwarz,

$$N(\Sigma_C A \cdot v, q) \geq q^{-O(\varepsilon)} q^{\dim V}. \qquad \blacksquare$$

4.2. Représentation adjointe. Nous appliquons maintenant les résultats du paragraphe précédent dans la représentation adjointe de G, pour en déduire un résultat d'expansion qui nous permettra, plus tard, de démontrer la proposition 5.

Rappelons que μ est une probabilité à support fini sur $\mathrm{SL}_d(\mathbb{Z})$, Γ le sous-groupe engendré par le support de μ, G l'adhérence de Zariski de Γ, et Ω l'adhérence de Γ dans $\mathrm{SL}_d(\widehat{\mathbb{Z}})$. On suppose de plus que G est un groupe simple, connexe et simplement connexe.

Dorénavant, le nombre q s'écrira $q = \prod_p p^{m_p}$. Dans la suite, la variable utilisée dans les produits $\prod$ est toujours p, et elle parcourt l'ensemble des nombres premiers vérifiant la condition précisée en-desous du symbole. On omettra la condition « p facteur premier de q », qui sera implicite dans cette notation. Pour tout ensemble I de nombres premiers, nous noterons

$$q_I = \prod_{p \in I} p^{m_p}.$$

De plus, si $x \in \mathfrak{gl}_d(\widehat{\mathbb{Z}})$ et p est un nombre premier, nous noterons $v_p(x)$ la valuation p-adique de x, i.e., le plus grand entier n tel que $p^{-n}x \in \mathfrak{gl}_d(\widehat{\mathbb{Z}})$. Enfin, pour $a, g \in \mathrm{SL}_d(\widehat{\mathbb{Z}})$, on note $\iota(a) \cdot g = aga^{-1}$; ainsi donc, pour $A \subset \mathrm{SL}_d(\widehat{\mathbb{Z}})$,

$$\iota(A) \cdot g = \{aga^{-1} \mid a \in A\}.$$

La proposition 22 ci-dessous exprime que si $g \in \Omega$ et $A \subset \Omega$ est tel que $\mu^{*n}(A) \geq q^{-\varepsilon}$, alors l'action par conjugaison de A sur l'élément g permet d'obtenir, en un nombre fini de produits, une part importante du plus petit sous-groupe de congruence contenant g. Sa démonstration occupera le restant de ce paragraphe. Ci-dessous, on utilise le symbole de Kronecker

$$\delta_2(p) = \begin{cases} 1 & \text{si } p = 2, \\ 0 & \text{sinon.} \end{cases}$$

Proposition 22. *Étant donné $\delta > 0$, il existe $C \geq 0$ tel que l'assertion suivante soit vraie pour tout $\varepsilon > 0$ suffisamment petit. Soit $g \in \Omega$ et I un ensemble de nombres premiers tel que*

$$\forall p \in I, \quad v_p(g-1) \geq \max\{1 + \delta_2(p), \lfloor \delta m_p \rfloor\}.$$

Si $A \subset \Omega$ vérifie $\mu^{*n}(A) \geq q^{-\varepsilon}$ pour $n \geq C \log q$, alors

$$N\big(\Pi_C(\iota(A) \cdot g), q_I\big) \geq q^{-O(\varepsilon)} \left(\frac{q_I}{\operatorname{pgcd}(q_I, g-1)} \right)^{\dim G}.$$

Démonstration. On a $g \in \Omega_{\dot{r}_I}$ où $\dot{r}_I = \prod_{p \in I} p^{1+\delta_2(p)}$. Soit $\mathfrak{g}$ l'algèbre de Lie de G et $\mathfrak{g}(\mathbb{Z}) = \mathfrak{g} \cap \mathfrak{gl}_d(\mathbb{Z})$. Par les lemmes B.3 et B.4, on peut écrire

$$g = \exp(x) \bmod q,$$

avec $x \in \mathfrak{g}(\mathbb{Z})$ satisfaisant

$$\forall p \in I, \quad v_p(x) = v_p(g-1).$$

En particulier,

$$\dot{r}_I | x \quad \text{et} \quad \operatorname{pgcd}(q_I, x) = \operatorname{pgcd}(q_I, g-1).$$

Or, comme G est simple, l'action de $G(\mathbb{C})$ sur $V(\mathbb{C})$ est irréductible. Par le théorème de Burnside [8, corollaire 1, chap. 8, §4, no. 3], l'algèbre engendrée par $G(\mathbb{C})$ dans $\operatorname{End}(V(\mathbb{C}))$ est égale à $\operatorname{End}(V(\mathbb{C}))$, et cela implique que l'algèbre engendrée par $G(\mathbb{R})$ dans $\operatorname{End}(V(\mathbb{R}))$ est égale à $\operatorname{End}(V(\mathbb{R}))$. De plus, Γ préserve le réseau $\mathfrak{g}(\mathbb{Z})$. Par conséquent, on peut appliquer la proposition 19 dans la représentation adjointe $\operatorname{Ad}\colon \Gamma \to \operatorname{GL}(\mathfrak{g}(\mathbb{R}))$, pour obtenir, pour une certaine constante C_0,

$$N\big(\Sigma_{C_0}(\operatorname{Ad} A) \cdot x, q_I\big) \geq q^{-C_0\varepsilon} \left(\frac{q_I}{\operatorname{pgcd}(q_I, g-1)} \right)^{\dim G}.$$

La proposition 23 ci-dessous permet alors de conclure. ∎

Il reste à démontrer le résultat que nous avons utilisé dans la démonstration ci-dessus, qui est en fait une conséquence de la formule de Campbell–Hausdorff.

Proposition 23. *Étant donnés $C_0 \in \mathbb{N}$ et $\delta > 0$, il existe une constante $C \geq 0$ telle que l'énoncé suivant soit vérifié pour tout entier $q \in \mathbb{N}^*$, tout vecteur $x \in \mathfrak{sl}_d(\mathbb{Z})$, et toute partie finie $A \subset \mathrm{SL}_d(\mathbb{Z})$.*

Soit I un ensemble de facteurs premiers de q tel que pour tout $p \in I$, on a $v_p(x) \geq \max\{1 + \delta_2(p), \lfloor \delta m_p \rfloor\}$, alors

$$N\big(\Pi_C \iota(A) \cdot \exp(x), q_I\big) \geq \frac{1}{C} N\big(\Sigma_{C_0} \mathrm{Ad}(A) \cdot x, q_I\big).$$

Dans ce qui suit, nous écrirons e^x au lieu de $\exp(x)$. Pour $s \in \mathbb{N}^*$, le groupe libre engendré par s générateurs $a_1, \ldots, a_s$ sera noté F_s. On identifie chaque élément de F_s avec l'application de mot qu'il induit sur $\mathrm{GL}_d(\widehat{\mathbb{Z}})$. Nous noterons aussi $\mathcal{F}_s(\mathbb{Z})$ la $\mathbb{Z}$-algèbre de Lie libre engendrée par s générateurs.

Lemme 24. *Étant donnés deux entiers naturels non nuls k et s, il existe un mot $w \in F_s$ et une constante $D \in \mathbb{N}^*$ tels que pour tout $R \in \mathbb{N}^*$ vérifiant $v_2(R) \neq 1$, pour tous $x_1, \ldots, x_s$ dans $R\mathfrak{gl}_d(\widehat{\mathbb{Z}})$,*

$$e^{D(x_1 + \cdots + x_s)} \equiv w(e^{x_1}, \ldots, e^{x_s}) \bmod R^k.$$

Démonstration. Il s'agit de reprendre la démonstration de [2, Lemma 3.5], en s'assurant, quitte à ajuster la valeur des constantes pour contrôler les dénominateurs, que le reste est bien divisible par R^k.

Par le lemme chinois, il suffit de traiter le cas où R a un seul facteur premier. On pourra donc travailler sur $\mathbb{Z}_p$. Les lettres C et C' seront utilisées pour désigner des quantités dépendant seulement de k et de s, et dont la valeur peut varier d'une ligne à l'autre.

La démonstration se fait en trois étapes.

(1) Soit $k \in \mathbb{N}^*$ et $w \in F_s$. Il existe $C \in \mathbb{N}^*$ et un élément $\mathsf{r} \in \mathcal{F}_s(\mathbb{Z})$ de degré strictement inférieur à k telle que pour tous $x_1, \ldots, x_s \in R\mathfrak{gl}_d(\widehat{\mathbb{Z}})$,

$$w(e^{Cx_1}, \ldots, e^{Cx_s}) \equiv e^{\mathsf{r}(x_1, \ldots, x_s)} \bmod R^k.$$

Cela se voit par récurrence sur la longueur du mot. Le résultat est trivial pour le mot vide, de longueur nulle. Supposons le résultat connu pour tous les mots de longueur au plus ℓ. Soit w' un mot de longueur $\ell + 1$. Pour un certain j, $w' = a_j w$, avec w de longueur ℓ. L'hypothèse de récurrence permet d'écrire, pour tous $x_1, \ldots, x_s \in R\mathfrak{gl}_d(\widehat{\mathbb{Z}})$, $w(e^{Cx_1}, \ldots, e^{Cx_s}) \equiv e^{\mathsf{r}(x_1, \ldots, x_s)} \bmod R^k$. Alors, quitte à ajuster la valeur de C, avec

la formule de Campbell–Hausdorff,

$$\begin{aligned} w'(e^{C^2x_1},\dots,e^{C^2x_s}) &\equiv e^{C^2x_j}\, w(e^{C^2x_1},\dots,e^{C^2x_s}) \\ &\equiv e^{C^2x_j}\, e^{\mathsf{r}(Cx_1,\dots,Cx_s)} \\ &\equiv e^{\mathsf{r}'(x_1,\dots,x_s)+U} \bmod R^k \end{aligned}$$

avec $U \equiv 0 \bmod R^k$. (La constante C permet d'absorber les dénominateurs qui apparaissent dans le reste de la formule de Campbell–Hausdorff, cf. Serre [33, p. 29].) Grâce au lemme B.1, on trouve donc bien

$$w'(e^{C'x_1},\dots,e^{C'x_s}) \equiv e^{\mathsf{r}'(x_1,\dots,x_s)} \bmod R^k.$$

(2) Remarquons que si $x_1,\dots,x_k$ sont dans $R\mathfrak{gl}_d(\widehat{\mathbb{Z}})$, alors

$$e^{[Cx_1,[\dots,[Cx_{k-1},Cx_k]\dots]]} \equiv [e^{Cx_1},[\dots,[e^{Cx_{k-1}},e^{Cx_k}]\dots]]] \bmod R^{k+1}.$$

Cela se voit par récurrence, avec la formule de Campbell–Hausdorff. (Ici encore, il faut contrôler les dénominateurs qui apparaissent dans le reste, d'où la constante C.) Par suite, utilisant encore la formule de Campbell–Hausdorff, si r_k est un élément de $\mathcal{F}_s(\mathbb{Z})$ homogène de degré k on peut écrire, pour $x_1,\dots,x_s$ dans $R\mathfrak{gl}_d(\widehat{\mathbb{Z}})$,

$$e^{\mathsf{r}_k(Cx_1,\dots,Cx_s)} \equiv u(e^{x_1},\dots,e^{x_s}) \bmod R^{k+1}. \tag{4.3}$$

Le mot u est obtenu comme le produit des commutateurs constituant r_k.

(3) On construit par récurrence sur k un mot w_k et une constante $C = C_k$ tels que pour tous $x_1,\dots,x_s \in R\mathfrak{gl}_d(\widehat{\mathbb{Z}})$,

$$e^{C(x_1+\cdots+x_s)} \equiv w_k(e^{x_1},\dots,e^{x_s}) \bmod R^k. \tag{4.4}$$

Supposons construit le mot w_k satisfaisant (4.4). D'après le point (1), nous pouvons écrire, pour $\mathsf{r} \in \mathcal{F}_s$ de degré inférieur à k,

$$w_k(e^{Cx_1},\dots,e^{Cx_s}) \equiv e^{\mathsf{r}(x_1,\dots,x_s)} \bmod R^{k+1}.$$

Comme $w_k(e^{Cx_1},\dots,e^{Cx_s}) \equiv e^{C^2(x_1+\cdots+x_s)} \bmod R^k$, on a naturellement

$$\mathsf{r}(x_1,\dots,x_s) = C^2(x_1+\cdots+x_s) + \mathsf{r}_k(x_1,\dots,x_s),$$

où $\mathsf{r}_k \in \mathcal{F}_s(\mathbb{Z})$ est un élément homogène de degré k. D'après (4.3), il existe un mot u tel que $e^{-\mathsf{r}_k(Cx_1,\dots,Cx_s)} = u(e^{x_1},\dots,e^{x_s}) \bmod R^{k+1}$ et par suite

$$\begin{aligned} e^{C'(x_1+\cdots+x_s)} &= e^{\mathsf{r}(Cx_1,\dots,Cx_s)-\mathsf{r}_k(Cx_1,\dots,Cx_s)} \\ &\equiv e^{\mathsf{r}(Cx_1,\dots,Cx_s)} e^{-\mathsf{r}_k(Cx_1,\dots,Cx_s)} \\ &\equiv w_k(e^{C^2x_1},\dots,e^{C^2x_s})u(e^{x_1},\dots,e^{x_s}) \bmod R^{k+1}, \end{aligned}$$

ce qu'il fallait démontrer. ∎

Nous pouvons maintenant démontrer la proposition 23.

