

ÉQUIRÉPARTITION DE SOMMES EXPONENTIELLES

[Travaux de Katz]

par Javier FRESÁN

1. INTRODUCTION

Cent ans se sont écoulés depuis la parution de l'article de Weyl [48] sans que les résultats d'équirépartition en théorie des nombres cessent de faire florès, révélant des liens profonds avec la géométrie algébrique et la théorie des représentations. L'interaction de ces domaines est particulièrement riche dans les travaux de Katz dont il sera question ici. Ce sont des théorèmes, anciens et récents, d'équirépartition de sommes exponentielles sur les corps finis, le plus souvent à caractéristique fixée. Les sommes concernées s'obtiennent par transformation de Fourier, relative à un caractère, de la fonction trace d'un faisceau ℓ -adique sur un groupe algébrique commutatif, et il s'agit de comprendre leur répartition lorsque le faisceau est fixe mais que l'on fait varier le caractère.

1.1. L'exemple des sommes de Gauss et des sommes de Kloosterman

Soient p un nombre premier, q une puissance de p et \mathbf{F}_q un corps fini à q éléments. Étant donné un caractère additif non trivial $\psi: \mathbf{F}_q \rightarrow \mathbf{C}^\times$ et un caractère multiplicatif $\chi: \mathbf{F}_q^\times \rightarrow \mathbf{C}^\times$, on définit la *somme de Gauss* $g(\psi, \chi)$ comme l'entier algébrique

$$g(\psi, \chi) = \sum_{x \in \mathbf{F}_q^\times} \psi(x)\chi(x).$$

Par exemple, si $q = p$ et si l'on prend pour ψ le caractère $x \mapsto \exp(2\pi ix/p)$ et pour χ le symbole de Legendre, il s'agit de la somme considérée par Gauss dans sa quatrième preuve de la loi de réciprocité quadratique [12].

Si χ est trivial, la somme de Gauss vaut -1 ; sinon, sa valeur absolue est égale à \sqrt{q} . Choisissons, pour chaque p , un caractère non trivial ψ_p de \mathbf{F}_p et notons ψ_q le caractère de \mathbf{F}_q obtenu par composition avec la trace. Gardant ψ_q fixe et faisant varier χ parmi les caractères multiplicatifs non triviaux, on obtient $q - 2$ points

$$\theta_{q,\chi} = \frac{g(\psi_q, \chi)}{\sqrt{q}}$$

dans le cercle unité S^1 . Comment ces points se répartissent-ils quand q tend vers l'infini ?

Soient (X, μ) un espace topologique compact muni d'une mesure de probabilité μ et (S_N) une suite⁽¹⁾ d'ensembles finis non vides avec des applications $\theta_N: S_N \rightarrow X$. Rappelons que les (S_N, θ_N) sont dits *équirépartis selon μ* si la suite de mesures $|S_N|^{-1} \sum_{x \in S_N} \delta_{\theta_N(x)}$ converge vaguement vers μ lorsque N tend vers l'infini, c'est-à-dire si, pour toute fonction continue $f: X \rightarrow \mathbf{C}$, on a l'égalité

$$\int_X f(x) \mu(x) = \lim_{N \rightarrow \infty} \frac{1}{|S_N|} \sum_{x \in S_N} f(\theta_N(x)).$$

Il suffit en fait de la vérifier pour une classe de fonctions test dont les combinaisons linéaires finies sont denses dans l'espace $\mathcal{C}(X)$ des fonctions continues à valeurs complexes muni de la topologie de la convergence uniforme.

Dans le cas qui nous occupe, Katz remarqua dans [17, §1.3.3] que la majoration des sommes de Kloosterman obtenue par Deligne comme conséquence de ses travaux sur la conjecture de Weil entraînait le résultat d'équirépartition suivant :

THÉORÈME 1.1 (Deligne). — *Lorsque q tend vers l'infini, les points $\{\theta_{q,\chi}\}_{\chi \neq 1}$ s'équirépartissent selon la mesure de Haar normalisée sur le cercle unité. Autrement dit, pour toute fonction continue $f: S^1 \rightarrow \mathbf{C}$ on a l'égalité*

$$(1) \quad \frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta}) d\theta = \lim_{q \rightarrow \infty} \frac{1}{q-2} \sum_{\chi \neq 1} f(\theta_{q,\chi}).$$

Comme les polynômes de Laurent sont denses dans $\mathcal{C}(S^1)$, il suffit de considérer les fonctions $f(z) = z^n$ avec n entier. Le cas $n = 0$ est évident. Le membre gauche de (1) étant nul pour $n \neq 0$, il faut démontrer que la suite

$$\frac{1}{q-2} \sum_{\chi \neq 1} f(\theta_{q,\chi}) = \frac{1}{q^{\frac{n}{2}}(q-2)} \sum_{\chi \neq 1} g(\psi_q, \chi)^n$$

converge vers zéro lorsque q tend vers l'infini (c'est le *critère d'équirépartition de Weyl*). Grâce à la relation $g(\psi_q, \chi)^{-1} = g(\bar{\psi}_q, \bar{\chi})q^{-1}$, on peut se ramener à $n \geq 1$, auquel cas les puissances des sommes de Gauss sont égales à

$$(2) \quad \begin{aligned} g(\psi_q, \chi)^n &= \sum_{x_1, \dots, x_n \in \mathbf{F}_q^\times} \psi_q(x_1 + \dots + x_n) \chi(x_1 \cdots x_n) \\ &= \sum_{a \in \mathbf{F}_q^\times} \chi(a) \sum_{\substack{x_1, \dots, x_n \in \mathbf{F}_q^\times \\ x_1 \cdots x_n = a}} \psi_q(x_1 + \dots + x_n). \end{aligned}$$

1. Bien que l'on utilise N comme paramètre, dans les énoncés qui suivent la suite n'est pas forcément indexée par des entiers mais par des caractères, des points d'une variété algébrique, etc.

Il s'ensuit que $\chi \mapsto g(\psi_q, \chi)^n$ est la transformée de Fourier, au sens du groupe abélien fini \mathbf{F}_q^\times , de la fonction qui à un élément $a \in \mathbf{F}_q^\times$ associe la *somme de Kloosterman*

$$\mathrm{Kl}_n(a, q) = \sum_{\substack{x_1, \dots, x_n \in \mathbf{F}_q^\times \\ x_1 \cdots x_n = a}} \psi_q(x_1 + \dots + x_n).$$

Pour $n = 2$, ces sommes font un caméo dans l'article posthume de Poincaré sur les formes modulaires, où il « se borne à constater » qu'elles ne sont pas nulles en général⁽²⁾ [39, p. 148]. Kloosterman les introduisit de manière indépendante en 1926, en raffinant la méthode du cercle pour étudier l'asymptotique du nombre de représentations d'un entier par une forme quadratique définie positive en quatre variables [29]. Un point clé de son travail est la majoration $|\mathrm{Kl}_2(a, q)| < 2q^{3/4}$, qu'il obtint en calculant le quatrième moment

$$(3) \quad \sum_{a \in \mathbf{F}_q^\times} \mathrm{Kl}_2(a, q)^4 = 2q^3 - 3q^2 - 3q - 1.$$

Quelques années plus tard, Salié [43] et Davenport [7] purent améliorer l'exposant de $3/4$ à $2/3$ en estimant le sixième moment. Puis en 1934 Hasse observa, en comparant la somme de Kloosterman au nombre de solutions de l'équation $y^q - y = x + ax^{-1}$, que la borne optimale $2\sqrt{q}$ découlait de l'hypothèse de Riemann pour les courbes sur les corps finis [15]; avec la preuve de Weil entre 1940 et 1948, elle fut enfin établie [46].

Trouver la majoration optimale pour les sommes de Kloosterman en plusieurs variables est une tâche significativement plus compliquée qui requiert l'analogie de l'hypothèse de Riemann pour la cohomologie à coefficients dans un faisceau ℓ -adique. En la démontrant dans l'article [9], auquel on se référera comme « Weil II » par la suite, Deligne ouvrit la voie à de nombreuses applications à l'étude des sommes exponentielles que nous sommes encore loin d'avoir épuisées. Lui-même exposa le principe de la méthode dans [8], où il montre comment en déduire l'estimée

$$|\mathrm{Kl}_n(a, q)| \leq nq^{\frac{n-1}{2}}$$

pour n'importe quels $n \geq 2$ et $a \in \mathbf{F}_q^\times$. C'est ce qu'il fallait pour conclure la preuve.

FIN DE LA DÉMONSTRATION — En sommant la formule (2) sur les caractères multiplicatifs non triviaux, il vient

$$\sum_{\chi \neq 1} g(\psi_q, \chi)^n = -g(\psi, 1)^n + \sum_{a \in \mathbf{F}_q^\times} \mathrm{Kl}_n(a, q) \sum_{\chi} \chi(a) = (-1)^{n+1} + (q-1)\mathrm{Kl}_n(1, q)$$

par orthogonalité des caractères. D'après la majoration de Deligne, nous avons donc

$$\left| \frac{1}{q^{\frac{n}{2}}(q-2)} \sum_{\chi \neq 1} g(\psi_q, \chi)^n \right| \leq \frac{2n+1}{\sqrt{q}}$$

2. Les sommes de Poincaré portent sur $(\mathbf{Z}/q\mathbf{Z})^\times$ et peuvent être nulles. Celles que l'on considère ici ne le sont *jamais*, car $\mathrm{Kl}_2(a, q)$ appartient au sous-anneau de \mathbf{C} engendré par une racine primitive p -ème de l'unité ζ_p et l'on a $\mathrm{Kl}_2(a, q) \equiv -1$ modulo l'idéal premier $1 - \zeta_p$.

pour tout $q > 2$ et la limite du membre gauche est bien zéro lorsque $q \rightarrow \infty$. \square

Remarque 1.2. — Le théorème s’applique tant à la situation où p est fixe et l’on fait tendre q vers l’infini parmi les puissances de p qu’à la situation où p varie aussi, ce qui est possible car la constante dans la majoration des moments (en l’occurrence $2n + 1$) est indépendante de p . En théorie analytique des nombres, on parle souvent d’équirépartition *verticale* ou *horizontale* pour distinguer ces deux cas.

Revenons maintenant aux sommes de Kloosterman. Comme appliquer la conjugaison complexe revient à échanger x_i et $-x_i$ dans l’expression de $\text{Kl}_2(a, q)$, ce sont des nombre réels (il en va de même pour tout n pair). Au vu de la borne de Weil, pour chaque $a \in \mathbf{F}_q^\times$, il existe un unique angle $\theta_{q,a} \in [0, \pi]$ tel que

$$\text{Kl}_2(a, q) = 2\sqrt{q} \cos \theta_{q,a}.$$

Comment ces $q - 1$ angles varient-ils avec q ? En s’appuyant sur l’interprétation de la somme $\text{Kl}_2(a, q)$ comme la trace de Frobenius en $a \in \mathbb{G}_m(\mathbf{F}_q)$ d’un système local ℓ -adique sur \mathbb{G}_m et sur un théorème de Deligne affirmant que la répartition de telles traces est gouvernée par le groupe de monodromie, Katz démontra dans [18] que les angles $\{\theta_{q,a}\}_{a \in \mathbf{F}_q^\times}$ se répartissent comme les classes de conjugaison de matrices aléatoires dans le groupe spécial unitaire $\text{SU}(2)$. Plus précisément, si l’on identifie l’intervalle $[0, \pi]$ à l’espace de ces classes par l’application qui envoie θ sur la classe de conjugaison de $\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$, l’image directe de la mesure de Haar normalisée sur $\text{SU}(2)$ par la projection canonique est la mesure $(2/\pi) \sin^2 \theta d\theta$ sur $[0, \pi]$. Elle porte en théorie des nombres le nom de *mesure de Sato–Tate*, d’après leur célèbre conjecture sur la répartition du terme d’erreur dans l’approximation par $p + 1$ du nombre de points de la réduction modulo p d’une courbe elliptique sur \mathbf{Q} sans multiplication complexe.

