ÉQUIRÉPARTITION ADÉLIQUE DE MESURES ALGÉBRIQUES DANS UN GROUPE RÉSOLUBLE ET SOMMES DE KLOOSTERMAN

E. KOWALSKI

Abstract. This paper answers a question of Clozel and Ullmo, showing that certain sequences of adelically-defined probability measures defined on an adelic quotient of a solvable group converge to the uniform measure on that quotient. This turns out to depend on any non-trivial estimate for classical Kloosterman sums. At the end, an "horizontal" analogue of the problem is stated and solved using a result of Duke, Friedlander and Iwaniec.

1. Introduction

Le but de cette note est de répondre à une question de Clozel et Ullmo concernant un cas particulier du problème d'équirépartition de mesures algébriques introduit dans [CU], dans le cas d'un groupe résoluble.

Rappellons d'abord rapidement le contexte général (voir [CU, 1.1] pour les détails complets) : on considère un groupe algébrique $G/\mathbf{Q}$ (connexe) et un réseau de congruence $\Gamma = G(\mathbf{Q}) \cap K$ pour un sous-groupe compact ouvert $K \subset G(\mathbf{A}_f)$, $\mathbf{A}_f$ étant l'anneau des adèles finies de $\mathbf{Q}$. On regarde l'espace adélique

$$S(G,K) = G(\mathbf{Q})\backslash G(\mathbf{R})G(\mathbf{A}_f)/K \tag{1}$$

qui a un nombre fini de composantes connexes paramétrées par

$$G(\mathbf{Q})\backslash G(\mathbf{A}_f)/K,$$

dont l'une est le quotient « classique », c'est à dire $\Gamma\backslash G^+$ où G^+ est la composante connexe de l'identité de $G(\mathbf{R})$.

On se donne ensuite un sous-groupe $H \subset G$ (défini sur $\mathbf{Q}$) et $K_H = K \cap H(\mathbf{A}_f)$. Le quotient

$$S(H,K) = H(\mathbf{Q})\backslash H(\mathbf{R})H(\mathbf{A}_f)/K_H \tag{2}$$

est plongé naturellement dans $S(G,K)$ et chaque composante irréductible X est munie d'une mesure de probabilité canonique μ_X venant de la mesure de Haar.

Soit alors $\mathcal{E}^+$ l'ensemble des composantes irréducibles contenues dans la composante $\Gamma\backslash G^+$ de $S(G,K)$ et soit $\mu_{a,H}$ la mesure de probabilité

$$\mu_{a,H} = \frac{1}{|\mathcal{E}^+|}\sum_{\gamma\in\mathcal{E}^+}\mu_\gamma.$$

Finalement, on dit que la propriété $(\mathcal{E}_a)$ est vérifiée pour une suite (H_α) de sous-groupes de G comme ci-dessus si les mesures $\mu_{a,\alpha} = \mu_{a,H_\alpha}$ ainsi associées à H_α convergent faiblement vers la mesure induite par la mesure de probabilité G-invariante canonique sur l'espace classique $\Gamma\backslash G^+$.

Dans [CU], Clozel et Ullmo montrent que cette propriété est vraie dans un certain nombre de situations, tout particulièrement lorsque G est la restriction des scalaires à $\mathbf{Q}$ d'un groupe $SL(2)$ ou $PGL(2)$ sur un corps de nombre totalement réel.

Dans [CU, 2.2], le cas d'un groupe G résoluble est considéré sur un exemple particulier et la la propriété $(\mathcal{E}_a)$ démontrée (sous la forme plus forte appelée propriété $(\mathcal{E})$ dans loc. cit.) pour

2000 *Mathematics Subject Classification.* 20G35,11L05.

Key words and phrases. Equidistribution, Kloosterman sums, quadratic congruences.

une suite particulière de sous-groupes. Plus précisément, soit $k = \mathbf{Q}(i)$ et G le groupe résoluble défini sur $\mathbf{Q}$ donné par

$$G = N \rtimes T \tag{3}$$

où $N/\mathbf{Q}$ est la restriction de k à $\mathbf{Q}$ du groupe additif $\mathbf{G}_a/k$ et T est le tore défini comme noyau de la norme de k vers $\mathbf{Q}$:

$$N \,:\, \mathrm{Res}^k_{\mathbf{Q}}\mathbf{G}_m \to \mathbf{G}_m.$$

On a donc

$$T(\mathbf{R}) = \{z \in \mathbf{C} \mid |z| = 1\} \simeq \mathbf{R}/\mathbf{Z}, \quad N(\mathbf{R}) = \mathbf{C} \simeq \mathbf{R}^2$$

et $G^+ = G(\mathbf{R})$ peut se voir comme le groupe des transformations affines du plan de la forme $z \mapsto rz + n$ où $n \in \mathbf{C}$, $|r| = 1$.

On choisit les sous-groupes compacts adéliques de la manière suivante :

- Pour N, on prend $K_N = \mathbf{A}_{k,f}$, le groupe des adèles finies de k.
- Pour T, on prend $K_T = T(\mathbf{A}_f) \cap I_{k,f}(4)$, où $I_{k,f}(4)$ est le sous-groupe du groupe $I_{k,f}$ des idèles finies de k formé de ces idèles qui sont $\equiv 1 \pmod 4$. (Ce choix, plutôt que celui de $K'_T = T(\mathbf{A}_f) \cap I_{k,f}$, sera expliqué plus bas).
- Pour G, on prend $K = K_N \rtimes K_T$.

Cela étant, les sous-groupes considérés dans loc. cit. sont les tores

$$T_\alpha = \alpha T \alpha^{-1} \subset G,$$

pour $\alpha \in N(\mathbf{Q}) \simeq \mathbf{Q}(i)$, et le Corollaire 2.5 de loc. cit. dit que $(\mathcal{E})$ est vraie pour la suite T_α si $\alpha \in \mathbf{Z}[i]$ vérifie $|\alpha| \to +\infty$. Cela s'avère équivalent à l'équirépartition dans $\mathbf{R}^2/\mathbf{Z}^2$ (pour la mesure de Lebesgue) des cercles de centre 0 et de rayon $|\alpha|$ lorsque ce rayon tend vers l'infini.