Démonstration de la proposition 23. Soit $k = \lceil 2/\delta \rceil$ et

$$R = \prod_{p \in I} p^{\max\{1+\delta_2(p), \lfloor \delta m_p \rfloor\}},$$

de sorte que $R | X$ et $q_I | R^k$. D'après le lemme 24 il existe une constante $D \in \mathbb{N}^*$ et un mot $w \in F_{C_0}$ tels que pour tous $x_1, \dots, x_{C_0}$ dans $R\mathfrak{sl}_d(\widehat{\mathbb{Z}})$,

$$e^{D(x_1+\cdots+x_{C_0})} \equiv w(e^{x_1}, \dots, e^{x_{C_0}}) \bmod q_I.$$

Cette égalité vaut en particulier si $x_i = \mathrm{Ad}(a_i) \cdot x$, avec $a_i \in A$. Mais on a $e^{x_i} = \iota(a_i) \cdot e^x$ et par conséquent, si C désigne la longueur du mot w,

$$\exp(D\Sigma_{C_0} \mathrm{Ad}(A) \cdot x) \subset \Pi_C(\iota(A) \cdot e^x) \bmod q_I.$$

Avec le lemme B.3, on trouve bien

$$\begin{aligned} N\left(\Sigma_{C_0} \mathrm{Ad}(A) \cdot x, q_I\right) &\ll_D N\left(D\Sigma_{C_0} \mathrm{Ad}(A) \cdot x, q_I\right) \\ &= N\left(\exp(D\Sigma_{C_0} \mathrm{Ad}(A) \cdot x), q_I\right) \\ &\leq N\left(\Pi_C(\iota(A) \cdot e^x), q_I\right). \end{aligned}$$

Cela conclut la démonstration de la proposition puisque D ne dépend que de C_0 et de δ. ∎

5. Croissance des ensembles de grande μ^{*n}-masse

Nous voulons maintenant conclure la démonstration de la proposition 5. Grâce aux résultats des parties 3 et 4, le problème se ramène à la construction d'un élément g dans un ensemble produit A^C qui satisfait certaines congruences. Pour cela, l'instrument principal est la propriété presque diophantienne de μ^{*n}, mais la mise en place des différents paramètres est subtile. Nous reprenons en grande partie l'argument de Bourgain et Varjú [16, §5], avec quelques changements notables.

Dans toute la suite, μ désigne une probabilité symétrique à support fini sur $\mathrm{SL}_d(\mathbb{Z})$, Γ le sous-groupe engendré par le support de μ, G l'adhérence de Zariski de Γ dans $\mathrm{SL}_d(\mathbb{Z})$, et Ω l'adhérence de Γ dans le groupe profini $\mathrm{SL}_d(\widehat{\mathbb{Z}})$. Le groupe algébrique G est supposé simple, connexe, et simplement connexe. On note q un entier arbitraire, dont la décomposition en facteurs premiers s'écrit

$$q = \prod_p p^{m_p},$$

et r son radical :

$$r = \prod_{p|q} p.$$

Pour tout ensemble de nombres premiers I, nous noterons

$$q_I = \prod_{p\in I} p^{m_p} \quad \text{et} \quad r_I = \prod_{p\in I} p.$$

5.1. Les conditions de congruences. Les conditions de divisibilité convenables pour l'élément g recherché sont celles de la proposition ci-dessous, qui sera démontrée dans les paragraphes suivants.

Proposition 25. *Étant donné $\tau > 0$, il existe des constantes $C > 1$ et $\delta > 0$ telles que l'assertion suivante soit vraie pour tout entier naturel q suffisamment grand. Si $n \geq C \log q$, et $A \subset \mathrm{SL}_d(\mathbb{Z})$ est une partie symétrique vérifiant $\mu^{*n}(A) \geq q^{-\delta}$, alors il existe $g \in \Pi_C A$ vérifiant*

$$\mathrm{pgcd}(q, g-1) \leq q^{O(\tau)} r \tag{5.1}$$

et

$$q_I \geq q^{1-O(\tau)} \tag{5.2}$$

avec

$$I = \big\{p \mid v_p(g-1) \geq \max\{1, \lfloor \delta m_p \rfloor\}\big\}.$$

Admettant ce résultat pour le moment, nous pouvons aisément démontrer la proposition 5.

Démonstration de la proposition 5. Soit $g \in \Pi_C A$ et I l'ensemble de premiers donnés par la proposition 25. Si $2 \in I$ et $\delta m_2 < 2$, on peut remplacer I par $I \setminus \{2\}$ pour avoir

$$\forall p \in I, \quad v_p(g-1) \geq \max\{1 + \delta_2(p), \lfloor \delta m_p \rfloor\},$$

tout en gardant les conditions (5.1) et (5.2), si q est suffisamment grand. La proposition 22, le lemme B.3 et le lemme B.4 nous donnent alors

$$N\big(\Pi_C(\iota(A)\cdot g), q_I\big) \geq q^{-O(\tau)} \Big(\frac{q_I}{r_I}\Big)^{\dim G} \geq q^{-O(\tau)} N(\Omega_{r_I}, q_I).$$

Or, $\Pi_C(\iota(A)\cdot g) \subset (\Pi_{C'} A) \cap \Omega_{r_I}$, car $g \in (\Pi_C A) \cap \Omega_{r_I}$. Quitte à ajuster la valeur de C, on trouve donc

$$N\big((\Pi_C A) \cap \Omega_{r_I}, q_I\big) \geq q^{-O(\tau)} N(\Omega_{r_I}, q_I).$$

Mais d'autre part, comme r_I est sans facteur carré, d'après le lemme 14,

$$N(\Pi_C A, r_I) \geq q^{-O(\varepsilon)} N(\Omega, r_I).$$

Mis bout à bout, cela montre

$$\begin{aligned} N(\Pi_{2C} A, q_I) &\geq N(\Pi_C A, r_I) N((\Pi_C A) \cap \Omega_{r_I}, q_I) \\ &\geq q^{-O(\tau)} N(\Omega, r_I) N(\Omega_{r_I}, q_I) \\ &\geq q^{-O(\tau)} N(\Omega, q_I), \end{aligned}$$

Comme $q_I \geq q^{1-O(\tau)}$, et donc $N(\Omega, q_I) \geq q^{-O(\tau)} N(\Omega, q)$, cela démontre la proposition 5. ∎

5.2. Propriété presque diophantienne. Pour démontrer la proposition 25, nous utiliserons une propriété importante de non concentration pour la loi μ^{*n} de la marche aléatoire au temps n.

Proposition 26 (Propriété presque diophantienne). *Soit μ une probabilité symétrique sur $\mathrm{SL}_d(\mathbb{Z})$ dont le support est fini et engendre un sous-groupe Γ non moyennable. Il existe des constantes $C \geq 0$ et $c > 0$ telles que pour tout entier $q \in \mathbb{N}^*$,*

$$\forall n \geq C \log q, \quad \mu^{*n}(\Omega_q) \leq C q^{-c}.$$

Démonstration. Comme Γ est non moyennable, il existe $c' > 0$ tel que

$$\forall n \geq 1, \quad \max_{g \in \Gamma} \mu^{*n}(g) \ll e^{-c'n}.$$

Posons

$$M = \max_{g \in \mathrm{Supp}(\mu)} \|g\| \quad \text{et} \quad m = \left\lfloor \frac{\log q}{2 \log M} \right\rfloor.$$

Nous avons, pour tout $g \in \mathrm{Supp}(\mu^{*2m})$, $\|g\| < q$. Donc $\mathrm{Supp}(\mu^{*2m}) \cap \Omega_q = \{1\}$ et par conséquent, pour tout $g \in \Gamma$, $\mathrm{Supp}(\mu^{*m}) \cap g\Omega_q$ contient au plus un élément. Par suite,

$$\sup_{g \in \Gamma} \mu^{*m}(g\Omega_q) \leq \max_{g \in \Gamma} \mu^{*m}(g) \ll e^{-c'm} \ll q^{-c}$$

avec $c = c'/(2 \log M)$. Enfin, pour tout entier $n \geq m$,

$$\begin{aligned} \mu^{*n}(\Omega_q) &= \sum_{g \in \Gamma} \mu^{*(n-m)}(g^{-1}) \mu^{*m}(g\Omega_q) \\ &\leq \sup_{g \in \Gamma} \mu^{*m}(g\Omega_q) \ll q^{-c}. \end{aligned}$$

∎

Pour $\delta \in]0,1[$, nous noterons

$$q_\delta = \prod p^{\lfloor \delta m_p \rfloor}.$$

À l'aide de la propriété presque diophantienne, il est facile de trouver un élément $g \in \Pi_C A$ vérifiant (5.1) et $q_\delta | g-1$ au lieu de (5.2).

Lemme 27. *Étant donné $\tau > 0$, il existe des constantes $C, \delta > 0$ telles que l'assertion suivante soit vraie. Si $n \geq C \log q$ et $A \subset \mathrm{SL}_d(\mathbb{Z})$ est une partie symétrique vérifiant $\mu^{*n}(A) \geq q^{-\delta}$, alors il existe un élément $g_0 \in AA$ tel que*

$$\mathrm{pgcd}(q, g_0 - 1) \leq q^\tau \quad \textit{et} \quad q_\delta | g_0 - 1.$$

Démonstration. D'une part, par l'inégalité de Schwarz, et avec la symétrie de μ et de A,

$$\begin{aligned}
\mu^{*2n}(AA \cap \Omega_{q_\delta}) &\geq \sum_{g \in \Omega/\Omega_{q_\delta}} \mu^{*n}(A \cap g\Omega_{q_\delta})^2 \\
&\geq [\Omega : \Omega_{q_\delta}]^{-1} \Big(\sum_{g \in \Omega/\Omega_{q_\delta}} \mu^{*n}(A \cap g\Omega_{q_\delta}) \Big)^2 \\
&\geq [\Omega : \Omega_{q_\delta}]^{-1} \mu^{*n}(A)^2.
\end{aligned}$$

On majore l'indice $[\Omega : \Omega_{q_\delta}]$ simplement par $q_\delta^{d^2} \leq q^{d^2\delta}$, d'où l'on tire

$$\mu^{*2n}(AA \cap \Omega_{q_\delta}) \geq q^{-(d^2+2)\delta}.$$

D'autre part, par le lemme 26, il existe $c > 0$ dépendant seulement de μ tel que

$$\sum_{s|q \text{ et } s \geq q^\tau} \mu^{*2n}(\Omega_s) \leq \sum_{s|q \text{ et } s \geq q^\tau} s^{-c} \leq \sum_{s|q} q^{-c\tau} \leq q^{-\frac{c\tau}{2}},$$

où la dernière inégalité est valable si q est suffisamment grand, puisqu'on peut majorer le nombre D de diviseurs de $q = \prod p^{m_p}$ de la façon suivante, pour tout $\varepsilon > 0$

$$D = \prod_p (m_p + 1) \leq C_\varepsilon \prod_p p^{\varepsilon m_p} = C_\varepsilon q^\varepsilon.$$

Si $\delta > 0$ est choisi tel que $(d^2+2)\delta < c\tau/2$, l'ensemble $(AA \cap \Omega_{q_\delta}) \setminus \bigcup_{s|q \text{ et } s \geq q^\tau} \Omega_s$ est nécessairement non vide. ∎

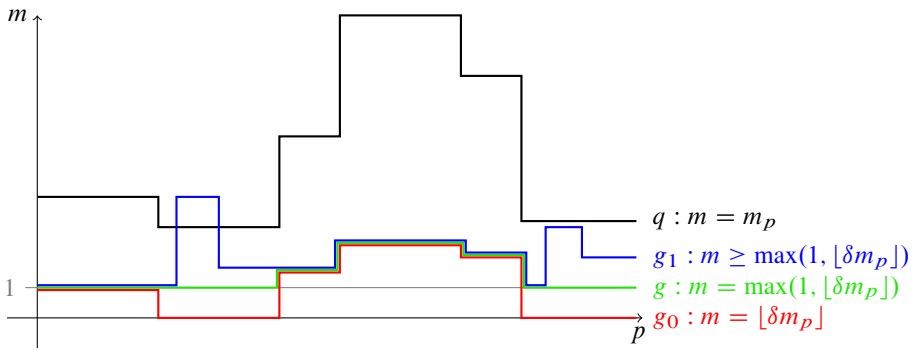


FIGURE 1
Valuations des éléments g_0, g_1, g.