THÉORÈME 1.3 (Katz). — *Lorsque q tend vers l’infini, les angles $\{\theta_{q,a}\}_{a \in \mathbf{F}_q^\times}$ s’équirépartissent selon la mesure de Sato–Tate, c’est-à-dire pour toute fonction continue $f: [0, \pi] \rightarrow \mathbf{C}$ on a l’égalité*

$$\frac{2}{\pi} \int_0^\pi f(\theta) \sin^2 \theta d\theta = \lim_{q \rightarrow \infty} \frac{1}{q-1} \sum_{a \in \mathbf{F}_q^\times} f(\theta_{q,a}).$$

À nouveau, ce résultat est valable pour n’importe quelle suite de corps finis de cardinaux croissants. On conjecture également que, pour un entier fixe a , les angles $\{\theta_{p,a}\}_{p \leq N}$ s’équirépartissent selon la mesure de Sato–Tate lorsque p tend vers l’infini parmi les nombres premiers ne divisant pas a , mais même des conséquences faibles de cet énoncé paraissent hors de portée à l’heure actuelle⁽³⁾.

3. Mentionnons, à titre d’exemple, la *conjecture du changement de signe* : puisque $\sin^2 \theta$ est symétrique par rapport à $\theta = \pi/2$ et que les $\text{Kl}_2(a, p)$ sont tous non nuls, il devrait y avoir asymptotiquement autant de premiers p pour lesquels la somme de Kloosterman est positive que négative. On n’en sait rien ! Dans [10], Fouvry et Michel démontrent des résultats dans cette direction quand la

1.2. Les sommes d’Evans et de Rudnick

Autour de 2003, Evans et Rudnick trouvèrent d’autres exemples de sommes exponentielles dépendant d’un caractère multiplicatif qui, d’après leurs expériences numériques, semblaient s’équirépartir selon la mesure de Sato–Tate. D’un côté, Evans étudia les sommes

$$S(\chi) = -\frac{1}{\sqrt{q}} \sum_{x \in \mathbf{F}_q^\times} \chi(x) \psi_q(x - x^{-1}),$$

qui sont des nombres réels de valeur absolue au plus 2 par l’hypothèse de Riemann sur les courbes. Ils s’écrivent donc $S(\chi) = 2 \cos \theta_{q,\chi}$ pour un unique $\theta_{q,\chi} \in [0, \pi]$. Est-il vrai que les angles $\{\theta_{q,\chi}\}_\chi$ s’équirépartissent selon la mesure de Sato–Tate quand q tend vers l’infini ? Ou, ce qui revient au même, les sommes $S(\chi)$ s’équirépartissent-elles selon la mesure du demi-cercle $(1/2\pi)\sqrt{4-x^2} dx$ sur l’intervalle $[-2, 2]$?

À la même époque, Rudnick rencontra des sommes semblables dans ses travaux sur le chaos quantique. Décrivons brièvement le contexte, en nous référant à [32], [33] et [42] pour plus de détails. Il s’agit de quantifier le système dynamique obtenu en itérant la transformation du tore $T^2 = \mathbf{R}^2/\mathbf{Z}^2$ définie par une matrice hyperbolique $A \in \mathrm{SL}(2, \mathbf{Z})$, des applications connues comme « cat maps » dans la littérature. Soient $N \geq 1$ un entier et \mathcal{H}_N l’espace de Hilbert $L^2(\mathbf{Z}/N\mathbf{Z})$. On pense à N comme à l’inverse de la constante de Planck \hbar , de sorte que la limite semi-classique $\hbar \rightarrow 0$ devienne $N \rightarrow \infty$. Après avoir associé à chaque observable classique $f: T^2 \rightarrow \mathbf{R}$ de classe \mathcal{C}^∞ un opérateur autoadjoint $\mathrm{Op}_N(f)$ sur \mathcal{H}_N (l’observable quantique), une quantification de A est une suite d’opérateurs unitaires $U_N(A)$ sur \mathcal{H}_N vérifiant la formule d’Egoroff

$$U_N(A)^* \mathrm{Op}_N(f) U_N(A) = \mathrm{Op}_N(f \circ A)$$

pour toute observable f . Si $\varphi_1, \dots, \varphi_N$ est une base orthonormale de \mathcal{H}_N formée de vecteurs propres pour l’opérateur $U_N(A)$, on sait que la moyenne des espérances $\langle \mathrm{Op}_N(f) \varphi_i, \varphi_i \rangle$ converge vers $\int_{T^2} f(x) dx$ lorsque N tend vers l’infini. Est-ce encore vrai pour chaque terme pris individuellement ?

Dans [32], Kurlberg et Rudnick observent que A admet une quantification qui ne dépend que de la réduction de la matrice modulo $2N$, ce qui leur permet d’introduire une classe d’opérateurs d’origine arithmétique sur \mathcal{H}_N qu’ils appellent opérateurs de Hecke. Le théorème d’*unique ergodicité quantique* est l’énoncé que, si les φ_i sont simultanément des fonctions propres pour $U_N(A)$ et les opérateurs de Hecke, on a

$$\lim_{N \rightarrow \infty} \langle \mathrm{Op}_N(f) \varphi_i, \varphi_i \rangle = \int_{T^2} f(x) dx$$

pour tout i . Comment les espérances $\langle \mathrm{Op}_N(f) \varphi_i, \varphi_i \rangle$ fluctuent-elles autour de la limite ? Puisque l’on s’attend à ce que le terme d’erreur soit génériquement d’ordre $1/\sqrt{N}$, il

suite des p est remplacée par une suite de nombres « presque premiers », c’est-à-dire non premiers, sans facteur carré et ayant un nombre de facteurs premiers borné uniformément.

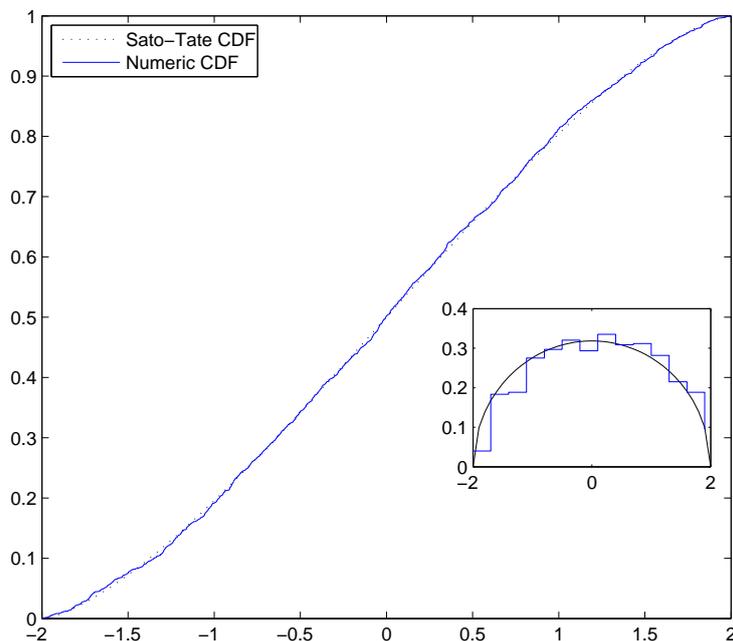


FIGURE 1. Comparaison entre la fonction de répartition des fluctuations pour la matrice $A = \begin{pmatrix} 7 & -2 \\ 4 & -1 \end{pmatrix}$ et le premier $p = 1997$ et celle d'une variable aléatoire pour la mesure du demi-cercle, d'après Rosenzweig [41].

est naturel de considérer les fluctuations définies par

$$F_i^{(N)} = \sqrt{N} \left(\langle \text{Op}_N(f) \varphi_i, \varphi_i \rangle - \int_{T^2} f(x) dx \right).$$

Prenons pour N un nombre premier $p \geq 3$ tel que la matrice A soit diagonalisable modulo p , disons par une matrice de passage P . Dans ce cas, chaque caractère multiplicatif χ de \mathbf{F}_p donne lieu à une fonction propre $\varphi_\chi = U_N(P)\chi$ pour $U_N(A)$ et les opérateurs de Hecke. À un facteur près, les fluctuations des φ_χ sont les sommes

$$E(\chi) = -\frac{1}{\sqrt{p}} \sum_{x \in \mathbf{F}_p \setminus \{0,1\}} \chi(x) \psi_p((x+1)/(x-1)).$$

Si χ n'est pas trivial, $E(\chi)$ est encore un nombre réel compris entre -2 et 2 . Des expériences numériques (figure 1) suggèrent que les $\{E(\chi)\}_{\chi \neq 1}$ s'équirépartissent selon la mesure du demi-cercle lorsque p tend vers l'infini. Peut-on le démontrer ?

Dans ce texte, nous expliquerons comment un théorème de Katz [22] permet entre autres d'apporter une réponse positive aux questions d'Evans et de Rudnick. Leur difficulté vient du fait que, n'étant pas les traces de Frobenius d'un même système local ℓ -adique, ces familles de sommes exponentielles indexées par des caractères multiplicatifs ne rentrent pas dans le cadre du théorème d'équirépartition de Deligne. Il

faut notamment trouver un substitut du groupe de monodromie : c'est là que le formalisme tannakien nous viendra en aide. Avant d'énoncer le théorème principal, nous illustrerons la démarche par les sommes de Gauss ⁽⁴⁾.