La question posée [CU, p. 1266] est alors de savoir si ce résultat reste valable pour une suite α qui converge dans $\mathbf{C}$; dans ce cas les cercles correspondant ne « remplissent pas » le tore $\mathbf{R}^2/\mathbf{Z}^2$ et l'équirépartition (si elle est valide) doit faire intervenir le caractère adélique du problème.

Nous répondons à cette question ici, en nous limitant à un cas simple pour ne pas compliquer l'exposition au delà de ce avec quoi l'auteur est familier. Voici le résultat précis :

Proposition 1. *Soit G le groupe ci-dessus, $\alpha = 1/p$ où p est un nombre premier scindé dans $\mathbf{Q}(i)$, c'est à dire $p \equiv 1 \pmod 4$. Alors la suite de tores T_α associée vérifie la propriété $(\mathcal{E}_a)$.*

Cette équirépartition sera « explicitée » complètement dans la section suivante ; elle s'avère équivalente à n'importe quelle estimation non triviale de sommes de Kloosterman.

Dans la dernière section, motivée par les calculs explicites menés pour démontrer la proposition, on introduit une variante « horizontale » du problème d'équirépartition (dans ce cas particulier) ; sa solution fait appel à un résultat très profond de Duke, Friedlander et Iwaniec.

Remerciements. Je remercie E. Ullmo de m'avoir mentionné le problème et de m'avoir expliqué comment expliciter concrètement (et correctement) les différents objets adéliques qui interviennent.

Notations. On note $e(z) = e^{2i\pi z}$ pour $z \in \mathbf{C}$. Si X est un ensemble, $|X|$ est son cardinal.

2. Équirépartition et sommes de Kloosterman

En plus du groupe G défini par (3) et de ses sous-groupes N et T, on notera $T' = \mathrm{Res}^k_{\mathbf{Q}}\mathbf{G}_m$, de sorte que $T \subset T'$.

On commence par expliciter le quotient adélique (1) dans ce cas. Il s'avère être aussi simple que possible, c'est à dire qu'il n'y a qu'une composante connexe.

Lemme 2. *On a les égalités*

$$N(\mathbf{A}_f) = N(\mathbf{Q})K_N, \quad T(\mathbf{A}_f) = T(\mathbf{Q})K'_T, \quad T(\mathbf{A}_f) = T(\mathbf{Q})K_T, \quad G(\mathbf{Q})\backslash G(\mathbf{A}_f)/K = 1,$$

où les groupes de points rationnels sont plongés diagonalement dans les groupes de points adéliques finis.

Démonstration. Pour N, il s'agit du fait que $\mathbf{Z}[i]$ est principal (par identification avec le nombre de classes classique), pour T et K'_T, cela découle par exemple de [V, p. 198, p. 200] (car l'extension $k/\mathbf{Q}$ est quadratique, donc cyclique), ou de calculs simples que l'on referra plus ou moins ci-dessous.

Pour T et K_T, il suffit de remarquer que de plus $K'_T = \{\pm 1, \pm i\}K_T$ et $\{\pm 1, \pm i\} \subset T(\mathbf{Q})$.

Pour G, on se ramène à ces deux cas : soit $(n,t) \in G(\mathbf{A}_f)$. On note $n = n_1 + n_2$, $t = t_1 t_2$, où l'indice 1 correspond à un point dans $N(\mathbf{Q})$, $T(\mathbf{Q})$ respectivement, et l'indice 2 à un point dans le sous-groupe compact K_N, K_T correspondant. On a alors

$$(n,t) = (n_1 + n_2, t_1 t_2) = (n_1, 1)(n_2, 1)(0, t_1)(0, t_2) = (n_1, 1)(0, t_1)x(0, t_2)$$

où $x = (0,t_1)^{-1}(n_2,1)(0,t_1) = (n_2 t_1^{-1}, t_1^{-1})(0,t_1) = (n_2 t_1^{-1}, 1)$. Appliquant de nouveau le fait que N a nombre de classes 1, on a $x = (n_3 + n_4, 1)$ avec $n_3 \in N(\mathbf{Q})$, $n_4 \in K_N$, et donc

$$(n,t) = x_1 x_2$$

avec $x_1 = (n_1, t_1)(n_3, 1) \in G(\mathbf{Q})$, $x_2 = (n_4, t_2) \in K$. □

Le quotient adélique (1) est alors donné par

$$S(G,K) = X = (G(\mathbf{Q}) \cap K) \backslash G(\mathbf{R}).$$

Cet espace est tout à fait classique.

Lemme 3. *On a des difféomorphismes naturels*

$$X \simeq \mathbf{C}/\mathbf{Z}[i] \times T(\mathbf{R}) \simeq \mathbf{C}/\mathbf{Z}[i] \times \mathbf{R}/\mathbf{Z}.$$

Démonstration. On a $K_T \cap T(\mathbf{R}) = \{1\}$ (la seule unité de $\mathbf{Z}[i]^\times$ congrue à 1 modulo 4) et $K_N \cap N(\mathbf{R}) = \mathbf{Z}[i]$. Comme $T(\mathbf{R}) \simeq \mathbf{R}/\mathbf{Z}$, on a le résultat. □

On notera (z, θ) les coordonnées de X identifié à $\mathbf{C}/\mathbf{Z}[i] \times \mathbf{R}/\mathbf{Z}$. L'action de la seconde composante sur $\mathbf{C}/\mathbf{Z}[i]$ est évidemment donnée par $z \mapsto e(\theta)z$.

Si l'on considère le groupe compact $K' = K_N \rtimes K'_T$, le quotient correspondant est

$$X' = (G(\mathbf{Q}) \cap K') \backslash G(\mathbf{R}) \simeq U \backslash \mathbf{C}/\mathbf{Z}[i] \times U \backslash \mathbf{R}/\mathbf{Z},$$

où $U = \mathbf{Z}[i]^\times = \{\pm 1, \pm i\}$. Le choix du groupe de congruence K_T permet d'éviter ce quotient supplémentaire ennuyeux. L'analogue de la Proposition 1 reste valide cependant (par exemple parce que les fonctions sur X' s'identifient aux fonctions sur X invariante par l'action naturelle de U, et en appliquant le critère de Weyl).