5.3. Construction de l'élément g. Pour aider à la compréhension de la démonstration un peu technique qui va suivre, nous commençons par en donner une interprétation plus imagée. Pour cela, nous représentons l'entier $q = \prod p^{m_p}$ sous la forme du graphe de la fonction $p \mapsto m_p$. Le support de cette fonction est l'ensemble $\mathcal{P}$ des diviseurs premiers de q, que l'on munit de la mesure ν définie par $\nu(p) = \log p$. Ensuite, à un élément $g \in \Omega$ nous associons la fonction f définie sur $\mathcal{P}$ par $f(p) = v_p(g-1)$. En termes de la fonction f, les conditions de la proposition 25 deviennent à peu près :

(1) $\frac{2}{\delta} f(p) \geq m_p$ pour tout p hors d'un ensemble exceptionnel ${}^c I$ tel que

$$\int_{{}^c I} m_p \, \mathrm{d}\nu(p) \leq \tau \log q;$$

(Cette condition permet d'appliquer la formule de Campbell–Hausdorff à un ordre borné par $2/\delta$, en arrivant à la précision donnée par q.)

(2) $\int f(p) \, \mathrm{d}\nu(p) \leq \log r + \tau \log q = \int 1 \, \mathrm{d}\nu(p) + \tau \int m_p \, \mathrm{d}\nu(p)$. (Cela nous permet de récupérer à partir de g, via la proposition 22, la quasi-totalité de q, excepté bien sûr le radical r inaccessible par cette méthode.)

La construction de l'élément g se fait en trois étapes, illustrées dans la figure 1, et décrites grossièrement comme suit.

(a) Le lemme 27 donne l'existence d'un élément g_0 tel que la fonction f_0 associée satisfasse

$$f_0(p) \geq \lfloor \delta m_p \rfloor \quad \text{et} \quad \int f_0(p) \, \mathrm{d}\nu(p) \leq \log r + \tau \log q.$$

(b) Pour avoir la condition (1), on doit corriger g_0 aux places p où $\lfloor \delta m_p \rfloor = 0$. Cela se fait à l'aide de la proposition 13. On obtient un élément g_1 dont la fonction associée f_1 vérifie $f_1(p) = f_0(p)$ si $\delta m_p \geq 1$, et pour tout $p \in \mathcal{P}$, $f_1(p) \geq 1$.

(c) Malheureusement, en passant de g_0 à g_1 on perd la propriété

$$\int f_1(p)\,\mathrm{d}\nu(p) \leq \log r + \tau \log q.$$

Il faut donc réduire la valuation p-adique de $g_1 - 1$ aux places p telles que $\delta m_p < 1$. Cela se fait à l'aide du lemme 18, et permet d'obtenir l'élément g désiré.

Nous donnons enfin la démonstration rigoureuse de la proposition 25. Soit $\tau > 0$ fixé. La construction de g dépend de certaines quantités $\alpha > \beta > \gamma > \delta > 0$. Pour le choix de ces quantités, nous utilisons un paramètre auxiliaire $L \in \mathbb{N}$, et procédons en plusieurs étapes. Au départ, $L = 1$, et ensuite, à chaque tentative infructueuse, nous ajustons la valeur de L. Il est important de noter que si la valeur finale de L dépend de q, elle est toutefois bornée indépendamment de q.

Dans cette démonstration, C désigne une constante dépendant de μ et de τ et $A \subset \mathrm{SL}_d(\mathbb{Z})$ est une partie symétrique satisfaisant $\mu^{*n}(A) \geq q^{-\delta}$ pour un certain $n \geq C \log q$.

(1) Choisissons $\alpha > 0$ tel que $L\alpha < \tau$.

(2) Choisissons $\beta > 0$ tel que, pour $n \geq C \log q$, si $A' \subset \mathrm{SL}_d(\mathbb{Z})$ est une partie symétrique et $\mu^{*n}(A') \geq q^{-\beta}$, alors il existe $r' | r$ avec $r' \geq q^{-\alpha} r$ tel que

$$\pi_{r'}(\Pi_C A') = \Omega / \Omega_{r'}.$$

Cela est possible, d'après la proposition 13.

(3) Choisissons $\gamma > 0$ tel que si A est une partie symétrique vérifiant $\mu^{*n}(A) \geq q^{-\gamma}$, alors $\mu^{*2n}(AA \cap \Omega_{q_\gamma}) \geq q^{-\beta}$. Il suffit de prendre $\gamma = \beta/(d^2+2)$. La preuve est identique à la première moitié de la démonstration du lemme 27.

(4) Choisissons $\delta > 0$ tel qu'il existe g_0 dans AA satisfaisant $q_\delta | g_0 - 1$ tandis que $\mathrm{pgcd}(q, g_0 - 1) \leq q^{\alpha\gamma}$. Cela est possible, d'après le lemme 27 appliqué avec $\tau = \alpha\gamma$.

(5) Si $\prod_{L < m_p \leq 1/\delta} p^{m_p} \leq q^\tau$, les quantités α, β, etc. sont fixées pour le restant de la démonstration. Sinon, nous reprenons la construction ci-dessus en partant de $L = \lfloor 1/\delta \rfloor$.

Vue la condition $\prod_{L < m_p \leq 1/\delta} p^{m_p} \geq q^\tau$ obtenue en cas d'échec, le nombre de tentatives nécessaires pour conclure cette procédure est majoré, indépendamment de q, par $1/\tau$. Cela montre que la quantité finale δ est minorée par une constante indépendante de q.

Partons de l'élément g_0 obtenu au point (4), qui satisfait

$$\forall p | q, \quad v_p(g_0 - 1) \geq \lfloor \delta m_p \rfloor$$

et

$$\operatorname{pgcd}(q, g_0 - 1) \leq q^{\alpha\gamma}. \tag{5.3}$$

Nous devons en premier lieu faire en sorte que $g - 1$ soit divisible par presque tous les facteurs premiers de q, afin qu'il puisse vérifier la propriété (5.2). Avec le point (3), le point (2) appliqué à $A' = AA \cap \Omega_{q_\gamma}$ montre que l'on peut trouver $r = r'r_0$ avec $r_0 \leq q^\alpha$ tel que

$$\pi_{r'}((\Pi_C A) \cap \Omega_{q_\gamma}) = \Omega/\Omega_{r'}. \tag{5.4}$$

En particulier il existe $g_0' \in (\Pi_C A) \cap \Omega_{q_\gamma}$ tel que

$$g_0' \equiv g_0 \bmod r'.$$

Posons $g_1 = g_0' g_0^{-1}$, et montrons que g_1 satisfait

$$q_{I_1} \geq q^{1-O(\tau)}, \tag{5.5}$$

où

$$I_1 = \{p \mid v_p(g_1 - 1) \geq \max\{1, \lfloor \delta m_p \rfloor\}\}.$$

Tout d'abord, $g_1 \in \Omega_{q_\delta} \cap \Omega_{r'}$, et donc, pour tout $p|q$, $p \notin I_1$ implique $p|r_0$ et $\delta m_p < 1$, d'où

$$\frac{q}{q_{I_1}} = \prod_{p \notin I_1} p^{m_p} \leq \prod_{p|r_0 \text{ et } \delta m_p < 1} p^{m_p}.$$

En séparant les premiers p selon $m_p \leq L$ ou non, on trouve

$$\frac{q}{q_{I_1}} \leq r_0^L \prod_{L < m_p \leq 1/\delta} p^{m_p} \leq q^{L\alpha+\tau} \leq q^{O(\tau)},$$

ce qui démontre (5.5). Il ne nous resterait donc qu'à montrer l'inégalité

$$\operatorname{pgcd}(q, g_1 - 1) \leq q^{O(\tau)} r.$$

Malheureusement, l'élément g_1 n'a pas de raison de vérifier cette propriété, à cause des nombres premiers p tels que $\gamma m_p < 1$ et $v_p(g_1 - 1) \geq 2$. La suite de la démonstration a pour but de corriger g_1 en ces places ; cela va nous contraindre à un petit détour.

Soit

$$J = \{p \mid \gamma m_p \geq 1 \text{ ou } v_p(g_1 - 1) \leq 1\}.$$

Montrons que

$$\operatorname{pgcd}(q_J, g_1 - 1) \leq q^{O(\alpha)} r_J. \tag{5.6}$$

On peut écrire $J = J_1 \cup J_2 \cup J_3$ avec

$$\begin{aligned} J_1 &= \{p \mid \gamma m_p \geq 1 \text{ et } v_p(g_0 - 1) \geq \lfloor \gamma m_p \rfloor\}, \\ J_2 &= \{p \mid \gamma m_p \geq 1 \text{ et } v_p(g_0 - 1) < \lfloor \gamma m_p \rfloor\}, \\ J_3 &= \{p \mid v_p(g_1 - 1) \leq 1\}. \end{aligned}$$

Remarquons que si $\gamma m_p \geq 1$ alors $\lfloor \gamma m_p \rfloor \geq \frac{\gamma}{2} m_p$. En particulier, pour tout $p \in J_1$, $m_p \leq \frac{2}{\gamma} v_p(g_0 - 1)$. Donc, avec (5.3),

$$q_{J_1} \leq \prod_{p \in J_1} p^{\frac{2}{\gamma} v_p(g_0 - 1)} \leq \operatorname{pgcd}(q, g_0 - 1)^{\frac{2}{\gamma}} \leq q^{2\alpha}.$$

Pour tout $p \in J_2$, $v_p(g_0 - 1) < v_p(g_0' - 1)$ donc $v_p(g_1 - 1) = v_p(g_0 - 1) < \lfloor \gamma m_p \rfloor$. Donc

$$\operatorname{pgcd}(q_{J_2}, g_1 - 1) \leq q_{J_2}^{\gamma} \leq q^{\alpha}.$$

Par la définition de J_3,

$$\operatorname{pgcd}(q_{J_3}, g_1 - 1) \leq r_{J_3} \leq r_J.$$

Enfin, on trouve (5.6) en combinant les trois inégalités ci-dessus avec la suivante

$$\operatorname{pgcd}(q_J, g_1 - 1) \leq q_{J_1} \operatorname{pgcd}(q_{J_2}, g_1 - 1) \operatorname{pgcd}(q_{J_3}, g_1 - 1).$$

La proposition 22 avec (5.6) montre donc que

$$N\big(\Pi_C(\iota(A) \cdot g_1), q_J\big) \geq q^{-O(\alpha)} \Big(\frac{q_J}{r_J}\Big)^{\dim G}. \tag{5.7}$$

Par ailleurs, l'égalité (5.4) et le lemme 18 appliqué à r' montrent qu'on peut écrire $r' = r_1 r''$ avec $r_1 \leq q^{\alpha}$ tel qu'il existe g_2 dans $(\Pi_C A) \cap \Omega_{q_\gamma}$ vérifiant

$$g_2 \in \Omega_{r'} \quad \text{et} \quad \forall p | r'', \ v_p(g_2 - 1) = 1.$$

L'inégalité (5.7) permet de choisir g_3 dans $\Pi_C(\iota(A) \cdot g_1)$ tel que $g = g_2 g_3$ vérifie

$$\operatorname{pgcd}(q_J, g - 1) \leq q^{O(\alpha)} r_J.$$

En effet,

$$N\big(g_2 \Pi_C(\iota(A) \cdot g_1), q_J\big) \geq q^{-O(\alpha)} \Big(\frac{q_J}{r_J}\Big)^{\dim G},$$

tandis que pour tout entier $1 \leq s \leq q_J$,

$$N\big(\{g \in \Omega \mid \operatorname{pgcd}(g - 1, q_J) \geq s\}, q_J\big) \ll q^{o(1)} \Big(\frac{q_J}{s}\Big)^{\dim G}.$$

Par ailleurs, $p \notin J$ signifie $\gamma m_p < 1$ et $g_1 \in \Omega_{p^2}$ donc $g_3 \in \Omega_{p^2}$. Si de plus $p|r''$, alors $v_p(g_2 - 1) = 1$ donc $v_p(g - 1) = 1$. Ainsi,

$$\begin{aligned}\operatorname{pgcd}(q, g-1) &\le \operatorname{pgcd}(q_J, g-1)\Big(\prod_{p\notin J \text{ et } p|r''} p\Big)\Big(\prod_{p|r_0r_1 \text{ et } \gamma m_p<1} p^{m_p}\Big)\\ &\le q^{O(\alpha)} r_J \Big(\prod_{p\notin J \text{ et } p|r} p\Big)(r_0r_1)^L\Big(\prod_{L<m_p\le 1/\gamma} p^{m_p}\Big)\\ &\le q^{O(\alpha)} r q^{2L\alpha} q^{\tau} = q^{O(\tau)} r.\end{aligned}$$

Cela montre que x vérifie la condition (5.1).