1.3. La méthode ℓ -adique

Posons $k = \mathbf{F}_q$ et fixons une clôture algébrique \bar{k} de k . Soient ℓ un nombre premier distinct de p et $\overline{\mathbf{Q}}_\ell$ une clôture algébrique du corps des nombres ℓ -adiques. Le choix d'un plongement $\iota: \overline{\mathbf{Q}}_\ell \hookrightarrow \mathbf{C}$ induit un isomorphisme entre les clôtures algébriques de \mathbf{Q} dans $\overline{\mathbf{Q}}_\ell$ et dans \mathbf{C} par le biais duquel on peut voir les caractères à valeurs dans $\overline{\mathbf{Q}}_\ell^\times$. Soit donc $\psi: k \rightarrow \overline{\mathbf{Q}}_\ell^\times$ un caractère additif non trivial. Considérons une clôture séparable $k(T)^{\text{sep}}$ du corps des fractions rationnelles et une solution $U \in k(T)^{\text{sep}}$ de l'équation d'Artin–Schreier $U - U^q = T$. L'extension $k(T, U)$ est galoisienne sur $k(T)$ de groupe k , un élément $a \in k$ opérant par $U \mapsto U + a$. Notons \mathcal{L}_ψ la représentation

$$\text{Gal}(k(T)^{\text{sep}}/k(T)) \longrightarrow \text{Gal}(k(T, U)/k(T)) \cong k \xrightarrow{\psi} \overline{\mathbf{Q}}_\ell^\times$$

obtenue par composition de la surjection canonique avec le caractère ψ . Identifiant $k(T)$ au corps de fonctions de la droite projective \mathbb{P}_k^1 , on voit que \mathcal{L}_ψ est non ramifiée en dehors de l'infini. Par suite, pour chaque point x de la droite affine \mathbb{A}_k^1 à valeurs dans une extension finie E de k , la classe de conjugaison $\text{Frob}_{E,x}$ dans le groupe $\text{Gal}(k(T)^{\text{sep}}/k(T))$ définie par le Frobenius géométrique de $\text{Gal}(\bar{k}/E)$ agit sur $\overline{\mathbf{Q}}_\ell^\times$ au travers de la représentation \mathcal{L}_ψ . Pour calculer cette action, notons n le degré de E sur k . Si $y \in \bar{k}$ satisfait à l'équation $y - y^q = x$, alors $y^{q^j} = y^{q^{j-1}} - x^{q^{j-1}}$ pour tout entier $j \geq 1$; sommant sur les $j = 1, \dots, n$, on trouve que la substitution de Frobenius est donnée par $y \mapsto y^{q^n} = y - \text{Tr}_{E/k}(x)$. Le Frobenius géométrique étant son inverse, on en déduit après application du caractère ψ que la classe de conjugaison $\text{Frob}_{E,x}$ agit sur l'espace de la représentation \mathcal{L}_ψ comme la multiplication par $\psi(\text{Tr}_{E/k}(x))$.

De même, à partir de l'équation de Kummer $U^{1-q} = T$, on peut associer à chaque caractère multiplicatif $\chi: k^\times \rightarrow \overline{\mathbf{Q}}_\ell^\times$ une représentation \mathcal{L}_χ de $\text{Gal}(k(T)^{\text{sep}}/k(T))$ à valeurs dans $\overline{\mathbf{Q}}_\ell^\times$, cette fois-ci ramifiée en zéro et l'infini, telle que la classe de conjugaison $\text{Frob}_{E,x}$ agisse par multiplication par $\chi(N_{E/k}(x))$ pour tout $x \in E^\times$. En termes de ces représentations, la somme de Gauss s'écrit

$$g(\psi, \chi) = \sum_{x \in \mathbf{F}_q^\times} \text{Tr}(\text{Frob}_{E,x} | \mathcal{L}_\psi \otimes \mathcal{L}_\chi).$$

Dans le langage plus géométrique que l'on adoptera ici, \mathcal{L}_ψ et \mathcal{L}_χ sont des systèmes locaux ℓ -adiques de rang un sur \mathbb{A}_k^1 et sur $\mathbb{G}_{m,k}$ respectivement ; on notera encore \mathcal{L}_ψ la restriction à $\mathbb{G}_{m,k}$. Pour des raisons pour l'instant mystérieuses, il est préférable de

4. La recension [30] est un excellent point d'entrée aux idées de la preuve. L'exemple des sommes de Gauss est certes très particulier, en ce sens que pour déterminer leur répartition il suffit d'estimer leurs puissances n -ièmes et que l'on arrive à identifier celles-ci avec les sommes de Kloosterman, mais en l'interprétant géométriquement on y voit déjà apparaître tous les ingrédients essentiels.

travailler avec l'objet $M = \mathcal{L}_\psi(1/2)[1]$. Le symbole $(1/2)$ désigne une *demi-torsion à la Tate*, dont l'effet est de multiplier les traces de Frobenius par $1/\sqrt{q}$, et le décalage $[1]$ indique que l'on regarde $\mathcal{L}_\psi(1/2)$ non pas comme un faisceau mais comme un complexe concentré en degré -1 , ce qui change le signe des traces. Ainsi M est un objet de la catégorie dérivée $D_c^b(\mathbb{G}_{m,k}, \overline{\mathbf{Q}}_\ell)$ de faisceaux ℓ -adiques sur $\mathbb{G}_{m,k}$. Grâce au décalage, il appartient en fait à une sous-catégorie *abélienne* formée d'objets avec des propriétés remarquables que l'on appelle *faisceaux pervers*, même s'il s'agit plutôt de complexes.

Étant donné une extension finie E de k et un caractère multiplicatif $\chi: E^\times \rightarrow \overline{\mathbf{Q}}_\ell^\times$, l'objet $M \otimes \mathcal{L}_\chi$ est encore un faisceau pervers sur $\mathbb{G}_{m,E}$ dont les groupes de cohomologie à support compact s'annulent en degré non nul. En degré zéro,

$$\omega_\chi(M) = H_c^0(\mathbb{G}_{m,\bar{k}}, M \otimes \mathcal{L}_\chi)$$

est une $\overline{\mathbf{Q}}_\ell$ -droite munie d'une action du groupe $\text{Gal}(\bar{k}/E)$, en particulier du Frobenius géométrique F_E . La formule des traces de Grothendieck est dans ce cas l'égalité

$$(4) \quad \text{Tr}(F_E | \omega_\chi(M)) = \sum_{x \in E^\times} \text{Tr}(\text{Frob}_{E,x} | M \otimes \mathcal{L}_\chi) = -\frac{1}{\sqrt{|E|}} \sum_{x \in E^\times} \psi(x)\chi(x).$$

La distinction selon que le caractère χ soit trivial ou non se reflète dans l'action de Frobenius sur $\omega_\chi(M)$, qui est en l'occurrence réduite à la multiplication par le nombre ℓ -adique (4). À travers le plongement $\iota: \overline{\mathbf{Q}}_\ell \hookrightarrow \mathbf{C}$, on peut parler de sa valeur absolue : elle est égale à 1 si et seulement si χ n'est pas trivial. Pour des objets M plus généraux, on dira qu'un caractère multiplicatif χ est *bon* pour M si toutes les valeurs propres de F_E agissant sur $\omega_\chi(M)$ sont unitaires.

1.4. Convolution et équirépartition

L'étape suivante consiste à introduire une opération sur les faisceaux relevant le produit des sommes exponentielles ; c'est là que la structure de groupe sur $\mathbb{G}_{m,k}$ intervient. Pour ce faire, on définit sur la catégorie dérivée $D_c^b(\mathbb{G}_{m,k}, \overline{\mathbf{Q}}_\ell)$ un produit de *convolution*

$$M \star_! N = Rm_!(\text{pr}_1^* M \otimes \text{pr}_2^* N),$$

où pr_1 et pr_2 désignent les projections de $\mathbb{G}_{m,k} \times \mathbb{G}_{m,k}$ sur les deux facteurs et m la loi de multiplication. Un premier obstacle est que ce produit ne préserve pas les faisceaux pervers, à moins de se restreindre à une sous-catégorie convenable $\mathbf{P}(\mathbb{G}_{m,k})$. Un second point technique est que l'objet $M \star_! N$ doit être remplacé par un quotient $M \star_{\text{int}} N$ que l'on appelle convolution *intermédiaire*. Si M et N sont des faisceaux pervers dans $\mathbf{P}(\mathbb{G}_{m,k})$ pour lesquels un caractère χ est bon, on a un isomorphisme

$$\omega_\chi(M \star_{\text{int}} N) \cong \omega_\chi(M) \otimes \omega_\chi(N)$$

compatible à l'action de Frobenius. D'après Gabber et Loeser [11], avec la convolution intermédiaire pour produit tensoriel, $\mathbf{P}(\mathbb{G}_{m,k})$ a la structure d'une catégorie *tannakienne* dans laquelle l'objet neutre est le faisceau gratte-ciel supporté en 1, le dual M^\vee est le

tiré en arrière du dual de Verdier $\mathbb{D}(M)$ par l'inversion $x \mapsto x^{-1}$ et les objets ont pour dimension leur caractéristique d'Euler.

Concrètement, on se servira de cette information de la manière suivante. Soit $\langle M \rangle^\otimes$ la sous-catégorie de $\mathbf{P}(\mathbb{G}_{m,k})$ formée des objets qui s'obtiennent à partir de M en itérant les opérations produit tensoriel, dual, somme directe et sous-quotient, autrement dit qui sont des sous-quotients d'une *construction tensorielle* $M^{r,s} = \bigoplus M^{\otimes r_i} \otimes (M^\vee)^{\otimes s_i}$; c'est la plus petite sous-catégorie tannakienne de $\mathbf{P}(\mathbb{G}_{m,k})$ contenant l'objet M . De plus, ω_χ est un foncteur fibre sur $\langle M \rangle^\otimes$ pour tout bon caractère χ et les automorphismes linéaires de $\omega_\chi(M)$ agissent naturellement sur tous les $\omega_\chi(M^{r,s})$. Soit

$$G_{M,\chi} \subseteq \mathrm{GL}(\omega_\chi(M))$$

le sous-groupe de ceux laissant globalement stables les images par ω_χ de n'importe quel sous-quotient de $M^{r,s}$. C'est un sous-groupe algébrique défini sur $\overline{\mathbf{Q}}_\ell$ dont la catégorie des représentations de dimension finie est, par la théorie tannakienne, équivalente à $\langle M \rangle^\otimes$. On aura également besoin de prendre en compte le faisceau pervers $M_{\bar{k}}$ sur $\mathbb{G}_{m,\bar{k}}$ déduit de M par extension des scalaires. Comme ses constructions tensorielles ont plus de sous-quotients à respecter, le groupe correspondant est *a priori* plus petit; pour les distinguer, on notera $G_{\mathrm{arith},M,\chi}$ celui de M et $G_{\mathrm{geom},M,\chi}$ celui de $M_{\bar{k}}$ et on les appellera arithmétique et géométrique respectivement.

Le Frobenius F_E est un automorphisme de $\omega_\chi(M)$ vérifiant la propriété de stabilité ci-dessus et définit ainsi un élément $\mathrm{Frob}_{E,\chi}$ dans le groupe $G_{\mathrm{arith},M,\chi}$. Si l'on change de caractère, on change de groupe, la dépendance en χ étant la même que celle du groupe fondamental d'un espace topologique en le point base : tous les $G_{\mathrm{arith},M,\chi}$ sont isomorphes entre eux par des isomorphismes uniques à des automorphismes intérieurs près. On peut alors fixer un caractère χ_0 et voir les différents $\mathrm{Frob}_{E,\chi}$ comme des classes de conjugaison dans le même groupe $G_{\mathrm{arith},M,\chi_0}$, que l'on notera simplement $G_{\mathrm{arith},M}$. On ne sait pas si $\mathrm{Frob}_{E,\chi}$ est diagonalisable mais, quitte à prendre sa semisimplification $\mathrm{Frob}_{E,\chi}^{\mathrm{ss}}$ au sens de la décomposition de Jordan, on obtient une classe de conjugaison semisimple dans $G_{\mathrm{arith},M}(\overline{\mathbf{Q}}_\ell)$ avec des valeurs propres unitaires, que l'on peut ensuite regarder dans $G_{\mathrm{arith},M}(\mathbf{C})$ via le plongement $\iota: \overline{\mathbf{Q}}_\ell \hookrightarrow \mathbf{C}$.