La mesure de probabilité invariante canonique μ sur X vérifie

$$\int_X f d\mu = \int_{\mathbf{C}/\mathbf{Z}[i] \times \mathbf{R}/\mathbf{Z}} f(z,\theta) dz d\theta$$

pour toute fonction $f = f(z,\theta)$ sur X. Pour tester l'équirépartition sur X, on utilise le critère de Weyl ; une famille générant un sous-espace dense de l'espace des fonctions continues sur X est donnée par les caractères

$$\tau(z,\theta) = \psi(z) e(\kappa\theta) \tag{4}$$

où $\kappa \in \mathbf{Z}$ et $\psi(z)$ est un caractère additif de $\mathbf{C}/\mathbf{Z}[i]$. On a

$$\int_X \tau d\mu = \begin{cases} 1 & \text{si } \kappa = 0 \text{ et } \psi = 1 \\ 0 & \text{sinon.} \end{cases} \tag{5}$$

Revenons à l'espace adélique. On note T_α le tore conjugué $\alpha T \alpha^{-1} \subset G$ pour $\alpha \in G$, et $K_\alpha = K \cap T_\alpha$. Pour $\alpha \in N(\mathbf{Q})$ en particulier, on considère donc (cf. (2))

$$T_\alpha(\mathbf{Q}) \backslash T_\alpha(\mathbf{R}) T_\alpha(\mathbf{A}_f) / K_\alpha.$$

et l'on doit en déterminer les composantes irréductibles.

Commençons par remarquer qu'il est possible de définir T sur $\mathbf{Z}$ avec « bonne réduction » en dehors de 2 ; c'est à dire concrètement que pour tout anneau A de caractéristique $\neq 2$, on peut définir un groupe $T(A)$ comme étant

$$T(A) = \{(x, y) \in A \times A \mid x^2 + y^2 = 1\}$$

avec la loi de groupe usuelle

$$(x, y) \cdot (x', y') = (xx' - yy', xy' + yx') \in T(A).$$

De même $T'(A)$ et $N(A)$ sont définis de manière évidente ($T'(A)$ par la condition $x^2 + y^2$ inversible) et $T(A) \subset T'(A) \subset N(A)$.

Tout cela permet de parler par exemple de $T(\mathbf{Z}_p)$ ou de $T(\mathbf{Z}/p\mathbf{Z})$ pour p impair, et il y a une application de réduction naturelle $T(\mathbf{Z}_p) \to T(\mathbf{Z}/p\mathbf{Z})$. Celle ci est utilisée pour donner un sens aux congruences « multiplicatives »

$$x \equiv y \,(\mathrm{mod}\, p)$$

pour $x, y \in T(\mathbf{Z}_p)$, qui signifie que x et y ont même réduction dans $T(\mathbf{Z}/p\mathbf{Z})$. Pour une discussion intrinsèque beaucoup plus générale, on peut voir par exemple [V, 11.2].

Lemme 4. *Soit $\alpha = 1/p$ où p est un nombre premier scindé dans k. Alors il existe une bijection naturelle*

$$T(\mathbf{Z}/p\mathbf{Z}) \longrightarrow T_\alpha(\mathbf{Q})\backslash T_\alpha(\mathbf{A}_f)/K_\alpha,$$

où $T(\mathbf{Z}/p\mathbf{Z})$ est défini comme ci-dessus.

Démonstration. Supposons α quelconque pour commencer. On a

$$T_\alpha(\mathbf{A}_f) = \{(\alpha - t\alpha, t) \mid t \in T(\mathbf{A}_f)\}.$$

Le sous-groupe compact K_α est formé par ces éléments où la première composante est entière, et t est une unité. Autrement dit, K_α est l'ensemble des $(\alpha - t\alpha, t)$ où t est dans le groupe de congruence principal modulo α^{-1}, ou plus précisément, modulo $4\alpha^{-1}$, vu la définition de K_T ; c'est à dire

$$K(\alpha^{-1}) = \{t \in K_T \mid t_p \equiv 1 \,(\mathrm{mod}\, \alpha^{-1})\},$$

la composante t_p étant vue comme un élément de $T(\mathbf{Z}_p) \subset \mathbf{Q}[i] \otimes \mathbf{Q}_p$, et $\alpha^{-1} \in \mathbf{Q}[i]$. Pour $\alpha = 1/q$, $q \geqslant 1$ un entier impair, on a donc

$$K(q) = K_{T,2}(4) \times \prod_{p \nmid 2q} K_p \times \prod_{p \mid q} K_{T,p}(p^{v_p(q)})$$

où $K_{T,p}(p^m)$ est le sous-groupe de $K_{T,p}$ formé des unités (multiplicativement) congrues à 1 modulo p^m.

Pour démontrer le lemme, prenons finalement $\alpha = 1/p$ avec p scindé dans k. Fixons pour chaque $u \in T(\mathbf{Z}/p\mathbf{Z})$ une unité $t_u \in K_T \subset T(\mathbf{A}_f)$ dont les composantes $t_{u,\ell} \in T(\mathbf{Z}_p)$ vérifient

$$\begin{cases} t_{u,\ell} = 1 & \text{si } \ell \neq p \\ t_{u,p} \equiv u \,(\mathrm{mod}\, p) \end{cases} \tag{6}$$

(la congruence a bien un sens pour $t_{u,p} \in K_{T,p}$). L'existence de t_u provient de celle de $t_{u,p}$, et donc de la surjectivité de l'homomorphisme $T(\mathbf{Z}_p) \to T(\mathbf{Z}/p\mathbf{Z})$.