D'autre part, on a $g_1 \in \Omega_{q_\delta} \cap \Omega_{r'}$ et $g_2 \in \Omega_{q_\gamma} \cap \Omega_{r'}$. Donc $g_3 \in \Omega_{q_\delta} \cap \Omega_{r'}$ puis $g \in \Omega_{q_\delta} \cap \Omega_{r'}$. Avec le même argument que celui pour (5.5), on montre que g vérifie la condition (5.2).

A. Approximation dans les groupes semi-simples

Nous résumons dans cet appendice les résultats obtenus par Matthews, Vaserstein et Weisfeiler [29] et Nori [30] sur l'approximation dans les groupes algébriques simples, ainsi que quelques autres propriétés que nous avons utilisées dans le corps de l'article. Étant donné un sous-groupe Γ dans $\mathrm{SL}_d(\mathbb{Z})$, on s'intéresse à son adhérence Ω dans $\mathrm{SL}_d(\widehat{\mathbb{Z}})$. Pour parler sans ambiguïté des points sur $\mathbb{Z}/q\mathbb{Z}$ de l'adhérence de Zariski de Γ, nous commençons par introduire quelques éléments de langage de la théorie des schémas en groupes.

A.1. Le schéma en groupes G. Dans l'algèbre $\mathbb{Z}[X_{11}, \dots, X_{dd}]$ des polynômes à coefficients entiers sur les matrices $d \times d$, on considère l'idéal $\mathcal{I}$ défini par

$$\mathcal{I} = \{f \in \mathbb{Z}[X_{11}, \dots, X_{dd}] \mid \forall g \in \Gamma,\ f(g) = 0\}$$

et le foncteur

$$G = \mathrm{Hom}(\mathbb{Z}[X_{ij}]/\mathcal{I}, -)$$

de la catégorie des anneaux commutatifs unifères dans la catégorie des ensembles. Si R est un anneau commutatif unifère, alors $G(R)$ est l'ensemble des morphismes d'anneau de $\mathbb{Z}[X_{ij}]/\mathcal{I}$ dans R, et si $\phi\colon R \to R'$ est un morphisme, alors $G(\phi)$ est la composition par ϕ. De manière équivalente,

$$G(R) = \{(x_{ij}) \in R^{d^2} \mid \forall f \in \mathcal{I},\ f(x_{ij}) = 0\}.$$

Évidemment, $\det(X_{ij}) - 1 \in \mathcal{I}$, et $G(R)$ peut donc être identifié à une partie de $\mathrm{SL}_d(R)$. Cette identification sera implicite dans la suite. De l'hypothèse que Γ est un sous-groupe

de $\mathrm{SL}_d(\mathbb{Z})$, on peut déduire que pour tout R, $G(R)$ est un sous-groupe de $\mathrm{SL}_d(R)$. On peut alors voir G comme un foncteur de la catégorie des anneaux commutatifs unifères dans la catégorie des groupes. Comme G est de plus représentable – représenté par $\mathbb{Z}[X_{ij}]/\mathcal{I}$ – c'est un schéma en groupes affine sur $\mathbb{Z}$.

L'extension de base $\mathbb{Z} \to \mathbb{Q}$ permet d'obtenir à partir de G un schéma en groupes affine sur $\mathbb{Q}$,

$$G_{\mathbb{Q}} = \mathrm{Hom}\big((\mathbb{Z}[X_{ij}]/\mathcal{I}) \otimes_{\mathbb{Z}} \mathbb{Q}, -\big),$$

qu'on appelle la *fibre générique de* G. Le schéma $G_{\mathbb{Q}}$ est en fait une variété, qui coïncide avec la clôture de Zariski de Γ dans SL_d. Suivant la terminologie de Borel [6], nous dirons que $G_{\mathbb{Q}}$ est un $\mathbb{Q}$-groupe. La dimension de $G_{\mathbb{Q}}$ est simplement égale à la dimension de la variété $G_{\mathbb{Q}}$.

Si l'anneau R est muni d'une topologie, nous munirons $G(R)$ de la topologie induite par la topologie produit sur l'espace de matrices $M_d(R)$. Pour un nombre premier p, $G(\mathbb{Q}_p)$ est alors un sous-groupe fermé du groupe analytique $\mathrm{SL}_d(\mathbb{Q}_p)$, donc un sous-groupe analytique par le théorème de Cartan [33, Part II, Chap. V, §9]. Notons aussi que $G(\mathbb{Z}_p)$ est un sous-groupe ouvert dans $G(\mathbb{Q}_p)$.

A.2. L'algèbre de Lie. Au schéma en groupes G est associée une algèbre de Lie sur $\mathbb{Z}$, notée $\mathfrak{g}(\mathbb{Z})$. Nous rappelons les grandes lignes de cette construction, et renvoyons par exemple au livre [36, Chapter 12] de Waterhouse pour plus de détails sur le sujet. Concrètement, notant $I_d = (\delta_{ij}) \in M_d(\mathbb{Z})$,

$$\mathfrak{g}(\mathbb{Z}) = \left\{(x_{ij}) \in M_d(\mathbb{Z}) \mid \forall f \in \mathcal{I},\ \sum_{i,j} \partial_{ij} f(I_d) x_{ij} = 0\right\}.$$

C'est un sous-module de $\mathfrak{sl}_d(\mathbb{Z})$ sur $\mathbb{Z}$ et, muni du crochet usuel sur $\mathfrak{sl}_d(\mathbb{Z})$, une sous-algèbre de Lie sur $\mathbb{Z}$. Les équations qui définissent $\mathfrak{g}(\mathbb{Z})$ sont à coefficients dans $\mathbb{Z}$, on peut donc définir $\mathfrak{g}(R)$ pour tout anneau R commutatif et unifère :

$$\mathfrak{g}(R) = \left\{(x_{ij}) \in M_d(R) \mid \forall f \in \mathcal{I},\ \sum_{i,j} \partial_{ij} f(I_d) x_{ij} = 0\right\}.$$

On identifie naturellement $\mathfrak{g}(R)$ à une sous-algèbre de Lie de $\mathfrak{sl}_d(R)$. Si R est sans torsion, alors $\mathfrak{g}(R) = \mathfrak{g}(\mathbb{Z}) \otimes_{\mathbb{Z}} R$. De même, si p est un nombre premier suffisamment grand, alors $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z}) = \mathfrak{g}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}$.

On vérifie aisément que cette notion d'algèbre de Lie coïncide avec d'autres définitions :

(1) $\mathfrak{g}(\mathbb{C})$ est l'algèbre de Lie du groupe algébrique linéaire $G_{\mathbb{Q}}$. L'hypothèse que $G_{\mathbb{Q}}$ est simple implique que $\mathfrak{g}(\mathbb{C})$ est une algèbre de Lie simple sur $\mathbb{C}$.

(2) Pour tout premier p, $\mathfrak{g}(\mathbb{Q}_p)$ est égale à l'algèbre de Lie du groupe analytique p-adique $G(\mathbb{Q}_p)$.

Nous aurons aussi besoin du lemme suivant, qui relie l'algèbre de Lie et le groupe des points sur l'anneau $\mathbb{Z}/q\mathbb{Z}$.

Lemme A.1. *Pour tout nombre premier p et tout entier $k \geq 1$, le noyau de $G(\mathbb{Z}/p^{k+1}\mathbb{Z}) \to G(\mathbb{Z}/p^k\mathbb{Z})$ est isomorphe au groupe additif $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$.*

Démonstration. Un antécédent de $I_d \in M_d(\mathbb{Z}/p^k\mathbb{Z})$ dans $M_d(\mathbb{Z}/p^{k+1}\mathbb{Z})$ s'écrit de manière unique sous la forme $I_d + p^k x$, avec $x \in \mathfrak{gl}_d(\mathbb{Z}/p\mathbb{Z})$. Pour tout $f \in \mathcal{A}$,

$$f(I_d + p^k x) = p^k \sum_{i,j} \partial_{ij} f(I_d) x_{ij} \bmod p^{k+1},$$

et par conséquent, $I_d + p^k x \in G(\mathbb{Z}/p^{k+1}\mathbb{Z})$ si et seulement si $x \in \mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$. Cela donne l'isomorphisme souhaité. ∎

A.3. Approximation forte. Le groupe $G(\widehat{\mathbb{Z}})$ des points de G sur l'anneau profini $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/q\mathbb{Z}$ s'identifie à un sous-groupe fermé de $\mathrm{SL}_d(\widehat{\mathbb{Z}})$ pour la topologie profinie. Si Ω désigne l'adhérence de Γ dans $\mathrm{SL}_d(\widehat{\mathbb{Z}})$, nous avons donc $\Omega \subset G(\widehat{\mathbb{Z}})$. Le théorème d'approximation forte ci-dessous est une forme de réciproque à cette inclusion. Il est dû à Matthews, Vaserstein et Weisfeiler [29] lorsque $G_{\mathbb{Q}}$ est simple, et à Nori [30] dans le cas général.

Théorème A.2 (Approximation forte). *Soit Γ un sous-groupe de $\mathrm{SL}_d(\mathbb{Z})$, et G le schéma en groupes associé. Si $G_{\mathbb{Q}}$ est connexe, semi-simple et simplement connexe, alors*

(1) *pour tout nombre premier p assez grand, $\Omega/\Omega_p = G(\mathbb{Z}/p\mathbb{Z})$;*

(2) *le groupe Ω est ouvert dans $G(\widehat{\mathbb{Z}})$ pour la topologie profinie. En particulier, Ω est d'indice fini dans $G(\widehat{\mathbb{Z}})$.*

Remarque. Cela est faux si le groupe n'est pas simplement connexe, comme le montre l'exemple de l'image de $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ dans PGL_2. Cette image est Zariski dense. Cependant, pour chaque p, l'image de Γ dans $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ est d'indice au moins 2, car on ne peut pas obtenir une matrice de la forme $\mathrm{diag}(1, a)$, où a n'est pas un carré modulo p.

Notons deux corollaires importants du théorème ci-dessus.

Corollaire A.3 (Lemme chinois). *Il existe un entier $q_0 \in \mathbb{N}$ tel que pour tout entier $q \in \mathbb{N}^*$ premier avec q_0, si $q = q_1 \cdots q_n$ avec $q_1, \ldots, q_n \in \mathbb{N}^*$ deux-à-deux premiers*

entre eux, alors

$$(\pi_{q_1}, \dots, \pi_{q_n}) \colon \Omega/\Omega_q \to \Omega/\Omega_{q_1} \times \cdots \times \Omega/\Omega_{q_n}$$

est un isomorphisme de groupes.

Démonstration. Le lemme chinois usuel pour $M_d(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^{d^2}$ et la définition des groupes $G(\mathbb{Z}/q\mathbb{Z})$ montre qu'on a un isomorphisme entre $G(\mathbb{Z}/q\mathbb{Z})$ et $\prod G(\mathbb{Z}/q_i\mathbb{Z})$, pour tout $q = q_1 \dots q_n$, avec les q_i deux-à-deux premiers entre eux. On a de même $G(\widehat{\mathbb{Z}}) \simeq \prod_p G(\mathbb{Z}_p)$. Comme Ω est d'indice fini dans $G(\widehat{\mathbb{Z}})$, il doit contenir tous les $G(\mathbb{Z}_p)$, pour $p \geq p_0$. Si l'on note $q_0 = \prod_{p \leq p_0} p$, on a donc, pour tout q premier à q_0,

$$\Omega/\Omega_q \simeq G(\widehat{\mathbb{Z}})/G(\widehat{\mathbb{Z}})_q \simeq G(\mathbb{Z}/q\mathbb{Z}).$$

La dernière égalité provient de la remarque à la fin du paragraphe A.1. ∎

Corollaire A.4. *Il existe une constante $C \geq 1$ tel que pour tout entier $q \in \mathbb{N}^*$, si $q = q_1 \cdots q_n$ avec $q_1, \dots, q_n \in \mathbb{N}^*$ deux-à-deux premiers entre eux,*

$$[\Omega : \Omega_q] \geq \frac{1}{C}[\Omega : \Omega_{q_1}] \cdots [\Omega : \Omega_{q_n}].$$

Outre ces deux corollaires, nous aurons encore besoin de quelques lemmes sur la structure du groupe $G(\mathbb{Z}/p\mathbb{Z})$. Une matrice g est dite unipotent si $g - 1$ est nilpotent. Si p est un premier avec $p > d$ alors $g \in \mathrm{SL}_d(\mathbb{Z}/p\mathbb{Z})$ est unipotent si et seulement si $g^p = 1$.