Les propriétés des objets d'une catégorie tannakienne se traduisent en des propriétés de leurs groupes et *vice versa*. Par exemple, si M est somme directe d'objets simples, alors le groupe $G_{\mathrm{arith},M}$ est réductif car il possède une représentation fidèle et complètement réductible. Supposons que c'est le cas et choisissons un sous-groupe compact maximal K du groupe de Lie complexe $G_{\mathrm{arith},M}(\mathbf{C})$. Chaque élément dans $\mathrm{Frob}_{E,\chi}^{\mathrm{ss}}$ est alors conjugué à un élément dans K , qui est à son tour bien défini à conjugaison près par un élément de K . On en déduit une classe de conjugaison $\theta_{E,\chi}$ dans K dont les traces $\mathrm{Tr}(\theta_{E,\chi})$ ne sont rien d'autre que les sommes exponentielles

$$S(M, E, \chi) = \sum_{x \in E^\times} \chi(x) \mathrm{Tr}(\mathrm{Frob}_{E,x} | M)$$

que l'on souhaite étudier. On y pense comme aux transformées de Fourier, relatives aux caractères χ , de la *fonction trace* $x \mapsto \text{Tr}(\text{Frob}_{E,x}|M)$ sur le groupe multiplicatif E^\times . Comment varient-elles lorsque le degré des extensions E/k tend vers l'infini ?

Voici le résultat principal de cet exposé :

THÉORÈME 1.4 (Katz). — *Soit M un faisceau pervers dans $\mathbf{P}(\mathbb{G}_{m,k})$. Supposons que M est ι -pur de poids zéro, semisimple, et que les groupes $G_{\text{geom},M}$ et $G_{\text{arith},M}$ coïncident. Lorsque le degré des extensions E/k tend vers l'infini, les éléments $\{\theta_{E,\chi}\}_{\chi \text{ bon}}$ s'équirépartissent dans l'espace des classes de conjugaison dans K selon la mesure induite par la mesure de Haar normalisée.*

En particulier, les sommes $S(M, E, \chi)$ varient comme les traces de matrices aléatoires dans K . Il ne reste plus qu'à calculer le groupe $G_{\text{arith},M}$. L'avantage du point de vue tannakien est que l'on dispose de maintes techniques pour le faire. On cherche d'abord des bornes par le haut en étudiant la géométrie de M et de ses constructions tensorielles, puis des bornes par le bas en exhibant des éléments explicites dans $G_{\text{arith},M}$. Une fois ces contraintes obtenues, la théorie des représentations permet souvent de conclure qu'il n'y a qu'un seul groupe les satisfaisant. Dans le cas des sommes de Gauss, $G_{\text{geom},M}$ est par définition un sous-groupe de $\text{GL}(1)$; comme aucune puissance de convolution de M n'est égale à l'objet neutre, il s'agit forcément de $\text{GL}(1)$ tout entier, si bien que l'on retrouve le théorème 1.1. Quant aux objets associés aux sommes d'Evans et de Rudnick, on verra que leurs groupes arithmétiques et géométriques sont dans les deux cas égaux à $\text{SL}(2)$; l'équirépartition des angles $\theta_{q,\chi}$ selon la mesure de Sato–Tate en découle.

Le texte est organisé comme suit. Le numéro 2 contient des rappels des résultats sur les faisceaux ℓ -adiques qui seront utilisés au long du texte ; j'ai essayé de les rendre aussi accessibles que possible. Dans le numéro 3, on présente le théorème d'équirépartition de Deligne et ses applications aux sommes de Kloosterman, puis on explique pourquoi ce résultat permet d'établir la variante additive de l'équirépartition des sommes $S(M, E, \chi)$. Enfin, le numéro 4 est consacré aux résultats de la monographie [22], notamment le théorème 1.4, une version horizontale et les trois exemples ci-dessus. J'aurais voulu aussi parler des applications du théorème de Katz en théorie analytique des nombres ([3], [14], [23], [25], [28], [49]), du cas des courbes elliptiques ([5], [24]), de l'approche tannakienne aux conjectures d'équirépartition horizontale [44] et des théorèmes d'annulation générique pour les faisceaux pervers sur les variétés abéliennes ([31], [47]), mais cela aurait fait de ce texte un séminaire-fléuve...

Remerciements — Ils vont tout d'abord à Nick Katz pour la joie des livres orange (renouvelée à chaque lecture!), puis à Henryk Iwaniec et à Emmanuel Kowalski, qui m'ont demandé en premier de présenter ces résultats dans un séminaire informel à l'ETH. Je tiens à remercier aussi Olivier Benoist, Brian Conrad, Nick Katz, Arthur Forey, Emmanuel Kowalski, Corentin Perret-Gentil, Lior Rosenzweig et Zeév Rudnick pour l'aide qu'ils m'ont apportée au cours de la rédaction de ce texte.

2. RAPPELS SUR LES FAISCEAUX ℓ -ADIQUES

Dans ce numéro, on fait un tour rapide de la théorie des systèmes locaux et des faisceaux constructibles ℓ -adiques. On rappelle notamment la notion de poids et le théorème principal de Weil II, qui sera l'outil essentiel pour obtenir les majorations des sommes exponentielles requises par le critère d'équirépartition de Weyl.

2.1. Groupe fondamental étale

Pour tout schéma connexe X , notons $\mathbf{Fét}_X$ la catégorie des revêtements finis étales $Y \rightarrow X$. Soit $\xi: \text{Spec}(\Omega) \rightarrow X$ un *point géométrique* de X , où Ω est un corps algébriquement clos. En associant à chaque $Y \rightarrow X$ l'ensemble sous-jacent à la fibre $Y_\xi = Y \times_X \text{Spec}(\Omega)$, on obtient un foncteur

$$\text{Fib}_\xi: \mathbf{Fét}_X \longrightarrow \mathbf{Ensembles\ finis}.$$

Dans [1], Grothendieck définit *le groupe fondamental étale avec point base ξ* comme le groupe $\pi_1(X, \xi)$ des automorphismes de Fib_ξ , c'est-à-dire les familles $(\sigma_{Y_\xi})_{Y \rightarrow X}$ de permutations σ_{Y_ξ} des ensembles finis Y_ξ telles que $\sigma_{Y'_\xi} = f \circ \sigma_{Y_\xi}$ pour tout morphisme de X -schémas $f: Y \rightarrow Y'$. Par suite, $\pi_1(X, \xi)$ est un groupe *profini*, muni en particulier d'une topologie. Comme en théorie de Galois classique, on a

$$\pi_1(X, \xi) \cong \varprojlim \text{Aut}_X(Y),$$

la limite étant prise sur les revêtements finis étales *galoisiens*, pour lesquels le schéma Y est connexe et le groupe $\text{Aut}_X(Y)$ agit transitivement sur Y_ξ .

Puisque X est supposé connexe, les foncteurs fibre Fib_{ξ_1} et Fib_{ξ_2} définis par deux points géométriques ξ_1 et ξ_2 sont isomorphes. Le choix d'un isomorphisme, que l'on appelle parfois *chemin* par analogie avec la topologie, induit un isomorphisme continu

$$\pi_1(X, \xi_1) \simeq \pi_1(X, \xi_2)$$

qui ne dépend du chemin qu'à un automorphisme intérieur près.

De plus, la formation du groupe fondamental est *covariante* : un morphisme de schémas $f: X \rightarrow X'$ induit un homomorphisme continu $f_*: \pi_1(X, \xi) \rightarrow \pi_1(X', f \circ \xi)$. Pour un autre choix de point base ξ' sur X' , on peut encore parler de l'homomorphisme

$$f_*: \pi_1(X, \xi) \rightarrow \pi_1(X', \xi'),$$

mais celui-ci n'a un sens qu'à conjugaison près.

Exemple 2.1. — Si X est le spectre d'un corps k , un point géométrique ξ est un corps algébriquement clos L contenant k , et le groupe fondamental $\pi_1(X, \xi)$ s'identifie au groupe de Galois $\text{Gal}(k^{\text{sep}}/k)$ de la clôture séparable k^{sep} de k dans L . En particulier, si k est un corps fini à q éléments, ce groupe est canoniquement isomorphe à la complétion profinie $\widehat{\mathbf{Z}}$ de \mathbf{Z} , avec générateur la substitution de Frobenius $x \mapsto x^q$. On appellera

Frobenius géométrique l'inverse F_k de ce générateur. Pour une extension E de degré n sur k , l'homomorphisme induit par $\text{Spec}(E) \rightarrow \text{Spec}(k)$ envoie F_E sur F_k^n .

Soient k un corps, \bar{k} une clôture algébrique de k , X une variété géométriquement connexe sur k et $X_{\bar{k}}$ son extension des scalaires à \bar{k} . Pour tout $\xi: \text{Spec}(\bar{k}) \rightarrow X_{\bar{k}}$, on a d'après un théorème de Grothendieck [1] la suite exacte

$$(5) \quad 1 \longrightarrow \pi_1(X_{\bar{k}}, \xi) \longrightarrow \pi_1(X, \xi) \longrightarrow \text{Gal}(\bar{k}/k) \longrightarrow 1,$$

où les flèches non triviales sont induites par $X_{\bar{k}} \rightarrow X$ et $X \rightarrow \text{Spec}(k)$. En particulier, si k est un corps fini, on dispose d'une application *degré* $\pi_1(X, \xi) \rightarrow \widehat{\mathbf{Z}}$.

Voici la description galoisienne du groupe fondamental d'une courbe. Soit C une courbe projective, lisse et géométriquement connexe sur un corps parfait k , avec corps de fonctions $K = k(C)$ et point générique $\eta: \text{Spec}(K) \rightarrow C$. Fixons une clôture algébrique \bar{K} de K et notons $\bar{\eta}$ le point géométrique au-dessus de η qu'elle définit. Chaque point fermé x de C donne lieu à une valuation discrète $v: K^\times \rightarrow \mathbf{Z}$ de corps résiduel $\kappa(x)$, qui se prolonge en une valuation discrète \bar{v} sur K^{sep} (deux tels prolongements sont conjugués sous l'action de $\text{Gal}(K^{\text{sep}}/K)$, et choisir \bar{v} revient à choisir un point géométrique \bar{x} au-dessus de x). Soient $K_{\bar{v}}^{\text{sep}}$ et K_v les complétés par rapport aux valuations \bar{v} et v . Le *groupe de décomposition* de \bar{v} est le stabilisateur

$$D_{\bar{x}} = \{g \in \text{Gal}(K^{\text{sep}}/K) \mid \bar{v} \circ g = \bar{v}\},$$

que l'on peut identifier au groupe de Galois de l'extension locale $K_{\bar{v}}^{\text{sep}}/K_v$. Par passage aux corps résiduels, on obtient une surjection $D_{\bar{x}} \rightarrow \text{Gal}(\bar{k}/\kappa(x))$, où \bar{k} est la clôture algébrique de k dans \bar{K} . Son noyau est par définition le *groupe d'inertie* $I_{\bar{x}}$.