Vérifions ce point, qui est sans aucune doute bien connu. Notons d'abord que $x \in T'(\mathbf{Z}/p\mathbf{Z})$ est dans $T(\mathbf{Z}/p\mathbf{Z})$ si et seulement si $x = \bar{u}/u$ pour un certain $u \in T'(\mathbf{Z}/p\mathbf{Z})$, la conjugaison $\bar{u}$ étant ici l'application induite par la conjugaison complexe vue comme générateur du groupe de Galois de $k/\mathbf{Q}$. Cette caractérisation est évidente dans le cas présent où p est scindé dans k (cela reste vrai si p est inerte, par le Th. 90 de Hilbert par exemple) : on a alors un isomorphisme

$$T'(\mathbf{Z}/p\mathbf{Z}) \simeq (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/p\mathbf{Z})^\times \tag{7}$$

où la conjugaison ci-dessus s'identifie avec $\overline{(\alpha, \beta)} = (\beta, \alpha)$ et alors

$$T(\mathbf{Z}/p\mathbf{Z}) \simeq \{(\alpha, \beta) \in T'(\mathbf{Z}/p\mathbf{Z}) \mid \alpha\beta = 1\},$$

et on a bien $(\alpha,\beta) = \overline{(1,\alpha)}(1,\alpha)^{-1} = \bar{u}/u$ avec $u = (1,\alpha) \in T'(\mathbf{Z}/p\mathbf{Z})$. Soit maintenant $x \in T(\mathbf{Z}/p\mathbf{Z})$ donné, et écrivons donc $x = \bar{u}/u$. Clairement la réduction $T'(\mathbf{Z}_p) \to T'(\mathbf{Z}/p\mathbf{Z})$ est surjective, et si l'on relève u en $v \in T'(\mathbf{Z}_p)$, il est clair que $\bar{v}/v$ est dans $T(\mathbf{Z}_p)$ et se réduit en x modulo p, ce qui montre bien la surjectivité de $T(\mathbf{Z}_p) \to T(\mathbf{Z}/p\mathbf{Z})$.

Cela étant, t_u étant donc donné, soit $x_u = ((1-t_u)\alpha, t_u) \in T_\alpha(\mathbf{A}_f)$. Le lemme est la conséquence immédiate du fait que

$$T_\alpha(\mathbf{A}_f) = \bigcup_{u \in T(\mathbf{Z}/p\mathbf{Z})} T_\alpha(\mathbf{Q}) x_u K_\alpha,$$

et d'autre part du fait que

$$T_\alpha(\mathbf{Q}) x_u K_\alpha = T_\alpha(\mathbf{Q}) x_v K_\alpha \tag{8}$$

si et seulement si $v = u$.

Montrons d'abord la première égalité. Chaque terme $T_\alpha(\mathbf{Q})x_uK_\alpha$ est dans $T_\alpha(\mathbf{A}_f)$, il suffit donc de montrer l'inclusion réciproque.

Soit $t \in T(\mathbf{A}_f)$. D'après le Lemme 2, on peut trouver $\gamma \in T(\mathbf{Q})$ tel que $\beta = \gamma t \in K_T$. On peut alors parler de $\beta \pmod p \in T(\mathbf{Z}/p\mathbf{Z})$ en réduisant la composante en p. Notons u cette réduction. Il est clair que $\kappa = t_u^{-1}\beta \in K(p)$, et donc

$$t = \gamma^{-1}\beta = \gamma^{-1} t_u \kappa,$$

d'où

$$(\alpha(1-t), t) = (\alpha(1-\gamma^{-1}), \gamma^{-1}) \cdot x_u \cdot (\alpha(1-\kappa), \kappa) \in T_\alpha(\mathbf{Q}) x_u K_\alpha$$

puisque $\kappa \in K(p)$.

Il ne reste qu'à déterminer les cas d'égalité (8). Une telle égalité pour u et v implique qu'il existe $t \in T(\mathbf{Q})$ et $\kappa \in K(p)$ tels que $t_u = t t_v \kappa$. Donc $t \in T(\mathbf{Q}) \cap K_T = 1$, d'où le résultat. □

La preuve fournit une forme explicite de la bijection, qui sera utilisée dans la suite. On indexera les composantes par $u \in T(\mathbf{Z}/p\mathbf{Z})$, notant t_u et x_u des éléments comme ci-dessus. On note $h_{a,\alpha} = |T(\mathbf{Z}/p\mathbf{Z})|$ le nombre de composantes irréductibles pour $\alpha = 1/p$, p étant scindé dans k comme ci-dessus.

La propriété $(\mathcal{E}_a)$ pour la suite des tores T_α, $\alpha = 1/p$, concerne la convergence des mesures adéliques

$$\mu_{a,\alpha} = \frac{1}{h_{a,\alpha}} \sum_u \mu_u$$

vers la mesure invariante canonique μ sur $X = S(G,K)$, μ_u étant la mesure invariante canonique sur la u-ème composante, et ici u parcoure $T(\mathbf{Z}/p\mathbf{Z})$ entièrement. Pour décrire l'intégrale d'une fonction par rapport à cette mesure, on utilise le lemme suivant.

Lemme 5. *Soit $\alpha = 1/p$ avec p scindé dans k. Pour $u \in T(\mathbf{Z}/p\mathbf{Z})$, soit $x_u = ((1-\alpha)t_u, t_u)$ comme ci-dessus. On a dans $G(\mathbf{A}_f)$ une décomposition*

$$x_u = g_u k_u$$

avec g_u dans l'image de $G(\mathbf{Q})$ dans $G(\mathbf{A}_f)$ par le plongement diagonal, et $k_u \in K$, de sorte que $g_u = (\nu_u/p, 1)$ où ν_u est tel que

$$\nu_{u,p} \equiv 1 - t_{u,p} \pmod p.$$

Démonstration. D'après le Lemme 2, on sait qu'une décomposition $x_u = g_u k_u$ avec $g_u \in G(\mathbf{Q})$ et $k_u \in K$ existe. Pour déterminer g_u, posons $g_u = (n,t) \in G(\mathbf{Q})$. Alors on a

$$g_u^{-1}x_u = (n,t)^{-1}((1-t_u)/p, t_u) = (-nt^{-1}, t^{-1}((1-t_u)/p, t_u) = (t^{-1}((1-t_u)p^{-1} - n), t_u t^{-1}).$$

Si on prend $t = 1$, on aura $g_u^{-1}x_u \in K$ si $(1-t_u)/p - n$ est dans K_N. Clairement cela est vrai pour $n = \nu/p$ avec ν vérifiant la condition du lemme. □

Explicitons maintenant les plongements des composantes connexes de $T_\alpha(\mathbf{Q})\backslash T_\alpha(\mathbf{A})/K_\alpha$ dans $S(G,K) = G(\mathbf{Q})\backslash G(\mathbf{A})/K$.