Lemme A.5. *Soit Γ un sous-groupe de $\mathrm{SL}_d(\mathbb{Z})$ et G le schéma en groupes associé. Si $G_{\mathbb{Q}}$ est connexe, semi-simple et simplement connexe, alors, pour tout nombre premier p suffisamment grand, Ω/Ω_p est engendré par ses éléments unipotents.*

Démonstration. Cela découle du théorème A.2 et d'un résultat de Steinberg [34, Theorem 12.4] selon lequel $G(\mathbb{Z}/p\mathbb{Z})$ est engendré par ses éléments unipotents. ∎

Lemme A.6. *Soit Γ un sous-groupe de $\mathrm{SL}_d(\mathbb{Z})$ et G le schéma en groupes associé. On suppose que $G_{\mathbb{Q}}$ est connexe, semi-simple et simplement connexe. Pour tout nombre premier p suffisamment grand, le groupe quotient Ω_p/Ω_{p^2} est isomorphe au groupe abélien $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$. L'action de Ω sur Ω_p/Ω_{p^2} par conjugaison se factorise par Ω/Ω_p et s'identifie à l'action adjointe de $G(\mathbb{Z}/p\mathbb{Z})$ sur $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$. Le seul point fixe de cette action est $1 \in \Omega_p/\Omega_{p^2}$ (autrement dit $0 \in \mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$).*

Démonstration. D'après le théorème A.2, pour p assez grand, les projections $\Omega \to G(\mathbb{Z}/p\mathbb{Z})$ et $\Omega \to G(\mathbb{Z}/p^2\mathbb{Z})$ sont surjectives. Donc

$$\Omega_p/\Omega_{p^2} \simeq \ker\big(G(\mathbb{Z}/p^2\mathbb{Z}) \to G(\mathbb{Z}/p\mathbb{Z})\big) \simeq \mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$$

par le lemme A.1. Cet isomorphisme est réalisé par l'application exponentielle. Par le lemme B.5, on voit donc que l'action de Ω sur Ω_p/Ω_{p^2} par conjugaison s'identifie à l'action adjointe de $G(\mathbb{Z}/p\mathbb{Z})$ sur $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$. Pour la dernière assertion, on observe que la propriété « l'action adjointe de $G(R)$ sur $\mathfrak{g}(R)$ est sans point fixe non trivial » peut être exprimée comme une formule logique du premier ordre sur le langage des anneaux. Comme l'action adjointe de $G(\mathbb{C})$ sur $\mathfrak{g}(\mathbb{C})$ est sans point fixe non trivial, [19, Corollary 9.2.2] implique qu'il existe c dans $\mathbb{Z}$ tel que pour tout p tel que $c \not\equiv 0 \bmod p$, l'action de $G(\overline{\mathbb{F}}_p)$ sur $\mathfrak{g}(\overline{\mathbb{F}}_p)$ est sans point fixe, où $\overline{\mathbb{F}}_p$ désigne la clôture algébrique de $\mathbb{Z}/p\mathbb{Z}$. Cela implique que l'action de $G(\mathbb{Z}/p\mathbb{Z})$ sur $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$ est sans point fixe, car d'après l'inégalité de Lang–Weil [27], l'ensemble $G(\mathbb{Z}/p\mathbb{Z})$ est suffisamment dense dans $G(\overline{\mathbb{F}}_p)$ pour la topologie de Zariski pour p suffisamment grand. ∎

Nous aurons aussi besoin du lemme suivant, qui précise le point ci-dessus dans le cas où le groupe G est simple.

Lemme A.7. *Soit Γ un sous-groupe de $\mathrm{SL}_d(\mathbb{Z})$ et G le schéma en groupes associé. On suppose que $G_{\mathbb{Q}}$ est simple. Alors pour p assez grand, l'action adjointe de $G(\mathbb{Z}/p\mathbb{Z})$ sur $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$ est irréductible.*

Démonstration. La propriété « l'action adjointe de $G(R)$ sur $\mathfrak{g}(R)$ est irréductible » peut être exprimée comme une formule logique du premier ordre sur le langage des anneaux. La théorie des corps algébriquement clos admet l'élimination des quantificateurs. Le lemme découle donc de [19, Corollary 9.2.2]. ∎

B. L'application exponentielle

Nous donnons ici la construction de l'application expontielle à valeurs dans $\mathrm{GL}_d(\mathbb{Z}/q\mathbb{Z})$, lorsque $q \in \mathbb{N}^*$ est un entier arbitraire, et rappelons quelques-unes de ses propriétés élémentaires. L'algèbre des matrices carrées de taille d à coefficients dans un anneau R est notée $\mathfrak{gl}_d(R)$.

B.1. L'application exponentielle p-adique. Rappelons d'abord les propriétés de l'application exponentielle sur $\mathfrak{gl}_d(\mathbb{Z}_p)$. Notons $\alpha_p = 1 + \delta_2(p)$, i.e., $\alpha_2 = 2$ et $\alpha_p = 1$ si $p \neq 2$.

Lemme B.1. *Pour tout nombre premier p, la série entière*

$$\exp(x) = \sum_{n=0}^{+\infty} \frac{x^n}{n!}$$

est convergente sur $p^{\alpha_p}\mathfrak{gl}_d(\mathbb{Z}_p)$ et définit une isométrie entre $p^{\alpha_p}\mathfrak{gl}_d(\mathbb{Z}_p)$ et le sous-groupe de congruence

$$\ker(\mathrm{GL}_d(\mathbb{Z}_p) \to \mathrm{GL}_d(\mathbb{Z}/p^{\alpha_p}\mathbb{Z})).$$

Sa fonction réciproque, notée log *s'écrit*

$$\log(1+x) = \sum_{n=1}^{+\infty} \frac{(-1)^{(n-1)}}{n} x^n.$$

Démonstration. Pour $n \in \mathbb{N}$, nous avons

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots \leq \frac{n}{p} + \frac{n}{p^2} + \cdots \leq \frac{n}{p-1}. \tag{B.1}$$

Pour tous $x, y \in p^{\alpha_p}\mathfrak{gl}_d(\mathbb{Z}_p)$,

$$\exp(y) - \exp(x) = (y-x)\left(1 + \frac{y+x}{2} + \sum_{n=3}^{+\infty} \frac{y^{n-1} + \cdots + x^{n-1}}{n!}\right).$$

On vérifie aisément que $v_p((y+x)/2) > 0$ et pour $n \geq 3$,

$$v_p\left(\frac{y^{n-1} + \cdots + x^{n-1}}{n!}\right) \geq (n-1)\alpha_p - \frac{n}{p-1} > 0. \qquad \blacksquare$$

Le lemme suivant nous sera utile dans l'appendice C, où nous étudierons la propriété quasi-aléatoire du groupe $G(\widehat{\mathbb{Z}})$, lorsque G est un sous-schéma en groupes sur $\mathbb{Z}$ de SL_d.

Lemme B.2. *Posons*

$$\beta_p = \begin{cases} 3 & \text{si } p = 2, \\ 2 & \text{si } p = 3, \\ 1 & \text{sinon.} \end{cases}$$

Pour tous $x, y \in p^{\beta_p}\mathfrak{gl}_d(\mathbb{Z}_p)$, on a

$$\log(\exp(x)\exp(y)) \equiv x + y \bmod p^{v_p(x)+v_p(y)-2\delta_2(p)}.$$

Démonstration. Formellement,

$$\begin{aligned}(\text{B.2}) \qquad \log(\exp(x)\exp(y)) &= \sum_{m=1}^{+\infty} \frac{(-1)^{m+1}}{m}(\exp(x)\exp(y)-1)^m \\ &= \sum_{m=1}^{+\infty} \frac{(-1)^{m+1}}{m}\Big(\sum_{k,\ell\geq 0}\frac{x^k y^\ell}{k!\ell!}-1\Big)^m \\ &= \sum_{m=1}^{+\infty}\frac{(-1)^{m+1}}{m}\sum_{\substack{k_1+\ell_1\geq 1\\ \cdots\\ k_m+\ell_m\geq 1}}\frac{x^{k_1}y^{\ell_1}\cdots x^{k_m}y^{\ell_m}}{k_1!\cdots k_m!\ell_1!\cdots\ell_m!}.\end{aligned}$$

En utilisant (B.1), on a

$$\begin{aligned}(\text{B.3}) \quad v_p\Big(\frac{(-1)^{m+1}}{m}\frac{x^{k_1}y^{\ell_1}\cdots x^{k_m}y^{\ell_m}}{k_1!\cdots k_m!\ell_1!\cdots\ell_m!}\Big) &\geq k v_p(x)+\ell v_p(y)-\frac{k+\ell+m}{p-1} \\ &\geq k v_p(x)+\ell v_p(y)-\frac{2}{p-1}(k+\ell),\end{aligned}$$

où $k = k_1 + \cdots + k_m$ and $\ell = \ell_1 + \cdots + \ell_m$. Ainsi, la série dans (B.2) est convergente pour $x, y \in p^{\beta_p}\mathfrak{gl}_d(\mathbb{Z}_p)$. À l'aide de (B.3), et en faisant attention aux cas $p = 2$ et $p = 3$, on vérifie que tous les termes de degré homogène supérieur à 2 qui apparaissent dans (B.2) sont de valuation p-adique au moins $v_p(x) + v_p(y) - 2\delta_2(p)$. ∎

D'après [33, Part I, Chap. IV, Theorem 7.4], chaque terme homogène dans la série dans (B.2) est en fait un élément dans l'algèbre de Lie libre à deux indéterminées sur $\mathbb{Q}$, c'est-à-dire une combinaison $\mathbb{Q}$-linéaire de crochets itérés en x et y.

B.2. L'application exponentielle modulo q. Étant donné $q = \prod p^{m_p}$, avec $m_2 \neq 1$, posons

$$\dot{r} = \prod_{p|q} p^{1+\delta_2(p)}.$$

En utilisant les isomorphismes

$$\mathfrak{gl}_d\Big(\prod_{p|q}\mathbb{Z}_p\Big) \simeq \prod_{p|q}\mathfrak{gl}_d(\mathbb{Z}_p) \quad \text{et} \quad \mathrm{GL}_d\Big(\prod_{p|q}\mathbb{Z}_p\Big) \simeq \prod_{p|q}\mathrm{GL}_d(\mathbb{Z}_p),$$

et en combinant les applications exponentielles sur chaque facteur, on obtient une bijection définie sur $\dot{r}\,\mathfrak{gl}_d(\prod_{p|q}\mathbb{Z}_p)$ et à valeurs dans

$$\ker\Big(\mathrm{GL}_d\Big(\prod_{p|q}\mathbb{Z}_p\Big) \to \mathrm{GL}_d(\mathbb{Z}/\dot{r}\mathbb{Z})\Big).$$

Ainsi, pour $x \in \dot{r}\mathfrak{gl}_d(\widehat{\mathbb{Z}})$, $\exp(x)$ est bien défini dans $\mathrm{GL}_d(\prod_{p|q}\mathbb{Z}_p)$. Plus généralement, si $A \subset \dot{r}\mathfrak{gl}_d(\widehat{\mathbb{Z}})$, l'image $\exp(A)$ est bien définie dans $\mathrm{GL}_d(\prod_{p|q}\mathbb{Z}_p)$, et l'on note

$$N(\exp(A), q) = \operatorname{card} \pi_q(\exp(A))$$

le cardinal de sa projection modulo q.

Lemme B.3. *Avec les notations ci-dessus, l'application exponentielle a les deux propriétés suivantes.*

(1) *Pour tout $x \in \dot{r}\mathfrak{gl}_d(\widehat{\mathbb{Z}})$, pour tout facteur premier p de q,*

$$v_p(\exp(x) - 1) = v_p(x).$$

(2) *Pour tout $B \subset \dot{r}\mathfrak{gl}_d(\widehat{\mathbb{Z}})$,*

$$N(\exp(B), q) = N(B, q).$$

Inversement, si $A \subset \ker(\mathrm{GL}_d(\widehat{\mathbb{Z}}) \to \mathrm{GL}_d(\mathbb{Z})/\mathrm{GL}_d(\mathbb{Z}/\dot{r}\mathbb{Z}))$,

$$N(\log(A), q) = N(A, q).$$

Démonstration. Ce sont des conséquences immédiates du lemme B.1. ∎

Naturellement, si Γ est un sous-groupe de $\mathrm{SL}_d(\mathbb{Z})$, G le schéma en groupes associé, et Ω l'adhérence de Γ dans $\mathrm{SL}_d(\widehat{\mathbb{Z}})$, on peut restreindre les applications exponentielles et logarithme à $\mathfrak{g}(\widehat{\mathbb{Z}})$ et $G(\widehat{\mathbb{Z}})$. En notant, pour $q \in \mathbb{N}^*$, $\Omega_q = \Omega \cap \ker \pi_q$, cela donne le lemme suivant.