PROPOSITION 2.2. — *Soit U un ouvert non vide de C . Le groupe fondamental étale de U avec point base $\bar{\eta}$ est le quotient de $\text{Gal}(K^{\text{sep}}/K)$ par le plus petit sous-groupe fermé distingué contenant $I_{\bar{x}}$ pour tout x dans U .*

En particulier, le groupe fondamental d'un ouvert de la droite projective \mathbb{P}_k^1 s'identifie à un quotient de $\text{Gal}(k(T)^{\text{sep}}/k(T))$; c'est le point de vue que l'on a adopté dans l'introduction pour définir les représentations \mathcal{L}_ψ et \mathcal{L}_χ .

2.2. Systèmes locaux ℓ -adiques et traces de Frobenius

Dorénavant, k désigne un corps fini à q éléments, ℓ un nombre premier différent de la caractéristique de k et X une variété lisse et géométriquement connexe sur k , de point générique η . Pour tout point fermé $x: \text{Spec}(E) \rightarrow X$, l'homomorphisme continu

$$x_*: \text{Gal}(\bar{k}/E) \longrightarrow \pi_1(X, \bar{\eta})$$

est bien défini à conjugaison près. L'image du Frobenius géométrique F_E par x_* est une classe de conjugaison⁽⁵⁾ dans $\pi_1(X, \bar{\eta})$, que l'on notera $\text{Frob}_{E,x}$.

DÉFINITION 2.3. — Un système local ℓ -adique \mathcal{L} de rang r sur X est la donnée d'un espace vectoriel $\mathcal{L}_{\bar{\eta}}$ de dimension r sur $\overline{\mathbf{Q}}_{\ell}$ et d'un homomorphisme continu

$$\rho: \pi_1(X, \bar{\eta}) \rightarrow \text{GL}(\mathcal{L}_{\bar{\eta}}).$$

Soit \mathcal{L} un système local ℓ -adique de rang r sur X . Puisque le groupe profini $\pi_1(X, \bar{\eta})$ est compact, moyennant le choix d'une base de $\mathcal{L}_{\bar{\eta}}$, l'image de ρ est un sous-groupe compact de $\text{GL}(r, \overline{\mathbf{Q}}_{\ell})$. Un tel sous-groupe est toujours contenu dans $\text{GL}(r, E_{\lambda})$ pour une extension finie E_{λ} de \mathbf{Q}_{ℓ} , et l'on peut même choisir la base de sorte que ρ prenne des valeurs dans l'anneau des entiers de cette extension [27, §9.0.7].

L'image de $\text{Frob}_{E,x}$ par la représentation ρ est une classe de conjugaison dans $\text{GL}(\mathcal{L}_{\bar{\eta}})$. Sa trace est donc un élément bien défini de $\overline{\mathbf{Q}}_{\ell}$, d'où une fonction trace

$$t_{\mathcal{L}}: X(E) \longrightarrow \overline{\mathbf{Q}}_{\ell}, \quad x \longmapsto \text{Tr}(\text{Frob}_{E,x} | \mathcal{L})$$

pour toute extension finie E de k . Les opérations usuelles sur les représentations (produit tensoriel, dual, etc.) fournissent de nouveaux systèmes locaux dont les fonctions trace s'expriment en termes des anciennes. Par exemple, on a $t_{\mathcal{L}_1 \otimes \mathcal{L}_2} = t_{\mathcal{L}_1} \cdot t_{\mathcal{L}_2}$ pour le produit tensoriel et, si $f: Y \rightarrow X$ est un morphisme de k -variétés lisses, le système local $f^* \mathcal{L}$ sur Y défini par la représentation $\rho \circ f_*$ a fonction trace $t_{f^* \mathcal{L}} = t_{\mathcal{L}} \circ f$.

Exemple 2.4. — Soit α une unité dans l'anneau des entiers de $\overline{\mathbf{Q}}_{\ell}$. L'unique homomorphisme continu $\widehat{\mathbf{Z}} \rightarrow \overline{\mathbf{Q}}_{\ell}^{\times}$ qui envoie 1 sur α définit un système local ℓ -adique de rang un sur $\text{Spec}(k)$; d'après la remarque après la définition 2.3, ils sont tous de cette forme. Par composition avec l'application degré $\pi_1(X, \xi) \rightarrow \widehat{\mathbf{Z}}$, on obtient un système local ℓ -adique de rang un sur X . Comme l'image de $\text{Frob}_{E,x}$ par la représentation associée est $\alpha^{[E:k]}$, il sera noté α^{deg} . Au vu de la suite exacte (5), les α^{deg} sont précisément les caractères du groupe fondamental dont la restriction à $\pi_1(X_{\bar{k}}, \xi)$ est triviale. Si $\alpha = q^n$ pour un entier n , on écrit $\overline{\mathbf{Q}}_{\ell}(-n)$ plutôt que $(q^n)^{\text{deg}}$. Si $\alpha \in \overline{\mathbf{Q}}_{\ell}$ est une racine carrée de $1/q$, les traces du système local $\mathcal{L} \otimes \alpha^{\text{deg}}$, que l'on notera $\mathcal{L}(1/2)$, sont celles de \mathcal{L} multipliées par $1/\sqrt{|E|}$; c'est la *demi-torsion à la Tate* de l'introduction.

Exemple 2.5. — Soit G un schéma en groupes commutatifs lisse et connexe sur k , la loi de groupe étant notée additivement. Soit F_G le morphisme de Frobenius absolu, c'est-à-dire le morphisme de k -schémas $F_G: G \rightarrow G$ qui est l'identité sur l'espace topologique sous-jacent et $x \mapsto x^q$ sur le faisceau structural \mathcal{O}_G . L'*isogénie de Lang*

$$\text{id} - F_G: G \rightarrow G$$

5. Avec les notations du paragraphe précédent, quand X est une courbe, il s'agit de l'image de F_E par $\text{Gal}(\bar{k}/E) \rightarrow \text{Gal}(\bar{k}/\kappa(x)) \cong D_{\bar{x}}/I_{\bar{x}} \hookrightarrow \text{Gal}(K^{\text{sep}}/K)/I_{\bar{x}} \rightarrow \pi_1(X, \bar{\eta})$. Comme l'on a dû choisir un point géométrique \bar{x} au-dessus de x pour définir $D_{\bar{x}}$, on obtient seulement une classe de conjugaison.

est un revêtement fini étale galoisien de groupe $G(k)$. Si G est le groupe additif, c'est le *revêtement d'Artin–Schreier* $x \mapsto x - x^q$ de la droite affine \mathbb{A}_k^1 et, si G est le groupe multiplicatif, c'est le *revêtement de Kummer* $x \mapsto x^{1-q}$ de $\mathbb{G}_{m,k}$.

Étant donné un caractère $\varphi: G(k) \rightarrow \overline{\mathbf{Q}}_\ell^\times$, la représentation

$$\pi_1(G, \bar{\eta}) \longrightarrow G(k) \xrightarrow{\varphi} \overline{\mathbf{Q}}_\ell^\times$$

obtenue en composant la surjection canonique associée à l'isogénie de Lang avec le caractère φ définit un système local ℓ -adique \mathcal{L}_φ de rang un sur G . Plus généralement, pour tout morphisme de k -schémas $f: X \rightarrow G$, on obtient un système local de rang un $f^*\mathcal{L}_\varphi$ sur X qu'il est coutumier de noter $\mathcal{L}_{\varphi(f)}$. Pour chaque point de X à valeurs dans E , en raisonnant comme dans le paragraphe 1.3 de l'introduction, on trouve

$$t_{\mathcal{L}_{\varphi(f)}}(x) = \mathrm{Tr}(\mathrm{Frob}_{E,x} | \mathcal{L}_{\varphi(f)}) = \varphi(\mathrm{Tr}_{E/k}^G f(x)),$$

où $\mathrm{Tr}_{E/k}^G$ désigne la trace au sens du groupe abélien $G(E)$, c'est-à-dire la trace $\mathrm{Tr}_{E/k}$ si G est le groupe additif, la norme $N_{E/k}$ si G est le groupe multiplicatif, etc.

Exemple 2.6. — Soit $f: \mathbb{G}_m \rightarrow \mathbb{A}^1$ la fonction $x \mapsto x - x^{-1}$. Le système local $\mathcal{L}_{\psi_q(f)}$ induit par le caractère additif $\psi_q: \mathbf{F}_q \rightarrow \overline{\mathbf{Q}}^\times$ a trace de Frobenius $\psi_q(x - x^{-1})$ en le point $x \in \mathbf{F}_q^\times$. Les sommes d'Evans sont donc égales à

$$S(\chi) = - \sum_{x \in \mathbf{F}_q^\times} \mathrm{Tr}(\mathrm{Frob}_{\mathbf{F}_q,x} | \mathcal{L}_\chi \otimes \mathcal{L}_{\psi_q}(1/2)).$$

De même, en prenant pour $f: \mathbb{G}_m \setminus \{1\} \rightarrow \mathbb{A}^1$ la fonction $(x+1)/(x-1)$, les sommes de Rudnick peuvent se récrire en termes du système local $\mathcal{L}_{\psi_q(f)}$.

Le cadre des systèmes locaux ℓ -adiques, par opposition aux faisceaux constructibles que l'on introduira dans le paragraphe suivant, est peu adapté aux méthodes cohomologiques. Par exemple, si $\chi: k^\times \rightarrow \overline{\mathbf{Q}}_\ell^\times$ est un caractère et $f: X \rightarrow \mathbb{G}_{m,k}$ un morphisme de k -variétés, $\chi(f(x))$ est bien la trace de Frobenius en x du système local $\mathcal{L}_{\chi(f)}$ sur X , mais il est souvent plus commode d'utiliser l'égalité

$$\sum_{x \in X(k)} \chi(f(x)) = \sum_{t \in k^\times} \chi(t) |f^{-1}(t)|$$

et de voir $t \mapsto |f^{-1}(t)|$ comme une fonction trace sur $\mathbb{G}_{m,k}$. Ceci correspond à étudier la variation en t de la cohomologie des fibres $f^{-1}(t)$ et l'on doit s'attendre à ce que seule la restriction à un ouvert de lissité de f soit la trace d'un système local.

2.3. Faisceaux constructibles, poids et cohomologie

Vers la fin des années 50, Grothendieck définit une « topologie » sur les schémas où la notion classique d'ouvert d'une variété X est remplacée par les morphismes étales vers X . Si A est un anneau de torsion, par exemple $\mathbf{Z}/\ell^n \mathbf{Z}$, on peut parler de faisceaux localement constants (aussi appelés *lisses*) et de faisceaux constructibles de A -modules

sur X , ces derniers ayant la propriété qu'il existe une stratification de X telle que la restriction à chaque strate soit un faisceau lisse. Par un double passage à la limite, d'abord sur les entiers n , puis sur les extensions finies de \mathbf{Q}_ℓ , on dégage la notion de $\overline{\mathbf{Q}}_\ell$ -faisceau constructible. On ne se contentera ici que de quelques aperçus.