Lemme 6. *Soit $\alpha = 1/p$ avec p scindé dans k, $u \in T(\mathbf{Z}/p\mathbf{Z})$ indexant la u-ème composante connexe X_u, x_u et g_u comme dans le lemme précédent. Notons $\gamma_u = g_u$ vu comme élément de $G(\mathbf{R})$. Alors le plongement $X_u \to S(G,K)$ est induit par*

$$x \mapsto \gamma_u^{-1} x_\infty$$

pour $x \in T_\alpha(\mathbf{R})$ dans la u-ème composante décomposé sous la forme

$$x = x_1 x_\infty x_u \kappa$$

avec $x_1 \in T_\alpha(\mathbf{Q})$, $x_\infty \in T_\alpha(\mathbf{R})$ et $\kappa \in K_\alpha$.

Démonstration. Notons d'abord que tout x dans la u-ème composante admet une décomposition du type décrit par définition même. L'image dans $S(G,K)$ de x est alors évidemment la même que celle de $x_\infty x_u$. Écrivons $x_u = g_u k_u$ comme dans le dernier lemme. Remarquons que $g_u \in G(\mathbf{A}_f)$ n'est *pas* dans $G(\mathbf{Q})$ plongé diagonalement dans $G(\mathbf{A}) = G(\mathbf{R}) \times G(\mathbf{A}_f)$ (il manque la composante infinie).

L'image de $x_\infty x_u$ est celle de $x_\infty g_u$. Comme $G(\mathbf{A}_f)$ commute avec $G(\mathbf{R})$ on a

$$x_\infty g_u = g_u x_\infty = g_u \gamma_u \gamma_u^{-1} x_\infty$$

et comme $g_u \gamma_u \in G(\mathbf{Q})$ (on a rajouté la composante manquante à l'infini), l'image dans $S(G,K)$ est bien celle de $\gamma_u^{-1} x_\infty$ comme annoncé. □

Vu la forme des isomorphismes

$$S(G,K) \simeq X = \Gamma \backslash (N(\mathbf{R}) \times T(\mathbf{R})) \text{ et } X_u \hookrightarrow \Gamma_{T_\alpha} \backslash T_\alpha(\mathbf{R}),$$

(où $\Gamma = \Gamma_N \simeq \mathbf{Z}[i]$ puisque $\Gamma_T = 1$), la projection de X_u dans le quotient « classique » X est donc donné par

$$t \mapsto \gamma_u^{-1} t$$

pour $t \in T_\alpha(\mathbf{R})$.

Notons que, concrètement, cela signifie aussi que le support de la mesure adélique $\mu_{a,\alpha}$ (vu dans $X \simeq \mathbf{C}/\mathbf{Z}[i] \times \mathbf{R}/\mathbf{Z}$) est l'union de $h_{a,\alpha}$ ensembles du type $C_u \times \mathbf{R}/\mathbf{Z}$, où C_u est l'image modulo $\mathbf{Z}[i]$ d'un cercle de rayon $|\alpha|$ centré en $(1-\nu_u)/p$, $u \in T(\mathbf{Z}/p\mathbf{Z})$.

Corollaire 7. *Soit toujours $\alpha = 1/p$ avec p scindé dans k, γ_u et ν_u comme décrits précédemment. Soit f une fonction intégrable sur X. L'intégrale de f pour la mesure $\mu_{a,\alpha}$ est donnée par*

$$\int f d\mu_{a,\alpha} = \frac{1}{h_{a,\alpha}} \sum_u \int_{T(\mathbf{R})} f(\gamma_u^{-1}((1-t)\alpha, t)) dt = \frac{1}{h_{a,\alpha}} \sum_u \int_{T(\mathbf{R})} f\Big(\frac{1-t-\nu_u}{p}, t\Big) dt,$$

où u parcourt $T(\mathbf{Z}/p\mathbf{Z})$.

Démonstration. Il suffit de traduire la définition de $\mu_{a,\alpha}$ et de faire un changement de variable en utilisant que $T_\alpha(\mathbf{R}) = \alpha T(\mathbf{R}) \alpha^{-1}$. □

En particulier, soit $f = \tau$, une des fonctions (4) permettant de tester l'équirépartition sur X. En utilisant le fait que $\nu_u \equiv 1 - u \pmod p$ (Lemme 5), on trouve d'après le corollaire que

$$\int \tau d\mu_{a,\alpha} = \frac{1}{h_{a,\alpha}} \sum_u \bar{\psi}\Big(\frac{u}{p}\Big) \int_0^1 \bar{\psi}\Big(\frac{e(\theta)}{p}\Big) e(\kappa\theta) d\theta.$$

On réécrit cela sous la forme

$$\int \tau d\mu_{a,\alpha} = S(\psi, p) J_\kappa(\psi, p) \tag{9}$$

où

$$S(\psi, p) = \frac{1}{|T(\mathbf{Z}/p\mathbf{Z})|} \sum_{u \in T(\mathbf{Z}/p\mathbf{Z})} \psi\Big(\frac{u}{p}\Big)$$

$$J_\kappa(\psi, p) = \int_0^1 \bar{\psi}\Big(\frac{e(\theta)}{p}\Big) e(\kappa\theta) d\theta.$$

Comme T est le tore des éléments de norme 1 dans k, la somme exponentielle $S(\psi, p)$ est une somme de Kloosterman généralisée du type considéré par Deligne ([D, 7.2]) : pour une algèbre étale $A/\mathbf{F}_p$ sur un corps fini et $b \in \mathbf{F}_p^\times$, Deligne pose

$$K_{A,b} = \sum_{N(x)=b} \eta(\mathrm{Tr}(x))$$

où η est un caractère additif de $\mathbf{F}_p$ et $N(x)$ (resp. $\mathrm{Tr}(x)$) est la norme (resp. la trace) de A vers $\mathbf{F}_p$.