Lemme B.4. *Si $g \in \Omega_{\dot{r}}$ alors $\log g \in \dot{r}\mathfrak{g}(\prod_{p|q}\mathbb{Z}_p)$. En particulier,*

$$\log g \in \dot{r}\mathfrak{g}(\mathbb{Z}) \bmod q\mathfrak{g}(\mathbb{Z}).$$

Démonstration. D'après les propriétés de l'exponentielle modulo q sur $\mathfrak{gl}_d$, l'élément $\log g$ est bien défini dans $\mathfrak{gl}_d(\dot{r}\prod_{p|q}\mathbb{Z}_p)$ dès que $g \in \Omega_{\dot{r}}$. Par ailleurs, pour tout nombre premier p, l'algèbre de Lie du groupe analytique $G(\mathbb{Z}_p)$ est $\mathfrak{g}(\mathbb{Q}_p)$, donc pour tout $g \in \Omega_{\dot{r}}$,

$$\log g \in \mathfrak{g}(\mathbb{Q}_p) \cap p^{\alpha_p}\mathfrak{gl}_d(\mathbb{Z}_p) = p^{\alpha_p}\mathfrak{g}(\mathbb{Z}_p).$$

puis

$$\log g \in \prod_{p|q} p^{\alpha_p}\mathfrak{g}(\mathbb{Z}_p) = \dot{r}\prod_{p|q}\mathfrak{g}(\mathbb{Z}_p) \simeq \dot{r}\mathfrak{g}\Big(\prod_{p|q}\mathbb{Z}_p\Big).$$ ∎

B.3. Exponentielle et représentation adjointe. Si R est un anneau unifère quelconque, l'action adjointe de $\mathrm{GL}_d(R)$ sur l'algèbre de Lie $\mathfrak{gl}_d(R)$ est définie par

$$\forall a \in \mathrm{GL}_d(R), \forall x \in \mathfrak{gl}_d(R), \quad \mathrm{Ad}(a) \cdot x = axa^{-1}.$$

Nous noterons aussi, pour $a, g \in \mathrm{GL}_d(R)$,

$$\iota(a) \cdot g = aga^{-1}.$$

En particulier, pour $A \subset \mathrm{GL}_d(R)$,

$$\iota(A) \cdot g = \{aga^{-1} \mid a \in A\}.$$

Lemme B.5. *Soit $q = \prod p^{m_p}$, avec $m_p \neq 1$, et $\dot{r} = \prod_{p|q} p^{1+\delta_2(p)}$.*
(1) *Pour tout $a \in \mathrm{SL}_d(\mathbb{Z})$ et $x \in \dot{r}\mathfrak{sl}_d(\mathbb{Z})$,*

$$\iota(a) \cdot \exp(x) \equiv \exp(\mathrm{Ad}(a) \cdot x) \bmod q.$$

(2) *Pour tout $a \in G(\mathbb{Z})$ la restriction de $\mathrm{Ad}(a)$ à $\mathfrak{g}(\mathbb{Z})$ est un automorphisme de $\mathbb{Z}$-module.*

Démonstration. Le premier point est une conséquence du développement en série entière de l'application exponentielle sur $\mathfrak{sl}_d$. Le second découle de ce que $\mathrm{Ad}\, a$ préserve $\mathfrak{g}(\mathbb{Z}) = \mathfrak{g}(\mathbb{Q}) \cap \mathfrak{sl}_d(\mathbb{Z})$ et admet pour inverse $\mathrm{Ad}\, a^{-1}$. ∎

C. Propriété quasi-aléatoire

Comme ci-dessus, Γ désigne un sous-groupe de $\mathrm{SL}_d(\mathbb{Z})$, G est le schéma en groupes associé, et Ω l'adhérence de Γ dans $\mathrm{SL}_d(\widehat{\mathbb{Z}})$. Dans ce dernier appendice, nous donnons une démonstration de la propriété quasi-aléatoire du groupe $G(\widehat{\mathbb{Z}})$, déjà énoncée comme proposition 9 dans le corps de l'article, et que nous rappelons ici pour plus de lisibilité.

Proposition C.1 (Propriété quasi-aléatoire). *On suppose que $G_{\mathbb{Q}}$ est semi-simple, connexe, et simplement connexe. Alors, il existe $\kappa > 0$ tel que pour toute représentation irréductible (ρ, V_ρ) de Ω, il existe $q \in \mathbb{N}^*$ tel que*

$$\Omega_q \subset \ker \rho \quad \textit{et} \quad \dim V_\rho \geq \kappa[\Omega : \Omega_q]^\kappa.$$

C.1. Cas des groupes p-adiques. Pour un nombre premier p et $m \in \mathbb{N}$, notons $H_{p,m}$ le sous-groupe de congruence de $G(\mathbb{Z}_p)$,

$$H_{p,m} = \{g \in G(\mathbb{Z}_p) \mid g \equiv 1 \bmod p^m\}.$$

Nous dirons que le schéma en groupes G est parfait si sa fibre générique $G_{\mathbb{Q}}$ l'est, ce qui revient à dire que son algèbre de Lie $\mathfrak{g}_{\mathbb{Q}}$ coïncide avec son algèbre dérivée $[\mathfrak{g}_{\mathbb{Q}}, \mathfrak{g}_{\mathbb{Q}}]$.

Proposition C.2. *On suppose que G est parfait. Alors, il existe une famille d'entiers naturels $(o_p)_p$ telle que $o_p = 0$ sauf pour un nombre fini de nombres premiers p et que l'assertion suivante soit vraie.*

Pour tout p premier, et tous entiers $k \geq 2$ et $m \geq 6$, si (ρ, V) est une représentation unitaire de $H_{p,k}$ triviale sur $H_{p,m}$ et non triviale sur $H_{p,m-1}$, alors

$$\dim V \geq p^{\lfloor m/2 \rfloor - k - o_p}.$$

Démonstration. Dans cette démonstration, nous écrirons

$$H_\ell = H_{p,\ell} \text{ pour } \ell \in \mathbb{N}, \quad \text{et} \quad H = H_k.$$

Posons $\mathfrak{h} = \log(H_k)$ et, pour tout $\ell \geq 2$, $\mathfrak{h}_\ell = \log H_\ell$. D'après la discussion dans les appendices A et B, $\mathfrak{h}_\ell = p^\ell \mathfrak{g}(\mathbb{Z}_p)$ et $\mathfrak{g}(\mathbb{Z}_p) = \mathfrak{g}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. En particulier $\mathfrak{h}$ et $\mathfrak{h}_\ell$ sont des sous-algèbres de Lie de $\mathfrak{g}(\mathbb{Z}_p)$ sur $\mathbb{Z}_p$.

Maintenant posons $\ell = \lceil m/2 \rceil + \delta_2(p)$ de sorte que l'application exponentielle induit un isomorphisme de groupes entre $\mathfrak{h}_\ell/\mathfrak{h}_m$ et H_ℓ/H_m, par lemme B.2. On peut supposer $\ell \geq k$, sans quoi il n'y a rien à démontrer. La représentation ρ se décompose en une somme directe suivant les caractères de $\mathfrak{h}_\ell$,

$$V = \bigoplus_{\psi \in \mathrm{Hom}(\mathfrak{h}_\ell, S^1)} V_\psi,$$

où ψ parcourt l'ensemble des caractères unitaires de $\mathfrak{h}_\ell$ se factorisant par $\mathfrak{h}_\ell/\mathfrak{h}_m$ et pour un tel ψ,

$$V_\psi = \{v \in V \mid \forall x \in \mathfrak{h}_\ell, \rho(\exp(x))v = \psi(x)v\}.$$

Comme H_ℓ est distingué dans H, l'action de H sur V permute les sous-espaces caractéristiques correspondant à l'action co-adjointe. Plus précisément, notant

$$\forall g \in H, \forall \psi \in \mathrm{Hom}(\mathfrak{h}_\ell, S^1), \quad \mathrm{Ad}^*(g)\psi = \psi \circ \mathrm{Ad}(g^{-1}),$$

nous avons

$$\forall g \in H, \forall \psi \in \mathrm{Hom}(\mathfrak{h}_\ell, S^1), \quad \rho(g)V_\psi = V_{\mathrm{Ad}^*(g)\psi}.$$

Il s'ensuit que pour des caractères $\psi \in \mathrm{Hom}(\mathfrak{h}_\ell, S^1)$ avec $V_\psi \neq \{0\}$, on a

$$\dim V \geq |\mathrm{Ad}^*(H)\psi| = [H : \mathrm{Stab}_H(\psi)]$$

où $\mathrm{Stab}_H(\psi) = \{g \in H \mid \mathrm{Ad}^*(g)\psi = \psi\}$ désigne le stabilisateur de ψ sous l'action co-adjointe. La fin de la démonstration consiste à minorer l'indice $[H : \mathrm{Stab}_H(\psi)]$, ce pour quoi nous aurons besoin de deux lemmes. Le premier est une variante d'un énoncé de Howe [25, Lemma 1.1].

Lemme C.3. *Posons* $\mathfrak{stab}_\mathfrak{h}(\psi) = \log \mathrm{Stab}_H(\psi)$, *alors*

$$\mathfrak{stab}_\mathfrak{h}(\psi) = \{x \in \mathfrak{h} \mid \forall y \in \mathfrak{h}_\ell,\ \psi([x, y]) = 1\}.$$

Démonstration. Pour $x \in \mathfrak{h}$, la somme $\tau(x) = \sum_{n=0}^{+\infty} \mathrm{ad}(x)^n/(n+1)!$ définit une isométrie de $\mathfrak{h} \to \mathfrak{h}$ vérifiant

$$\mathrm{ad}(x) \circ \tau(x) = e^{\mathrm{ad}(x)} - \mathrm{Id} = \mathrm{Ad}(\exp(x)) - \mathrm{Id}\,.$$

Comme $\tau(x)$ est une isométrie, $\tau(x)\mathfrak{h}_\ell = \mathfrak{h}_\ell$ et donc, pour tout $x \in \mathfrak{h}$,

$$\begin{aligned}
\exp(x) \in \mathrm{Stab}_H(\psi) &\iff \forall y \in \mathfrak{h}_\ell, \quad \psi(\mathrm{Ad}(\exp(x))y - y) = 1, \\
&\iff \forall y \in \mathfrak{h}_\ell, \quad \psi([x, \tau(x)y]) = 1, \\
&\iff \forall y \in \mathfrak{h}_\ell, \quad \psi([x, y]) = 1.
\end{aligned}$$

■

Le second lemme est tiré de la démonstration de [31, Lemma 32].

Lemme C.4. *Pour tout caractère* $\psi \in \mathrm{Hom}(\mathfrak{h}_\ell, S^1)$, *si* $\mathfrak{stab}_\mathfrak{h}(\psi^p) = \mathfrak{stab}_\mathfrak{h}(\psi)$, *alors* $\mathfrak{h} = \mathfrak{stab}_\mathfrak{h}(\psi)$.

Démonstration. Notons que $\mathfrak{stab}_\mathfrak{h}(\psi)$ est ouvert dans $\mathfrak{h}$ et que par conséquent, le quotient $\mathfrak{h}/\mathfrak{stab}_\mathfrak{h}(\psi)$ est fini. Or, $\mathfrak{h}$ est pro-p, donc le quotient $\mathfrak{h}/\mathfrak{stab}_\mathfrak{h}(\psi)$ est un p-groupe. Pour montrer qu'il est trivial il suffit de montrer qu'il n'a pas de p-torsion.

Supposons que $\mathfrak{stab}_\mathfrak{h}(\psi^p) = \mathfrak{stab}_\mathfrak{h}(\psi)$, et soit $x \in \mathfrak{h}$ avec $px \in \mathfrak{stab}_\mathfrak{h}(\psi)$. Alors, pour tout $y \in \mathfrak{h}_\ell$, $\psi^p([x, y]) = \psi([px, y]) = 1$ d'après le lemme précédent. Par le lemme précédent de nouveau, $x \in \mathfrak{stab}_\mathfrak{h}(\psi^p)$ et donc $x \in \mathfrak{stab}_\mathfrak{h}(\psi)$ par hypothèse. Cela montre que $\mathfrak{h}/\mathfrak{stab}_\mathfrak{h}(\psi)$ n'a pas de p-torsion. ■

En itérant ce lemme, on obtient, pour tout caractère unitaire ψ de $\mathfrak{h}_\ell$, un entier n tel que

$$\mathfrak{stab}_\mathfrak{h}(\psi) \subsetneq \mathfrak{stab}_\mathfrak{h}(\psi^p) \subsetneq \cdots \subsetneq \mathfrak{stab}_\mathfrak{h}(\psi^{p^n}) = \mathfrak{h}.$$

Comme chaque terme de cette suite est d'indice au moins p dans le terme suivant,

$$[H : \mathrm{Stab}_H(\psi)] = [\mathfrak{h} : \mathfrak{stab}_\mathfrak{h}(\psi)] \geq p^n.$$

Reste à minorer l'entier n. Par hypothèse, $[\mathfrak{g}(\mathbb{Q}), \mathfrak{g}(\mathbb{Q})] = \mathfrak{g}(\mathbb{Q})$, et il existe donc un entier $D = \prod p^{o_p}$ tel que $D\mathfrak{g}(\mathbb{Z}) \subset [\mathfrak{g}(\mathbb{Z}), \mathfrak{g}(\mathbb{Z})]$. Avec l'égalité $\mathfrak{g}(\mathbb{Z}_p) = \mathfrak{g}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$, cela donne

$$p^{o_p}\mathfrak{g}(\mathbb{Z}_p) \subset [\mathfrak{g}(\mathbb{Z}_p), \mathfrak{g}(\mathbb{Z}_p)].$$