Soit \mathcal{F} un faisceau constructible sur X . La fibre \mathcal{F}_ξ en un point géométrique ξ est un espace vectoriel de dimension finie sur $\overline{\mathbf{Q}}_\ell$. Si \mathcal{F} est lisse, le groupe fondamental $\pi_1(X, \bar{\eta})$ agit continument sur la fibre $\mathcal{F}_{\bar{\eta}}$ en un point géométrique générique $\bar{\eta}$ et le foncteur $\mathcal{F} \mapsto \mathcal{F}_{\bar{\eta}}$ induit une équivalence de catégories entre les $\overline{\mathbf{Q}}_\ell$ -faisceaux lisses et les systèmes locaux ℓ -adiques sur X . En général, quel que soit \mathcal{F} , la fibre $\mathcal{F}_{\bar{x}}$ en un point géométrique \bar{x} au-dessus de $x \in X(E)$ est un système local ℓ -adique sur $\text{Spec}(E)$, d'où une action du Frobenius F_E qui permet d'étendre la définition de fonction trace à tout faisceau constructible.

Soit C une courbe projective, lisse et géométriquement connexe sur k . Si \mathcal{F} est un faisceau lisse sur un ouvert non vide $V \subseteq C$, pour tout point fermé $x \in C$, le groupe de décomposition $D_{\bar{x}}$ agit sur $\mathcal{F}_{\bar{\eta}}$ au travers de la flèche $D_{\bar{x}} \rightarrow \pi_1(V, \bar{\eta})$. On en déduit une action du groupe d'inertie $I_{\bar{x}}$ pour tout $x \in C \setminus V$, celle de $I_{\bar{x}}$ pour $x \in V$ étant triviale par la description galoisienne du groupe fondamental (proposition 2.2). Concrètement, un $\overline{\mathbf{Q}}_\ell$ -faisceau constructible \mathcal{F} sur une courbe U est la donnée :

- d'un ouvert non vide $V \hookrightarrow U$ et d'un faisceau ℓ -adique lisse $\mathcal{F}_{\bar{\eta}}$ sur V correspondant à une représentation continue $\pi_1(V, \bar{\eta}) \rightarrow \text{GL}(\mathcal{F}_{\bar{\eta}})$,
- pour chaque point fermé $u \in U \setminus V$, d'une représentation continue de $\text{Gal}(\bar{k}/\kappa(u))$ dans un $\overline{\mathbf{Q}}_\ell$ -espace vectoriel de dimension finie $\mathcal{F}_{\bar{u}}$,
- des *flèches de spécialisation* $\text{Gal}(\bar{k}/\kappa(u))$ -équivariantes $\text{sp}_{\bar{u}, \bar{\eta}}: \mathcal{F}_{\bar{u}} \rightarrow \mathcal{F}_{\bar{\eta}}^{I_{\bar{u}}}$ (les données de recollement).

Exemple 2.7. — Quelques opérations naturelles sur les faisceaux constructibles, par exemple les images directes par une immersion ouverte, admettent aussi une description en ces termes. Si \mathcal{F} est un faisceau constructible sur U et $j: U \hookrightarrow U'$ une immersion ouverte, le *prolongement par zéro* $j_! \mathcal{F}$ (resp. l'*image directe* $j_* \mathcal{F}$) est le faisceau constructible sur U' qui coïncide avec \mathcal{F} sur U et qui a fibre $(j_! \mathcal{F})_{\bar{x}} = 0$ (resp. $(j_* \mathcal{F})_{\bar{x}} = \mathcal{F}_{\bar{\eta}}^{I_{\bar{x}}}$, avec flèche de spécialisation l'identité) en tout point fermé x dans le complémentaire. L'*image directe supérieure* $R^1 j_* \mathcal{F}$ est le faisceau constructible supporté dans $U' \setminus U$ et ayant pour fibre en un point x les coinvariants sous l'inertie $(R^1 j_* \mathcal{F})_x = (\mathcal{F}_{\bar{\eta}})_{I_{\bar{x}}}(-1)$.

Soit X une variété lisse et géométriquement connexe, purement de dimension d , sur un corps fini k . À un $\overline{\mathbf{Q}}_\ell$ -faisceau constructible \mathcal{F} sur X on associe des *groupes de cohomologie* $H^i(X_{\bar{k}}, \mathcal{F})$ et de *cohomologie à support compact* $H_c^i(X_{\bar{k}}, \mathcal{F})$. Ce sont des espaces vectoriels de dimension finie sur $\overline{\mathbf{Q}}_\ell$, munis d'une action continue de $\text{Gal}(\bar{k}/k)$, qui s'annulent en degrés $i < 0$ et $i > 2d$. Pour chaque i , il y a une flèche canonique d'« oubli des supports » $H_c^i(X_{\bar{k}}, \mathcal{F}) \rightarrow H^i(X_{\bar{k}}, \mathcal{F})$ qui est un isomorphisme lorsque X

est propre. Si le faisceau \mathcal{F} est lisse sur X , on a

$$H^0(X_{\bar{k}}, \mathcal{F}) = (\mathcal{F}_{\bar{\eta}})^{\pi_1(X_{\bar{k}}, \bar{\eta})}, \quad H_c^{2d}(X_{\bar{k}}, \mathcal{F}) = (\mathcal{F}_{\bar{\eta}})_{\pi_1(X_{\bar{k}}, \bar{\eta})}(-d)$$

et le groupe de Galois opère sur ces espaces par le biais de l'action de $\pi_1(X, \bar{\eta})$ sur $\mathcal{F}_{\bar{\eta}}$ et de l'identification $\text{Gal}(\bar{k}/k) = \pi(X, \bar{\eta})/\pi_1(X_{\bar{k}}, \bar{\eta})$ donnée par la suite exacte (5). En général, un faisceau constructible \mathcal{F} peut avoir des sections globales ponctuelles non nulles (elles correspondent aux éléments dans le noyau des flèches de spécialisation).

Le lien entre les sommes exponentielles et l'action du Frobenius géométrique F_k sur la cohomologie à support compact est fourni par la formule des traces [13] :

THÉORÈME 2.8 (Formules des traces de Grothendieck). — *Pour toute extension finie E de k , on a l'égalité*

$$\sum_{x \in X(E)} \text{Tr}(\text{Frob}_{E,x} | \mathcal{F}) = \sum_{i=0}^{2d} (-1)^i \text{Tr}(F_E | H_c^i(X_{\bar{k}}, \mathcal{F})).$$

Cette formule n'acquiert toute sa force qu'en combinaison avec des estimées sur les valeurs propres de l'endomorphisme F_E : le formalisme des poids de la cohomologie. Pour pouvoir parler de la taille de ces valeurs propres, qui sont des éléments dans $\overline{\mathbf{Q}}_\ell$, on fixe un plongement $\iota: \overline{\mathbf{Q}}_\ell \hookrightarrow \mathbf{C}$.

DÉFINITION 2.9. — *Soient w un entier et \mathcal{F} un faisceau constructible sur X .*

(a) *On dit que \mathcal{F} est ι -pur de poids w si, pour toute extension finie E de k et pour tout point $x \in X(E)$, les valeurs propres de $\text{Frob}_{E,x}$ agissant sur la fibre $\mathcal{F}_{\bar{x}}$, où \bar{x} est un point géométrique quelconque au-dessus de x , ont valeur absolue $|E|^{w/2}$ quand on les regarde dans \mathbf{C} à travers le plongement ι .*

(b) *On dit que \mathcal{F} est ι -mixte s'il admet une filtration finie croissante par des sous-faisceaux constructibles $(\mathcal{F}_i)_{i \in \mathbf{Z}}$ dont les gradués $\text{gr}_i = \mathcal{F}_i/\mathcal{F}_{i-1}$ sont ι -purs de poids i . Si les poids des gr_i sont majorés (resp. minorés) par w , on dira que \mathcal{F} est ι -mixte de poids $\leq w$ (resp. $\geq w$).*

Le poids d'un faisceau dépend a priori fortement du plongement ι ; on dira que \mathcal{F} est *pur de poids w* s'il est ι -pur de poids w pour tout $\iota: \overline{\mathbf{Q}}_\ell \hookrightarrow \mathbf{C}$. Pour des questions concernant les faisceaux purs, quitte à les demi-tordre à la Tate, on pourra toujours supposer que le poids est zéro. Le théorème principal de Weil II relie le poids d'un faisceau constructible au sens de la définition ci-dessus aux valeurs propres de Frobenius agissant sur sa cohomologie et sa cohomologie à support compact.

THÉORÈME 2.10 (Deligne, [9]). — *Soit \mathcal{F} un faisceau constructible sur X . Si \mathcal{F} est ι -mixte de poids $\leq w$, alors chaque $H^i(X_{\bar{k}}, \mathcal{F})$ est ι -mixte de poids $\geq w + i$ et chaque $H_c^i(X_{\bar{k}}, \mathcal{F})$ est ι -mixte de poids $\leq w + i$. En particulier, si la flèche d'oubli des supports est un isomorphisme, $H^i(X_{\bar{k}}, \mathcal{F}) \cong H_c^i(X_{\bar{k}}, \mathcal{F})$ est ι -pur de poids $w + i$.*

On renvoie aux travaux de Laumon [35] et de Katz [21] pour des simplifications de la preuve originale, basées sur l’incarnation faisceautique de la transformation de Fourier. Voici un exemple frappant d’application de ces résultats qui reviendra dans la preuve du théorème d’équirépartition de Deligne :

Exemple 2.11 (Inégalités de Lang–Weil, [34]). — En prenant pour \mathcal{F} le faisceau constant $\overline{\mathbf{Q}}_\ell$, on trouve que le nombre de points E -rationnels de X est donné par

$$|X(E)| = \sum_{i=0}^{2d} (-1)^i \mathrm{Tr}(F_E | H_c^i(X_{\bar{k}}, \overline{\mathbf{Q}}_\ell)).$$

Comme $\overline{\mathbf{Q}}_\ell$ est pur de poids zéro, $H_c^i(X_{\bar{k}}, \overline{\mathbf{Q}}_\ell)$ est mixte de poids $\leq i$ d’après le théorème 2.10, ce qui signifie que les valeurs propres de F_E agissant sur cet espace ont toutes valeur absolue au plus $|E|^{i/2}$ quel que soit le plongement de $\overline{\mathbf{Q}}_\ell$ dans \mathbf{C} . Posons

$$b_c^i(X) = \dim_{\overline{\mathbf{Q}}_\ell} H_c^i(X_{\bar{k}}, \overline{\mathbf{Q}}_\ell), \quad A(X) = \sum_{i=0}^{2d-1} b_c^i(X).$$

On a vu que $H_c^{2d}(X_{\bar{k}}, \overline{\mathbf{Q}}_\ell)$ est le $\overline{\mathbf{Q}}_\ell$ -espace vectoriel de dimension un sur lequel F_E agit par multiplication par $|E|^d$, d’où les inégalités

$$(6) \quad \left| |X(E)| - |E|^d \right| \leq \sum_{i=0}^{2d-1} b_c^i(X) |E|^{i/2} \leq A(X) |E|^{(2d-1)/2}.$$

En particulier, la variété X a un point E -rationnel dès que $|E| > A(X)^2$.