Dans le cas ci-dessus, A est $N(\mathbf{Z}/p\mathbf{Z}) \simeq \mathbf{Z}[i]/p\mathbf{Z}[i]$. Il existe $c \in A$ tel que pour tout $u \in N(\mathbf{Z}/p\mathbf{Z})$ on a $\psi(u/p) = e(\mathrm{Tr}(cu)/p)$. Avec $\eta(x) = e(x/p)$, il vient

$$S(\psi, p) = \frac{1}{|T(\mathbf{Z}/p\mathbf{Z})|} K_{A,N(c)}.$$

Similairement, la fonction $J_\kappa(\psi, p)$ est une fonction de Bessel : on a

$$J_\kappa(\psi, p) = e(-\kappa\theta_0) \int_0^1 e(-R\cos\theta/p) e(\kappa\theta) d\theta = e(-\kappa\theta_0) J_\kappa\Big(\frac{2\pi R}{p}\Big),$$

où on a écrit $\psi(x + iy) = e(mx + ny)$ et $R = \sqrt{m^2 + n^2}$, θ_0 étant l'argument de $m + in$ (cette identification ne sera pas nécessaire pour la suite, la formule intégrale étant suffisante pour nos besoins). Bien évidemment on a $|S(\psi, p)| \leqslant 1$ et $|J_\kappa(\psi, p)| \leqslant 1$.

Lemme 8. (1) *Si ψ est trivial et $\kappa \neq 0$, on a*

$$\int \tau d\mu_{a,\alpha} = 0$$

pour tout α.

(2) *Si ψ est non trivial et $\kappa \neq 0$, on a*

$$\lim_{p\to+\infty} J_\kappa(\psi, p) = 0 \text{ donc } \int \tau d\mu_{a,\alpha} \to 0,$$

la limite portant sur les p premiers scindés dans k.

Démonstration. Le premier point est évident. Pour le second, $\psi(e(\theta)/p) \to 1$ quand $p \to +\infty$, donc le résultat provient du théorème de convergence dominée. □

Le seul cas « intéressant » est celui où $\psi \neq 1$ et $\kappa = 0$. Dans ce cas, par convergence dominée encore, on a $J_0(\psi, p) \to 1$ quand $p \to +\infty$. L'équirépartition dépend donc d'une majoration non triviale des sommes $S(\psi, p)$.

Deligne a montré ([D, (7.2.5),(7.1.3)]) que

$$|K_{A,b}| \leqslant np^{(n-1)/2}$$

où $n = [A : \mathbf{F}_p]$. Comme $|T(\mathbf{Z}/p\mathbf{Z})| = p - 1$ dans notre cas, cela donne

$$|S(\psi, p)| \leqslant \frac{2\sqrt{p}}{p-1} \to 0.$$

On en déduit finalement :

Proposition 9. *La suite de tores T_α avec $\alpha = 1/p$, p scindé dans k, $p \to +\infty$, vérifie la propriété $(\mathcal{E}_a)$.*

Remarque 10. La preuve de Deligne consiste à montrer que les sommes généralisées $K_{A,b}$ se ramènent aux sommes du type

$$K_{n,b} = \sum_{x_1 x_2 \cdots x_n = b} \psi(x_1 + \cdots + x_n),$$

autrement dit à $A = \mathbf{F}_p^n$, puis à estimer ces sommes par les méthodes cohomologiques ℓ-adiques. Comme $K_{2,b} = S(1, b; p)$ est une somme de Kloosterman « classique », l'estimation utilisée est

juste la borne de Weil, et on voit de plus que toute autre estimation « non triviale » serait suffisante pour démontrer la proposition, à commencer par le résultat élémentaire de Kloosterman $|S(1,b;p)| < 2p^{3/4}$, voir par exemple [I, (4.26)].

Explicitons la correspondance des sommes $S(\psi,p)$ avec une somme de Kloosterman usuelle. On écrit

$$\psi(x+iy) = e(mx+ny)$$

avec $(m,n) \in \mathbf{Z}^2$.

On a $p \equiv 1 \pmod 4$ de sorte que (comme déjà remarqué, cf. (7)), on a $\mathbf{Z}[i]/p\mathbf{Z}[i] \simeq \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ et la norme est alors donnée par $N(x,y) = xy$. Donc $T(\mathbf{Z}/p\mathbf{Z}) \simeq (\mathbf{Z}/p\mathbf{Z})^\times$. Trouvons des représentants de x_u et y_u tels que $\nu_u = x_u + iy_u$, pour $u \in (\mathbf{Z}/p\mathbf{Z})^\times$. Si $\nu \pmod p$ est une racine fixée de -1 modulo p, l'isomorphisme $\mathbf{Z}[i]/p\mathbf{Z}[i] \simeq \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ peut être donné par

$$a + ib \mapsto (a+\nu b, a-\nu b),$$

et $(\mathbf{Z}/p\mathbf{Z})^\times \simeq T(\mathbf{Z}/p\mathbf{Z}) \subset \mathbf{Z}[i]/p\mathbf{Z}[i]$ est

$$x \mapsto (x, x^{-1}).$$

On veut donc pour $x = u$ (tout est modulo p)

$$\begin{cases} x_u + \nu y_u = u \\ x_u - \nu y_u = u^{-1}, \end{cases}$$

ce qui se résout en

$$\begin{cases} x_u = \frac{1}{2}(u+u^{-1}) \\ y_u = \nu u^{-1} - x_u \end{cases}$$

donc

$$\psi\Big(\frac{u}{p}\Big) = e\Big(\frac{mx_u + ny_u}{p}\Big) = e\Big(\frac{\frac{1}{2}m(u+u^{-1}) + n(\nu u^{-1} - \frac{1}{2}\nu(u+u^{-1}))}{p}\Big) \tag{10}$$

et la somme $S(\psi,p)$ devient comme il se doit une somme de Kloosterman

$$\frac{1}{p-1}\sum_{u \pmod p}^{*} e\Big(\frac{\frac{1}{2}(m-n\nu)u + \frac{1}{2}(m+n\nu)\bar{u}}{p}\Big) = \frac{1}{p-1} S(\tfrac{1}{2}(m-n\nu), \tfrac{1}{2}(m+n\nu), p).$$