Par ailleurs, $p^k\mathfrak{g}(\mathbb{Z}_p) = \mathfrak{h}$ et $p^\ell\mathfrak{g}(\mathbb{Z}_p) = \mathfrak{h}_\ell$, donc

$$\mathfrak{h}_{k+\ell+o_p} = p^{k+\ell+o_p}\mathfrak{g}(\mathbb{Z}_p) \subset [\mathfrak{h}, \mathfrak{h}_\ell].$$

Mais l'égalité $\mathfrak{sta}_{\mathfrak{h}}(\psi^{p^n}) = \mathfrak{h}$ implique $p^n[\mathfrak{h}, \mathfrak{h}_\ell] \subset \ker\psi$, puis

$$\mathfrak{h}_{n+k+\ell+o_p} \subset p^n[\mathfrak{h}, \mathfrak{h}_\ell] \subset \ker\psi.$$

Par hypothèse, il existe $\psi \in \mathrm{Hom}(\mathfrak{h}_\ell, S^1)$ tel que $\dim V_\psi > 0$ et $\mathfrak{h}_{m-1} \not\subset \ker\psi$, d'où

$$n + k + \ell + o_p \geq m$$

et enfin

$$\dim V \geq [H : \mathrm{Stab}_H(\psi)] \geq p^n \geq p^{\lfloor m/2\rfloor - k - o_p - \delta_2(p)}.$$ ∎

C.2. Cas des groupes linéaires sur $\mathbb{Z}/p\mathbb{Z}$. Comme nous n'avons pas pu en trouver une démonstration en un seul tenant dans la littérature, nous montrons ici une borne inférieure sur le degré d'une représentation irréductible non triviale de $G(\mathbb{Z}/p\mathbb{Z})$. Ce résultat remonte à Frobenius [20] lorsque $G = \mathrm{SL}_2$, apparaît dans Landazuri et Seitz [26] lorsque G est un groupe de Chevalley, et dans le cas général dans l'article d'Emmanuel Breuillard [17, Proposition 6.1] sur le sujet.

Théorème C.5. *Soit G un sous-schéma en groupes fermé de $\mathrm{SL}_{d,\mathbb{Z}}$ dont la fibre générique $G_{\mathbb{Q}}$ est un groupe algébrique connexe semi-simple simplement connexe. Pour tout nombre premier p suffisamment grand, le degré de toute représentation linéaire irréductible non triviale de $G(\mathbb{Z}/p\mathbb{Z})$ est minoré par $\frac{p-1}{2}$.*

Démonstration. Supposons dans un premier temps que $G_{\mathbb{Q}}$ soit absolument simple. L'idée de la démonstration est de reprendre l'argument élémentaire valable pour $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ en utilisant un $\mathfrak{sl}_2$-triplet bien choisi dans $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$. Soit (ρ, V) une représentation linéaire non triviale de $G(\mathbb{Z}/p\mathbb{Z})$.

Comme $G_{\mathbb{Q}}$ est simplement connexe, pour tout p suffisamment grand, le groupe $G(\mathbb{Z}/p\mathbb{Z})$ est engendré par ses éléments unipotents [34, Theorem 12.4]. Soit u un élément unipotent quelconque de $G(\mathbb{Z}/p\mathbb{Z})$. Le théorème de Jacobson-Morozov pour les algèbres de Lie semi-simples est habituellement cité en caractéristique nulle, et c'est le cas dans Bourbaki [7, Chap. VIII, §11, Proposition 2]. Cependant, on peut vérifier que la démonstration reste valable dans notre cadre dès que p est suffisamment

grand. Par conséquent, l'élément nilpotent $x = \log u$ dans $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$ fait partie d'un certain $\mathfrak{sl}_2$-triplet (x, y, h). Les éléments $u = \exp x$ et $\exp y$ sont dans $G(\mathbb{Z}/p\mathbb{Z})$. Notons H le sous-groupe qu'ils engendrent. L'image de H dans la représentation adjointe sur l'algèbre de Lie $\langle x, y, h\rangle \simeq \mathfrak{sl}_2(\mathbb{Z}/p\mathbb{Z})$ est isomorphe à $\mathrm{Aut}\,\mathfrak{sl}_2(\mathbb{Z}/p\mathbb{Z}) \simeq \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$. En effet,

$$(\mathrm{Ad}\,u)x = x, \quad (\mathrm{Ad}\,u)h = e^{\mathrm{ad}\,x}h = h - 2x, \quad (\mathrm{Ad}\,u)y = e^{\mathrm{ad}\,x}y = y + h - x,$$

donc dans la base (x, h, y), $\mathrm{Ad}\,u$ a pour matrice

$$\begin{pmatrix} 1 & -2 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

On calcule de même la matrice de $\mathrm{Ad}\exp y$, égale à

$$\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix}.$$

Et ces deux éléments engendrent $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$. De plus, le noyau de $H \to \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ est contenu dans le centre de H.

Soit alors t un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ et $a \in G(\mathbb{Z}/p\mathbb{Z})$ un élément de H tel que les images de a et u dans $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ s'identifient respectivement à

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Il existe un élément z dans le centre de H tel que $aua^{-1} = zu^{t^2}$. Comme u est d'ordre p, on a $z^p = 1$. Soit k l'inverse de $1 - t^2$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Quitte à remplacer u par $z^k u$, on peut supposer

$$aua^{-1} = u^{t^2}. \tag{C.1}$$

D'après le lemme A.7, les logarithmes des conjugués de u engendrent linéairement $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$, pour p assez grand. D'après [30, Theorem B], u et ses conjugués engendrent $G(\mathbb{Z}/p\mathbb{Z})$. En effet, le groupe engendré par u et ses conjugués s'écrit $H(F_p)^+$, avec H algébrique, et comme son cardinal est $\gg p^{\dim G}$ (cf. [17, Proof of Theorem 2.2]), on doit avoir d'après l'inégalité de Lang–Weil, $\dim H = \dim G$, et par connexité de G, $H = G$. Mais G est simplement connexe, et donc

$$H(F_p)^+ = G(F_p)^+ = G(F_p),$$

d'après Steinberg [34, Theorem 12.4]. Si l'on décompose V suivant les caractères du groupe $U \simeq \mathbb{Z}/p\mathbb{Z}$ engendré par u,

$$V = \bigoplus_{\chi \in \mathrm{Hom}(U, S^1)} V_\chi,$$

où

$$V_\chi = \{v \in V \mid \forall g \in U,\ \rho(g)v = \chi(g)v\},$$

on voit apparaître un caractère non trivial. Or, a normalise le sous-groupe U. Il agit donc sur le groupe de ses caractères. À l'aide de (C.1), on voit aisément que l'orbite d'un caractère non trivial χ sous l'action du sous-groupe engendré par a est de cardinal $(p-1)/2$. Comme tous les éléments de cette orbite doivent apparaître dans la décomposition de V, on trouve bien

$$\dim V \ \geq \frac{p-1}{2}.$$

Ceci termine la démonstration dans le cas où $G_{\mathbb{Q}}$ est absolument simple ou, plus précisément, le cas où l'action adjointe de $G(\mathbb{Z}/p\mathbb{Z})$ sur $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$ est irréductible.

Dans le cas général, on se ramène au cas où l'action de $G(\mathbb{Z}/p\mathbb{Z})$ est irréductible grâce à une décomposition de la réduction modulo p de G en facteurs simples sur $\mathbb{Z}/p\mathbb{Z}$. Comme nous n'utilisons pas le théorème dans cette généralité, les détails de la démonstration sont laissés au lecteur. ∎

Corollaire C.6. *Soit G un sous-schéma en groupes fermé de $\mathrm{SL}_{d,\mathbb{Z}}$ dont la fibre générique $G_{\mathbb{Q}}$ est un groupe algébrique connexe semi-simple et simplement connexe. Alors pour tout nombre premier p suffisamment grand, l'indice d'un sous-groupe propre de $G(\mathbb{Z}/p\mathbb{Z})$ est minoré par $(p-1)/2$.*

Démonstration. Si H est un sous-groupe propre de $G(\mathbb{Z}/p\mathbb{Z})$ alors la représentation quasi-régulière $\ell^2(G(\mathbb{Z}/p\mathbb{Z})/H)$ de $G(\mathbb{Z}/p\mathbb{Z})$ est non triviale et son degré est égal à l'indice de H dans $G(\mathbb{Z}/p\mathbb{Z})$. ∎

Le théorème C.5 permet aussi de minorer le degré d'une représentation non triviale du groupe profini $G(\mathbb{Z}_p)$, lorsque G est simple.

Proposition C.7. *Soit G un sous-schéma en groupes fermé de $\mathrm{SL}_{d,\mathbb{Z}}$ dont la fibre générique $G_{\mathbb{Q}}$ est un groupe algébrique connexe semi-simple et simplement connexe. Pour tout nombre premier p suffisamment grand, le degré de toute représentation unitaire non triviale de $G(\mathbb{Z}_p)$ est au moins $(p-1)/2$.*

Démonstration. D'après le lemme de Hensel, si p est suffisamment grand, la projection $G(\mathbb{Z}_p) \to G(\mathbb{Z}/p^m\mathbb{Z})$ est surjective pour tout entier $m \geq 1$. Supposons en outre p assez grand pour que les conclusions du lemme A.7, du théorème C.5 et du corollaire C.6 soient vérifiées.

Soit (ρ, V) une représentation unitaire non triviale de $G(\mathbb{Z}_p)$ et $m \in \mathbb{N}$ minimal tel que ρ se factorise par $G(\mathbb{Z}/p^m\mathbb{Z})$. Alors, (ρ, V) s'identifie à une représentation linéaire de $G(\mathbb{Z}/p^m\mathbb{Z})$.

Si $m = 1$, alors $\dim V \geq (p-1)/2$ par le théorème C.5. Sinon, notons H le noyau de la projection $G(\mathbb{Z}/p^m\mathbb{Z}) \to G(\mathbb{Z}/p^{m-1}\mathbb{Z})$. Par le lemme A.1, H est abélien, isomorphe à $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$. On peut décomposer V en sous-espaces caractéristiques

$$V = \bigoplus_{\chi \in \mathrm{Hom}(H, S^1)} V_\chi,$$

où

$$V_\chi = \{v \in V \mid \forall g \in H, \rho(g)v = \chi(g)v\}.$$

Par minimalité de m, il existe un caractère χ non trivial tel que $V_\chi \neq \{0\}$. Comme dans la démonstration de la proposition C.2, l'action co-adjointe de $G(\mathbb{Z}/p^m\mathbb{Z})$ sur les caractères de H permet de montrer que

$$\dim V \geq [G(\mathbb{Z}/p^m\mathbb{Z}) : \mathrm{Stab}_{G(\mathbb{Z}/p^m\mathbb{Z})}(\chi)].$$

Or, cette action de $G(\mathbb{Z}/p^m\mathbb{Z})$ se factorise par $G(\mathbb{Z}/p\mathbb{Z})$, et sous l'isomorphisme $H \simeq \mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$, s'identifie à l'action co-adjointe de $G(\mathbb{Z}/p\mathbb{Z})$ sur le dual de $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$. Par le lemme A.7, la dernière action n'a pas de point fixe sauf l'élément 0 dans le dual de $\mathfrak{g}(\mathbb{Z}/p\mathbb{Z})$. Donc $[G(\mathbb{Z}/p^m\mathbb{Z}) : \mathrm{Stab}_{G(\mathbb{Z}/p^m\mathbb{Z})}(\chi)]$ est égal à l'indice d'un sous-groupe propre de $G(\mathbb{Z}/p\mathbb{Z})$, qui est minoré par $(p-1)/2$, d'après le corollaire C.6. ∎

C.3. La propriété quasi-aléatoire de Ω. Nous dirons qu'un groupe pro-fini Ω est *quasi-aléatoire* par rapport à une famille de sous-groupes distingués $(\Omega_q)_{q\in\mathbb{N}^*}$ si pour toute représentation irréductible unitaire (ρ, V_ρ) de Ω, il existe $q \in \mathbb{N}^*$ tel que

$$\Omega_q \subset \ker \rho \quad \text{et} \quad \dim V_\rho \geq \kappa[\Omega : \Omega_q]^\kappa.$$

Pour conclure la démonstration de la proposition C.1, nous utiliserons le lemme suivant.