2.4. Un peu de ramification

Dans ce qui suit, on rappelle une formule due à Grothendieck–Ogg–Shafarevich qui exprime la caractéristique d’Euler d’un faisceau constructible sur une courbe en termes de sa ramification à l’infini. Soit C une courbe projective, lisse et géométriquement connexe sur un corps parfait k de caractéristique $p > 0$. Pour chaque point fermé x de C et chaque point géométrique \bar{x} au-dessus de x , nous avons une suite exacte

$$1 \longrightarrow I_{\bar{x}} \longrightarrow D_{\bar{x}} \longrightarrow \mathrm{Gal}(\bar{k}/k) \longrightarrow 1.$$

Le groupe d’inertie $I_{\bar{x}}$ contient un unique p -sous-groupe de Sylow $P_{\bar{x}}$, sa partie *sauvage*, et le quotient $I_{\bar{x}}^{\mathrm{mod}} = I_{\bar{x}}/P_{\bar{x}}$ (l’inertie *modérée*) est canoniquement isomorphe à

$$\widehat{\mathbf{Z}}'(1) = \varprojlim_{(N,p)=1} \mu_N(\bar{k}) = \varprojlim_{E/k \text{ finie}} E^\times.$$

Il s’agit du premier cran d’une filtration décroissante $(I_{\bar{x}}^{(r)})_{r \in \mathbf{Q}_{\geq 0}}$ par des sous-groupes fermés distingués de $I_{\bar{x}}$ que l’on appelle la *filtration de ramification en numérotation supérieure* [45, Ch. IV] : on a $I_{\bar{x}}^{(0)} = I_{\bar{x}}$, la partie sauvage $P_{\bar{x}}$ est l’adhérence de $\bigcup_{r>0} I_{\bar{x}}^{(r)}$ dans $I_{\bar{x}}$, et $I_{\bar{x}}^{(r)} = \bigcap_{0 < s < r} I_{\bar{x}}^{(s)}$ pour tout $r \in \mathbf{Q}_{>0}$.

Soit $I_{\bar{x}} \rightarrow \mathrm{GL}(W)$ une représentation continue dans un espace vectoriel W de dimension finie sur $\overline{\mathbf{Q}}_\ell$. On dit que W est *modérée* si $P_{\bar{x}}$ agit trivialement et *totalelement sauvage* si $W^{P_{\bar{x}}} = 0$. La représentation W admet une décomposition unique

$$(7) \quad W = \bigoplus_{r \geq 0} W(r),$$

indexée par des nombres rationnels, en des sous-espaces vectoriels $W(r) \subseteq W$ stables sous l'action de $P_{\bar{x}}$ et vérifiant les propriétés suivantes :

$$W(0) = W^{P_{\bar{x}}}, \quad W(r)^{I_{\bar{x}}^{(r)}} = 0 \text{ si } r > 0, \quad W(r)^{I_{\bar{x}}^{(r')}} = W(r) \text{ si } r' > r.$$

Cette décomposition ne comporte qu'un nombre fini de valeurs de r pour lesquelles $W(r)$ n'est pas nul, que l'on appellera les *sauts*. De plus, $r \dim W(r)$ est un entier positif. On définit le *conducteur de Swan* de la représentation W comme l'entier positif

$$\mathrm{Sw}(W) = \sum_{r \geq 0} r \dim W(r).$$

Soient V un ouvert non vide de C et \mathcal{F} un faisceau lisse sur V , vu comme représentation ℓ -adique de $\pi_1(V, \bar{\eta})$. Par restriction, on en déduit une représentation du groupe d'inertie $I_{\bar{x}}$ pour tout point fermé $x \in C \setminus V$. On notera $\mathrm{Sw}_{\bar{x}}(\mathcal{F})$ son conducteur de Swan. Il s'agit d'un entier positif qui est nul si et seulement si la représentation de $I_{\bar{x}}$ est modérée, auquel cas on dira que \mathcal{F} a *ramification modérée* en x . Si $V = \mathbb{G}_{m,k}$, les systèmes locaux modérément ramifiés à l'infini sont les représentations du groupe fondamental modéré $\pi_1^{\mathrm{mod}}(\mathbb{G}_{m,k})$, qui s'insère dans une suite exacte

$$1 \longrightarrow \widehat{\mathbf{Z}}'(1) \longrightarrow \pi_1^{\mathrm{mod}}(\mathbb{G}_{m,k}) \longrightarrow \mathrm{Gal}(\bar{k}/k) \longrightarrow 1.$$

Exemple 2.12. — Soit k un corps fini. Le faisceau d'Artin–Schreier \mathcal{L}_ψ sur \mathbb{A}_k^1 a ramification totalelement sauvage à l'infini et son conducteur de Swan vaut 1. Le faisceau de Kummer \mathcal{L}_χ sur $\mathbb{G}_{m,k}$ a ramification modérée en 0 et ∞ . Par extension, on appellera *faisceau de Kummer* tout système local ℓ -adique de rang un sur $\mathbb{G}_{m,k}$ correspondant à un caractère de $\pi_1^{\mathrm{mod}}(\mathbb{G}_{m,k})$.

Soient maintenant $U \subseteq C$ un ouvert contenant V et \mathcal{F} un faisceau constructible sur U . Pour tout point fermé $u \in U \setminus V$, on définit l'entier

$$\mathrm{dr}_{\bar{u}}(\mathcal{F}) = \dim(\mathcal{F}_{\bar{\eta}}) - \dim(\mathcal{F}_{\bar{u}}).$$

Si \mathcal{F} n'a pas de sections globales ponctuelles non nulles, alors toutes les flèches de spécialisation $\mathcal{F}_{\bar{u}} \rightarrow \mathcal{F}_{\bar{\eta}}^{I_{\bar{u}}}$ sont injectives ; dans ce cas, $\mathrm{dr}_{\bar{u}}(\mathcal{F})$ est positif et le faisceau \mathcal{F} est lisse en \bar{u} si et seulement si $\mathrm{dr}_{\bar{u}}(\mathcal{F}) = 0$.

La formule de Grothendieck–Ogg–Shafarevich, exposée dans ce séminaire par Raynaud [40], est l'énoncé que la caractéristique d'Euler de \mathcal{F} s'exprime ainsi :

THÉORÈME 2.13 (Grothendieck–Ogg–Shafarevich). — Soient \mathcal{F} un faisceau ℓ -adique constructible sur U et $V \subseteq U$ un ouvert non vide sur lequel \mathcal{F} est lisse. Alors

$$\chi(U_{\bar{k}}, \mathcal{F}) = \text{rg}(\mathcal{F})\chi(U_{\bar{k}}) - \sum_{x \in (C \setminus V)(\bar{k})} \text{Sw}_{\bar{x}}(\mathcal{F}) - \sum_{u \in (U \setminus V)(\bar{k})} \text{dr}_{\bar{u}}(\mathcal{F}).$$

2.5. Catégorie dérivée et faisceaux pervers

Dans ce paragraphe, k désigne ou bien un corps fini, ou bien la clôture algébrique d'un corps fini. Soit $\pi: X \rightarrow \text{Spec}(k)$ une variété sur k . Grothendieck a défini la *catégorie dérivée* $D_c^b(X, \overline{\mathbf{Q}}_\ell)$ des complexes bornés de $\overline{\mathbf{Q}}_\ell$ -faisceaux sur X à cohomologie constructible et l'a munie d'un formalisme des six opérations :

- Pour tout morphisme $f: X \rightarrow Y$, on dispose des foncteurs *image directe* et *image directe à support compact*

$$Rf_*, Rf_!: D_c^b(X, \overline{\mathbf{Q}}_\ell) \longrightarrow D_c^b(Y, \overline{\mathbf{Q}}_\ell)$$

et des foncteurs *image inverse* et *image inverse exceptionnelle*

$$f^*, f^!: D_c^b(Y, \overline{\mathbf{Q}}_\ell) \longrightarrow D_c^b(X, \overline{\mathbf{Q}}_\ell).$$

En particulier, on obtient pour tout objet M dans $D_c^b(X, \overline{\mathbf{Q}}_\ell)$ des complexes de $\overline{\mathbf{Q}}_\ell$ -espaces vectoriels $R\pi_*M$ et $R\pi_!M$ que l'on notera $R\Gamma(X, M)$ et $R\Gamma_c(X, M)$. Si M est de la forme $\mathcal{F}[n]$, la cohomologie en degré i de ces complexes s'identifie à la cohomologie $H^{i+n}(X_{\bar{k}}, \mathcal{F})$ et à la cohomologie à support compact $H_c^{i+n}(X_{\bar{k}}, \mathcal{F})$.

- On dispose d'un bifoncteur *produit tensoriel*

$$- \otimes -: D_c^b(X, \overline{\mathbf{Q}}_\ell) \times D_c^b(X, \overline{\mathbf{Q}}_\ell) \longrightarrow D_c^b(X, \overline{\mathbf{Q}}_\ell)$$

et d'un bifoncteur *Hom interne*

$$R\mathcal{H}om(-, -): D_c^b(X, \overline{\mathbf{Q}}_\ell)^{\text{op}} \times D_c^b(X, \overline{\mathbf{Q}}_\ell) \longrightarrow D_c^b(X, \overline{\mathbf{Q}}_\ell).$$

Le *produit extérieur* des objets M dans $D_c^b(X, \overline{\mathbf{Q}}_\ell)$ et N dans $D_b(Y, \overline{\mathbf{Q}}_\ell)$ est l'objet

$$M \boxtimes N = \text{pr}_X^* M \otimes \text{pr}_Y^* N$$

dans $D_c^b(X \times Y, \overline{\mathbf{Q}}_\ell)$, où pr_X et pr_Y désignent les projections de $X \times Y$ sur X et Y .

- On définit le *complexe dualisant* comme $\omega_X = \pi^! \overline{\mathbf{Q}}_\ell$ et le foncteur de *dualité de Verdier* $\mathbb{D}: D_c^b(X, \overline{\mathbf{Q}}_\ell)^{\text{op}} \rightarrow D_c^b(X, \overline{\mathbf{Q}}_\ell)$ comme

$$\mathbb{D}(M) = R\mathcal{H}om(M, \pi^! \overline{\mathbf{Q}}_\ell).$$

La dualité échange Rf_* et $Rf_!$ (resp. f^* et $f^!$) pour tout morphisme $f: X \rightarrow Y$. Si X est lisse et purement de dimension d , le complexe dualisant est égal à $\omega_X = \overline{\mathbf{Q}}_\ell(d)[2d]$ et l'on retrouve la dualité de Poincaré $H^i(X, \overline{\mathbf{Q}}_\ell) \cong H_c^{2d-i}(X, \overline{\mathbf{Q}}_\ell)^*(-d)$ comme cas particulier. Plus généralement, $f^! = f^*(d)[2d]$ si f est lisse de dimension relative d .