3. Un problème « horizontal »

Une remarque intéressante venant de (10) est la suivante : supposons qu'au lieu de prendre toutes les composantes u pour un p donné, on ne prenne que celles correspondant à $u \pmod p$ fixé et son inverse $\bar{u} \pmod p$, où $u \geqslant 2$ est maintenant un entier fixé quelconque (impair pour simplifier la discussion ci-dessous) premier à p. Pour tout p scindé dans k on a donc deux composantes de $T_\alpha(\mathbf{Q})\backslash T_\alpha(\mathbf{A})/K_\alpha$. (C'est pour avoir $\bar{u} \neq u$ pour tout p que l'on prend $u \neq 1$). Considérons alors pour $x \geqslant 1$ la mesure

$$\nu_x = \nu_{x,u} = \frac{1}{\rho(x)} \sum_{p \leqslant x}^{\flat} \frac{1}{2}(\mu_{u,p} + \mu_{\bar{u},p}),$$

où $\rho(x)$ est le nombre de $p \leqslant x$ qui sont $\equiv 1 \pmod 4$ et tels qu'il y ait bien deux composantes choisies, la somme $\sum^\flat$ étant restreinte à ceux-ci, $\mu_{u,p}$ désignant la mesure de probabilité naturelle sur la u-ème composante pour $\alpha = 1/p$. La question naturelle est : y-a-t-il une limite faible de ces mesures ν_x, et si oui, quelle est-elle ?

Par rapport à la propriété $(\mathcal{E}_a)$, ce problème rappelle un peu la conjecture de Sato-Tate « horizontale », par opposition à la conjecture de Sato-Tate « verticale » (cf. par exemple [Ka] ou [M]). Cependant, la signification géométrique d'un tel problème n'est pas clair, et il n'est pas non plus évident d'énoncer une généralisation pour des types de groupes G plus généraux.

On va démontrer que la limite des mesures ν_x existe effectivement. À tout le moins, le résultat permet d'exhiber un problème assez naturel où la limite n'est pas une des mesures habituelles...

En effet, définissons une mesure de probabilité ν sur X (qui dépend de u) de la manière suivante : on considère le « peigne de Farey » $\mathcal{F}_u$ dans $\mathbf{C}/\mathbf{Z}[i]$, c'est à dire l'union des (images des) droites verticales d'équations $\mathrm{Re}(z) = \{\beta/u\}$ pour $\beta \pmod u$ inversible, où $\{x\}$ est la partie fractionnaire. Soit ν la mesure de probabilité uniforme naturelle supportée sur $\mathcal{F}_u$.

Par définition, si f est une fonction sur X vue comme une fonction sur $\mathbf{C}/\mathbf{Z}[i] \times \mathbf{R}/\mathbf{Z}$ on a :

$$\int_X f(z,\theta)d\nu = \frac{1}{\varphi(u)} \sideset{}{^*}\sum_{\beta \pmod u} \int_0^1 \int_0^1 f\Big(\frac{\beta}{u} + it, \theta\Big) dt d\theta$$

où $\sum^*$ est une somme sur β inversible modulo u.

Proposition 11. *Soit $u > 1$ impair. On a pour $x \to +\infty$ la limite faible $\nu_x \to \nu$.*

Déterminons d'abord la « fonction caractéristique » de la mesure prétendûment limite.

Lemme 12. *Soit $\beta \pmod u$ inversible, $\tau(z,\theta) = e(m\,\mathrm{Re}(z) + n\,\mathrm{Im}(z) + \kappa\theta)$ avec κ, m, $n \in \mathbf{Z}$. On a*

$$\int_X \tau d\nu = \begin{cases} 0 & \text{si } \kappa \neq 0 \text{ ou } mn \neq 0 \\ \dfrac{1}{\varphi(u)} c_m(u) & \text{si } \kappa = n = 0 \text{ et } m \neq 0 \\ 1 & \text{si } \kappa = m = n = 0, \end{cases}$$

où

$$c_m(u) = \sideset{}{^*}\sum_{\beta \pmod u} e\Big(\frac{m\beta}{u}\Big)$$

est une somme de Ramanujan.

Démonstration. On a par définition

$$\int_X \tau d\nu = \frac{1}{\varphi(u)} \sideset{}{^*}\sum_{\beta \pmod u} \int_0^1 \int_0^1 e\Big(\frac{m\beta}{u} + nt + \kappa\theta\Big) dt d\theta,$$

d'où le résultat. □

D'après la remarque finale de la section précédente, la somme d'équirépartition $T(x) = T(x; m, n)$ pour $\tau(z,\theta) = e(m\,\mathrm{Re}(z) + n\,\mathrm{Im}(z) + k\theta)$ est égale à

$$\begin{aligned} T(x;m,n) &= \int \tau d\nu_x \\ &= \frac{1}{\rho(x)} \sum_{p \leqslant x}{}^\flat J_\kappa(\psi, p) \sum_{\nu^2 = -1 \pmod p} e\Big(\frac{\frac{1}{2}(m - n\nu)u + \frac{1}{2}(m + n\nu)\overline{u}}{p}\Big), \end{aligned}$$

Il est clair que pour $\kappa \neq 0$ on a $T(x) \to 0$ quand $x \to +\infty$ puisque alors $J_\kappa(\psi, p) \to 0$ pour $p \to +\infty$. Reste le cas $\kappa = 0$. Le point est que si l'on note

$$\alpha = \tfrac{1}{2}(m - n\nu)u + \tfrac{1}{2}(m + n\nu)\overline{u}, \quad \beta = \tfrac{1}{2}(m - n\nu)\overline{u} + \tfrac{1}{2}(m + n\nu)u,$$

(dans $\mathbf{Z}/p\mathbf{Z}$), de sorte que la somme sur ν est

$$e\Big(\frac{\alpha}{p}\Big) + e\Big(\frac{\beta}{p}\Big),$$

alors on voit que α et β sont les solutions modulo p d'un polynôme quadratique $P \in \mathbf{Z}[X]$ indépendant de p, à savoir

$$P_1 = 4u^2X^2 - 4m(u^3 + u)X + ((m^2 + n^2)(u^4 + 1) + 2(m^2 - n^2)u^2) \in \mathbf{Z}[X],$$

qui ne dépend que de u, m et n. Le discriminant de P_1 vaut

$$\Delta(P_1) = -16u^2n^2(u^2 - 1)^2 \leqslant 0.$$

Si le discriminant est < 0, c'est à dire $n \neq 0$ (on a pris $u \neq 1$), la somme $T(x)$ devient une somme de Weyl pour l'équirépartition des racines du polynôme quadratique irréductible P modulo les nombres premiers (si $p \equiv 3 \pmod 4$, il n'y a évidemment pas de solutions modulo p.) D'après Duke, Friedlander et Iwaniec ([DFI], voir aussi [Ko]), les racines de ceux-ci deviennent équiréparties quand $x \to +\infty$, donc $T(x) \to 0$ si $n \neq 0$.