Lemme C.8. *Soit Ω un groupe profini et $(\Omega_q)_{q\in\mathbb{N}^*}$ une famille de sous-groupes ouverts distingués vérifiant $\Omega_q \cap \Omega_{q'} = \Omega_{\mathrm{pgcd}(q,q')}$ pour tous $q, q' \in \mathbb{N}^*$, et telle que $\bigcap_{q\in\mathbb{N}^*} \Omega_q = \{1\}$. Soit Ω' un sous-groupe fermé d'indice fini de Ω. Si Ω' est quasi-aléatoire par rapport à la famille $\Omega'_q = \Omega_q \cap \Omega'$, $q \in \mathbb{N}^*$, alors Ω est quasi-aléatoire par rapport à la famille $(\Omega_q)_{q\in\mathbb{N}^*}$.*

Démonstration. Comme Ω' est fermé et d'indice fini, il est ouvert dans Ω, et contient donc $\Omega_{q'}$ pour un certain $q' \in \mathbb{N}^*$.

Soit (ρ, V_ρ) une représentation irréductible unitaire de Ω et $(\rho', V_{\rho'}) \in \widehat{\Omega}'$ une sous-représentation irréductible de la restriction de ρ à Ω'. D'après la propriété quasi-aléatoire de Ω', il existe $\kappa > 0$ indépendant de ρ tel qu'il existe $q \in \mathbb{N}^*$ vérifiant $\Omega'_q \subset \ker \rho'$ et $\dim V_{\rho'} \geq \kappa[\Omega' : \Omega'_q]^\kappa$. En posant $s = \operatorname{pgcd}(q, q')$, on a

$$\Omega_s = \Omega_q \cap \Omega_{q'} \subset \Omega_q \cap \Omega' = \Omega'_q \subset \ker \rho.$$

Par conséquent,

$$\begin{aligned}[\Omega : \Omega_s] &= [\Omega : \Omega'_q][\Omega'_q : \Omega_s] \\ &= [\Omega : \Omega'_q][\Omega' \cap \Omega_q : \Omega_{q'} \cap \Omega_q] \leq [\Omega : \Omega_{q'}][\Omega' : \Omega'_q]\end{aligned}$$

et enfin,

$$\dim V_\rho \geq \dim V_{\rho'} \geq \kappa[\Omega' : \Omega'_q]^\kappa \geq \kappa \frac{[\Omega : \Omega_s]^\kappa}{[\Omega : \Omega_{q'}]^\kappa}.$$

Cela montre que Ω est quasi-aléatoire par rapport à la famille $(\Omega_q)_{q \in \mathbb{N}^*}$. ∎

Démonstration de la proposition 9. D'après le théorème A.2 il existe un entier $s = \prod p^{k_p}$ tel que Ω contienne le sous-groupe de congruence $\ker \pi_s \subset G(\widehat{\mathbb{Z}})$. Par le lemme C.8, on peut supposer Ω égal à ce sous-groupe de congruence. Alors, Ω s'écrit comme un produit direct

$$\Omega = \prod H_{p,k_p},$$

où $H_{p,k_p} = \ker \pi_{p^{k_p}} \subset G(\mathbb{Z}_p)$.

Soit $(\rho, V) \in \widehat{\Omega}$ une représentation unitaire irréductible, et q le multiple minimal de s tel que $\Omega_q \subset \ker \rho$. Écrivons $q = \prod p^{m_p}$. Comme Ω est un produit direct, (ρ, V) s'écrit comme un produit tensoriel

$$(\rho, V) = \bigotimes_{p|q} (\rho_p, V_p),$$

où pour tout facteur premier p de q, (ρ_p, V_p) est une représentation unitaire irréductible de H_{p,k_p}. De plus, pour tout p, m_p est l'entier minimal tel que ρ_p soit trivial sur H_{p,m_p}.

Soit $M \geq 0$ tel que pour tout $p \geq M$, la conclusion de la proposition C.7 soit valable, et qu'en outre $k_p = 0$ et $(p-1)/2 \geq p^{1/2}$. On partitionne les nombres premiers en trois parties en posant

$$\begin{aligned}I_1 &= \{p \mid p \leq M \text{ et } m_p \leq 5\}, \\ I_2 &= \{p \mid p \geq M \text{ et } m_p \leq 5\}, \\ I_3 &= \{p \mid m_p \geq 6\}.\end{aligned}$$

Évidemment,

$$\prod_{p\in I_1} \dim V_p \geq 1.$$

De plus, si $p \in I_2$, alors ρ_p est une représentation unitaire de $G(\mathbb{Z}_p)$, et d'après la proposition C.7,

$$\prod_{p\in I_2} \dim V_p \geq \prod_{p\in I_2} \frac{p-1}{2} \geq \prod_{p\in I_2} p^{\frac{m_p}{10}}.$$

Enfin, si $p \in I_3$, alors $\lfloor m_p/2 \rfloor \geq m_p/3$, et la proposition C.2 permet de minorer

$$\prod_{p\in I_3} \dim V_p \geq \prod_{p\in I_3} p^{\frac{m_p}{3}-k_p-o_p}.$$

Mis bout à bout, cela donne

$$\dim V = \prod_{p|q} \dim V_p \geq \frac{q^{\frac{1}{10}}}{C},$$

avec $C = (\prod_{p\in I_1} p^{\frac{1}{2}})(\prod_{p\in I_3} p^{k_p+o_p})$. ∎

Remerciements. Nous remercions Emmanuel Breuillard et Péter Varjú pour leur encouragement à rédiger en détail les démonstrations présentées ici.

Funding. W.H. a bénéficié du soutien de l'ERC 2020 grant HomDyn (grant no. 833423) à l'Université Hébraïque de Jérusalem et de KIAS Individual Grant (no. MG080401) à Korea Institute for Advanced Study.

Références

[1] M. Abért and G. Elek, Dynamical properties of profinite actions. *Ergodic Theory Dynam. Systems* **32** (2012), no. 6, 1805–1835. Zbl 1297.37004 MR 2995875

[2] M. Aka, E. Breuillard, L. Rosenzweig and N. de Saxcé, Diophantine properties of nilpotent Lie groups. *Compos. Math.* **151** (2015), no. 6, 1157–1188. Zbl 1332.22011 MR 3357181

[3] B. Bekka, P. de la Harpe and A. Valette, *Kazhdan's property (T)*. New Math. Monogr. 11, Cambridge University Press, Cambridge, 2008. Zbl 1146.22009 MR 2415834

[4] Y. Benoist and N. de Saxcé, A spectral gap theorem in simple Lie groups. *Invent. Math.* **205** (2016), no. 2, 337–361. Zbl 1357.22003 MR 3529116

[5] A. Borel, *Introduction aux groupes arithmétiques*. Publ. Inst. Math. Univ. Strasbourg XV. Actual. Sci. Ind. 1341, Hermann, Paris, 1969. Zbl 0186.33202 MR 244260

[6] — *Linear algebraic groups*. Second edn., Grad. Texts in Math. 126, Springer, New York, 1991. Zbl 0726.20030 MR 1102012

[7] N. Bourbaki, *Eléments de mathématique. Groupes et algèbres de Lie. Chapitres 7 et 8*. Reprint of the 1975 original, Springer, Berlin, 2006. Zbl 1181.17001 MR 453824

[8] — *Éléments de mathématique. Algèbre. Chapitre 8*. Second revised edition of the 1958 original, Springer, Berlin, 2012. Zbl 1245.16001 MR 3027127

[9] J. Bourgain, A. Furman, E. Lindenstrauss and S. Mozes, Stationary measures and equidistribution for orbits of nonabelian semigroups on the torus. *J. Amer. Math. Soc.* **24** (2011), no. 1, 231–280. Zbl 1239.37005 MR 2726604

[10] J. Bourgain and A. Gamburd, Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. I. *J. Eur. Math. Soc. (JEMS)* **10** (2008), no. 4, 987–1011. Zbl 1193.20059 MR 2443926

[11] — On the spectral gap for finitely-generated subgroups of SU(2). *Invent. Math.* **171** (2008), no. 1, 83–121. Zbl 1135.22010 MR 2358056

[12] — Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$. *Ann. of Math. (2)* **167** (2008), no. 2, 625–642. Zbl 1216.20042 MR 2415383

[13] — Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. II. *J. Eur. Math. Soc. (JEMS)* **11** (2009), no. 5, 1057–1103. Zbl 1193.20060 MR 2538500

[14] — A spectral gap theorem in $\mathrm{SU}(d)$. *J. Eur. Math. Soc. (JEMS)* **14** (2012), no. 5, 1455–1511. Zbl 1254.43010 MR 2966656

[15] J. Bourgain, A. Gamburd and P. Sarnak, Affine linear sieve, expanders, and sum-product. *Invent. Math.* **179** (2010), no. 3, 559–644. Zbl 1239.11103 MR 2587341

[16] J. Bourgain and P. P. Varjú, Expansion in $SL_d(\mathbf{Z}/q\mathbf{Z})$, q arbitrary. *Invent. Math.* **188** (2012), no. 1, 151–173. Zbl 1247.20052 MR 2897695

[17] E. Breuillard, Approximate subgroups and super-strong approximation. In *Groups (St Andrews, 2013)*, pp. 1–50, London Math. Soc. Lecture Note Ser. 422, Cambridge University Press, Cambridge, 2015. Zbl 1365.11010 MR 3445486

[18] G. B. Folland, *A course in abstract harmonic analysis*. Stud. Adv. Math., CRC Press, Boca Raton, FL, 1995. Zbl 0857.43001 MR 1397028

[19] M. D. Fried and M. Jarden, *Field arithmetic*. Third edn., Ergeb. Math. Grenzgeb. (3) 11, Springer, Berlin, 2008. Zbl 1145.12001 MR 2445111

[20] G. Frobenius, Über Gruppencharaktere. *Berl. Ber.* **1896** (1896), 985–1021. Zbl 27.0092.01

[21] A. S. Golsefidy and P. P. Varjú, Expansion in perfect groups. *Geom. Funct. Anal.* **22** (2012), no. 6, 1832–1891. Zbl 1284.20044 MR 3000503

[22] W. T. Gowers, Quasirandom groups. *Combin. Probab. Comput.* **17** (2008), no. 3, 363–387. Zbl 1191.20016 MR 2410393

[23] W. He and N. de Saxcé, Linear random walks on the torus. *Duke Math. J.* **171** (2022), no. 5, 1061–1133. Zbl 1518.37005 MR 4402559

[24] H. A. Helfgott, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. *Ann. of Math. (2)* **167** (2008), no. 2, 601–623. Zbl 1213.20045 MR 2415382

[25] R. E. Howe, Kirillov theory for compact p-adic groups. *Pacific J. Math.* **73** (1977), no. 2, 365–381. Zbl 0385.22007 MR 579176

[26] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra* **32** (1974), 418–443. Zbl 0325.20008 MR 360852

[27] S. Lang and A. Weil, Number of points of varieties in finite fields. *Amer. J. Math.* **76** (1954), 819–827. Zbl 0058.27202 MR 65218

[28] A. Lubotzky, *Discrete groups, expanding graphs and invariant measures*. Mod. Birkhäuser Class., Birkhäuser, Basel, 2010. Zbl 1183.22001 MR 2569682

[29] C. R. Matthews, L. N. Vaserstein and B. Weisfeiler, Congruence properties of Zariski-dense subgroups. I. *Proc. London Math. Soc. (3)* **48** (1984), no. 3, 514–532. Zbl 0551.20029 MR 735226

[30] M. V. Nori, On subgroups of $\mathrm{GL}_n(\mathbf{F}_p)$. *Invent. Math.* **88** (1987), no. 2, 257–275. Zbl 0632.20030 MR 880952

[31] A. Salehi Golsefidy, Super-approximation, I: p-adic semisimple case. *Int. Math. Res. Not. IMRN* (2017), no. 23, 7190–7263. Zbl 1405.22025 MR 3802123

[32] — Super-approximation, II: The p-adic case and the case of bounded powers of square-free integers. *J. Eur. Math. Soc. (JEMS)* **21** (2019), no. 7, 2163–2232. Zbl 1422.22013 MR 3959861

[33] J.-P. Serre, *Lie algebras and Lie groups*. Lecture Notes in Math. 1500, Springer, Berlin, 2006. Zbl 0742.17008 MR 2179691

[34] R. Steinberg, *Endomorphisms of linear algebraic groups*. Mem. Amer. Math. Soc. 80, American Mathematical Society, Providence, RI, 1968. Zbl 0164.02902 MR 230728

[35] T. Tao and V. Vu, *Additive combinatorics*. Cambridge Stud. Adv. Math. 105, Cambridge University Press, Cambridge, 2006. Zbl 1127.11002 MR 2289012

[36] W. C. Waterhouse, *Introduction to affine group schemes*. Grad. Texts in Math. 66, Springer, New York-Berlin, 1979. Zbl 0442.14017 MR 547117

(Reçu le 11 décembre 2020)

Weikun He, Institute of Mathematics, AMSS, Chinese Academy of Sciences, 55 ZhongGuanCun East Road, Beijing 100190, P.R. China; *e-mail:* heweikun@amss.ac.cn

Nicolas de Saxcé, CNRS – LAGA, Université Sorbonne Paris Nord, Institut Galilée, 99 avenue J.-B. Clément, 93430 Villetaneuse, France; *e-mail:* desaxce@math.univ-paris13.fr