Reste les cas $n = 0$ (et toujours $k = 0$). En repartant de la définition on a

$$T(x) = T(x; m, 0) = \frac{1}{\rho(x)} \sideset{}{^\flat}\sum_{p \leqslant x} J_0(\psi, p) e\Big(\frac{\frac{1}{2}m(u + \overline{u})}{p}\Big).$$

On élimine le $\bar{u}$ indésirable en notant (une astuce favorite en théorie analytique des nombres !) que dans $\mathbf{R}/\mathbf{Z}$ on a

$$\frac{\bar{u}}{p} = -\frac{\bar{p}}{u} + \frac{1}{up},$$

donc

$$e\Big(\frac{\frac{1}{2}m\bar{u}}{p}\Big) = e\Big(\frac{-\frac{1}{2}m\bar{p}}{u}\Big) + O(p^{-1})$$

(puisque u et m sont supposés fixés). La nouvelle exponentielle est périodique de période u donc en scindant la somme définissant $S(x)$ suivant les classes modulo u, on trouve la somme

$$\frac{1}{\rho(x)} \sideset{}{^*}\sum_{\alpha \,(\mathrm{mod}\, u)} e\Big(\frac{-\frac{1}{2}m\bar{\alpha}}{u}\Big) \sideset{}{^\flat}\sum_{\substack{p \leqslant x \\ p \equiv \alpha \,(\mathrm{mod}\, u)}} J_0(\psi, p) e\Big(\frac{\frac{1}{2}mu}{p}\Big) + O(x^{-1}(\log x)(\log\log x)).$$

Dans la somme intérieure, pour tout α, le terme général tend vers 1 quand $p \to +\infty$, puisque $J_0(\psi, p) \to 1$. D'après Cesaro et le théorème des nombres premiers en progression arithmétique, on a

$$\frac{1}{\rho(x)} \sideset{}{^\flat}\sum_{\substack{p \leqslant x \\ p \equiv \alpha \,(\mathrm{mod}\, u)}} J_0(\psi, p) e\Big(\frac{\frac{1}{2}mu}{p}\Big) \to \frac{1}{\varphi(u)}$$

quand $x \to +\infty$. Donc on trouve que $T(x; m, 0)$ a une limite quand $x \to +\infty$, à savoir

$$\frac{1}{\varphi(u)} \sideset{}{^*}\sum_{\alpha \,(\mathrm{mod}\, u)} e\Big(\frac{-\frac{1}{2}m\bar{\alpha}}{u}\Big) = \frac{1}{\varphi(u)} \sum_{\beta \,(\mathrm{mod}\, u)} e\Big(\frac{m\beta}{u}\Big).$$

Comparant avec le Lemme 12, on a donc bien démontré la Proposition 11.

Remarque 13. Vu l'interprétation de la mesure ν comme supportée sur un « peigne » avec des segments d'abcisses $\{\beta/u\}$, puisque de plus ces parties fractionnaires deviennent équiréparties dans $[0, 1]$ quand $u \to +\infty$, on retrouve bien qu'en prenant des u de plus en plus grand, tout devient équiréparti (mais ici après sommation sur p alors que les sommes de Kloosterman montrent que c'est vrai sans que cela soit nécessaire).

Remarque 14. Il peut paraître artificiel de prendre u et $\bar{u}$ plutôt que u tout seul, mais le point est qu'il faut avoir les deux racines de la congruence quadratique pour avoir équirépartition.[1] Vu autrement, l'association « globale » d'une composante connexe pour $\alpha = 1/p$ à partir d'un entier u fixé n'est pas canoniquement définie (en raison du choix de ν pour fixer l'isomorphisme $T(\mathbf{Z}/p\mathbf{Z}) \simeq (\mathbf{Z}/p\mathbf{Z})^\times$), mais la paire des deux composantes associées à u et $\bar{u}$ est bien définie.

[1] Sinon il se pourrait qu'on ait toujours celle qui est entre 0 et $p/2$...

Références

[CU] L. Clozel et E. Ullmo : *Équidistribution de mesures algébriques*, Compositio Math. 141 (2005), 1255–1309.

[D] P. Deligne : *Sommes trigonométriques*, dans S.G.A $4\frac{1}{2}$, Springer Lecture Notes 569, 1977.

[DFI] W. Duke, J. Friedlander, H. Iwaniec : *Equidistribution of roots of a quadratic congruence to prime moduli*, Ann. of Math. (2) 141 (1995), 423–441.

[I] H. Iwaniec : *Topics in classical automorphic forms*, Grad. Studies in Math. 17, A.M.S (1997).

[Ka] N. Katz : *Gauss sums, Kloosterman sums and monodromy groups*, Annals of Math. Studies 116, Princeton Univ. Press (1988).

[Ko] E. Kowalski : *Un cours de théorie analytique des nombres*, S.M.F Cours Spécialisé 13 (2004).

[M] P. Michel : *Autour de la conjecture de Sato-Tate pour les sommes de Kloosterman, I*, Invent. math. 121 (1995), 61–78.

[V] V. E. Voskresenskiĭ : *Algebraic groups and their birational invariants*, Translations of Mathematical Monographs 179, A.M.S (1998).

Université Bordeaux I - A2X, 351, cours de la Libération, 33405 Talence Cedex, France
E-mail address: emmanuel.kowalski@math.u-bordeaux1.fr