Dans le cas où k est un corps fini, on définit la fonction trace d'un objet M de la catégorie dérivée comme la somme alternée $t_M = \sum (-1)^i t_{\mathcal{H}^i(M)}$ des fonctions trace de ses faisceaux de cohomologie. La formule des traces de Grothendieck est alors l'égalité

$$(8) \quad t_{Rf_!M}(y) = \sum_{f(x)=y} t_M(x).$$

De même, la notion de poids s'étend à la catégorie dérivée comme suit : un objet M dans $D_c^b(X, \overline{\mathbf{Q}}_\ell)$ est dit ι -mixte de poids $\leq w$ si tous ses faisceaux de cohomologie $\mathcal{H}^i(M)$ sont ι -mixtes de poids $\leq w + i$, au sens de la définition 2.9, et ι -mixte de poids $\geq w$ si son dual de Verdier $\mathbb{D}(M)$ est ι -mixte de poids $\leq -w$. On dit enfin que M est ι -pur de poids w s'il est en même temps ι -mixte de poids $\leq w$ et $\geq w$. Le théorème principal de Weil II peut alors se formuler ainsi :

THÉORÈME 2.14 (Deligne). — *Si $f: X \rightarrow Y$ est un morphisme de k -variétés, le foncteur $Rf_!$ envoie les objets ι -mixtes de poids $\leq w$ sur des objets ι -mixtes de poids $\leq w$. Par dualité de Verdier, le foncteur Rf_* envoie les objets ι -mixtes de poids $\geq w$ sur des objets ι -mixtes de poids $\geq w$.*

En s'inspirant des travaux de Goresky et MacPherson sur l'homologie d'intersection d'un espace topologique singulier, Beilinson, Bernstein, Deligne et Gabber ont introduit la notion de faisceau pervers dans [2].

DÉFINITION 2.15. — *Un objet M de $D_c^b(X, \overline{\mathbf{Q}}_\ell)$ est dit semipervers si tous ses faisceaux de cohomologie $\mathcal{H}^i(M)$ satisfont à la condition de support*

$$\dim \operatorname{supp}(\mathcal{H}^i(M)) \leq -i.$$

On appelle M un faisceau pervers si tant M que $\mathbb{D}(M)$ sont semipervers.

Par exemple, si X est lisse de dimension d et \mathcal{L} est un système local ℓ -adique sur X , l'objet $\mathcal{L}[d]$ est un faisceau pervers car la condition de support est vérifiée trivialement et son dual $\mathbb{D}(\mathcal{L}[d]) = \mathcal{L}^\vee(d)[d]$ est encore de la même forme.

La sous-catégorie pleine $\mathbf{Perv}(X, \overline{\mathbf{Q}}_\ell)$ de $D_c^b(X, \overline{\mathbf{Q}}_\ell)$ formée des faisceaux pervers est abélienne et tout objet est extension successive d'un nombre fini d'objets simples [2]. Qui plus est, la catégorie dérivée de complexes bornés dans $\mathbf{Perv}(X, \overline{\mathbf{Q}}_\ell)$ est équivalente à $D_c^b(X, \overline{\mathbf{Q}}_\ell)$, d'où des foncteurs de *cohomologie perverse*

$${}^p\mathcal{H}^0: D_c^b(X, \overline{\mathbf{Q}}_\ell) \longrightarrow \mathbf{Perv}(X, \overline{\mathbf{Q}}_\ell)$$

et ${}^p\mathcal{H}^i = {}^p\mathcal{H}^0[i]$ pour tout entier i . Si $f: X \rightarrow Y$ est un morphisme affine, alors Rf_* préserve la semiperversité (théorème d'annulation d'Artin) et si $f: X \rightarrow Y$ est un morphisme lisse de dimension relative d , le foncteur $f^*[d]$ préserve la perversité.

La plupart du temps nous travaillerons avec des faisceaux pervers sur une courbe, auquel cas les objets admettent une description plus élémentaire.

Exemple 2.16 (Faisceaux pervers sur les courbes). — Soit X une courbe lisse et géométriquement connexe sur un corps fini k . Un faisceau pervers sur X est un complexe de faisceaux constructibles M dans $D_c^b(X, \overline{\mathbf{Q}}_\ell)$ satisfaisant aux conditions suivantes : $\mathcal{H}^i(M) = 0$ pour tout $i \notin \{-1, 0\}$, le faisceau constructible $\mathcal{H}^{-1}(M)$ n'a pas de sections globales ponctuelles non nulles, et le faisceau constructible $\mathcal{H}^0(M)$ est supporté dans des points. En posant $M_{\text{pct}} = \mathcal{H}^0(M)$ et $M_{\text{npct}} = \mathcal{H}^{-1}(M)[1]$, on trouve une suite exacte

$$(9) \quad 0 \longrightarrow M_{\text{npct}} \longrightarrow M \longrightarrow M_{\text{pct}} \longrightarrow 0.$$

De plus, les objets simples de la catégorie $\mathbf{Perv}(X, \overline{\mathbf{Q}}_\ell)$ sont d'un de ces deux types :

- *ponctuels* : de la forme $\alpha^{\text{deg}} \otimes \delta_x$ pour un point fermé x de X et une unité ℓ -adique α ;
- *non ponctuels* : de la forme $(j_* \mathcal{L})[1]$, où $j: U \hookrightarrow X$ est l'inclusion d'un ouvert non vide et \mathcal{L} est un système local ℓ -adique simple sur U . On les appelle *extensions intermédiaires*.

3. LE THÉORÈME D'ÉQUIRÉPARTITION DE DELIGNE

Dans ce numéro, on expose le théorème d'équirépartition de Deligne [9, §3.5] suivant les variantes qu'en ont données Katz [18, Ch. 3] et Katz–Sarnak [27, §9.2]. Sous des hypothèses assez faibles, il affirme que le groupe de monodromie d'un système local ℓ -adique gouverne la répartition de ses traces de Frobenius. Ces groupes sont en général difficiles à calculer, mais Katz a réussi à les déterminer complètement pour les faisceaux associés aux sommes de Kloosterman ; combiné avec le résultat de Deligne, ceci permet d'obtenir le théorème 1.3 dans l'introduction, ainsi que de l'étendre à un énoncé d'équirépartition pour les sommes $\text{Kl}_n(a, q)$ en plusieurs variables. Dans le dernier paragraphe, on analyse la répartition des traces de la transformée de Fourier d'un faisceau pervers sur la droite affine à l'aide du théorème de Deligne, puis on explique pourquoi cette approche est vouée à l'échec pour le groupe multiplicatif.

3.1. Préliminaires sur les représentations

Dans le théorème d'équirépartition de Deligne, les groupes de monodromie sont des groupes algébriques réductifs G sur $\overline{\mathbf{Q}}_\ell$ et l'on définit des classes de conjugaison dans des sous-groupes compacts maximaux K de leurs points complexes. Pour appliquer le critère d'équirépartition de Weyl, on aura besoin de relier les représentations continues de K à des systèmes locaux ℓ -adiques, vus comme des $\overline{\mathbf{Q}}_\ell$ -représentations algébriques de G .

THÉORÈME 3.1. — *Soit G un groupe réductif (pas nécessairement connexe) sur $\overline{\mathbf{Q}}_\ell$. Pour chaque choix d'un plongement $\iota: \overline{\mathbf{Q}}_\ell \hookrightarrow \mathbf{C}$ et d'un sous-groupe compact maximal K de $G(\mathbf{C})$, les foncteurs extension des scalaires, évaluation dans les points complexes et restriction à K induisent des bijections entre les classes d'isomorphisme de*

- (a) $\overline{\mathbf{Q}}_\ell$ -représentations du $\overline{\mathbf{Q}}_\ell$ -groupe algébrique G ,
- (b) \mathbf{C} -représentations du \mathbf{C} -groupe algébrique $G_{\mathbf{C}}$,
- (c) représentations holomorphes du groupe de Lie complexe $G(\mathbf{C})$,
- (d) représentations continues du groupe compact K ,

toutes les représentations étant supposées de dimension finie.

Démonstration. — Les catégories (b), (c) et (d) sont en fait équivalentes. Pour démontrer l'équivalence entre (b) et (c), on se ramène facilement au cas où G est connexe, qui est traité dans [6, Prop. D.2.1]. L'équivalence entre (c) et (d), sans des hypothèses de connexité, est le contenu de la proposition D.3.2 et de l'exemple D.3.3 dans *loc. cit.* Quant à (a), on a tautologiquement une équivalence de catégories si le plongement ι est un isomorphisme de corps. En général, étant donnée une représentation complexe $\rho' : G_{\mathbf{C}} \rightarrow \mathrm{GL}(V')$, il existe un espace vectoriel V sur $\overline{\mathbf{Q}}_\ell$ et une représentation $\rho : G \rightarrow \mathrm{GL}(V)$, unique à isomorphisme près, telle que $\rho' \simeq \rho_{\mathbf{C}}$. \square

3.2. Le théorème d'équirépartition de Deligne

Soient k un corps fini à q éléments, \bar{k} une clôture algébrique de k , X une variété lisse et géométriquement connexe sur k et $X_{\bar{k}}$ la variété sur \bar{k} qui s'en déduit par extension des scalaires. Fixons un nombre premier ℓ distinct de la caractéristique de k , une clôture algébrique $\overline{\mathbf{Q}}_\ell$ de \mathbf{Q}_ℓ et un plongement $\iota : \overline{\mathbf{Q}}_\ell \hookrightarrow \mathbf{C}$. Soit \mathcal{L} un faisceau ℓ -adique lisse de rang r sur X , correspondant à une représentation continue

$$\rho : \pi_1(X, \bar{\eta}) \rightarrow \mathrm{GL}(r, \overline{\mathbf{Q}}_\ell).$$

DÉFINITION 3.2. — *Les groupes de monodromie arithmétique $G_{\mathrm{arith}, \mathcal{L}}$ et géométrique $G_{\mathrm{geom}, \mathcal{L}}$ de \mathcal{L} sont les groupes algébriques sur $\overline{\mathbf{Q}}_\ell$ obtenus comme l'adhérence de Zariski de $\rho(\pi_1(X, \bar{\eta}))$ et de $\rho(\pi_1(X_{\bar{k}}, \bar{\eta}))$ dans $\mathrm{GL}(r, \overline{\mathbf{Q}}_\ell)$.*

En particulier, $G_{\mathrm{geom}, \mathcal{L}}$ est un sous-groupe de $G_{\mathrm{arith}, \mathcal{L}}$. Comme les classes de conjugaison de Frobenius sont denses dans le groupe fondamental par une forme du théorème de Cebotarev, $G_{\mathrm{arith}, \mathcal{L}}$ est aussi le plus petit sous-groupe algébrique contenant leurs images par la représentation. Dans Weil II, Deligne démontre que, si \mathcal{L} est ι -pur d'un certain poids, la représentation de $\pi_1(X_{\bar{k}}, \bar{\eta})$ associée est complètement réductible [9, Thm. 3.4.1 (iii)] et le groupe de monodromie géométrique $G_{\mathrm{geom}, \mathcal{L}}$ est donc réductif. Qui plus est, la composante neutre du groupe de monodromie géométrique $G_{\mathrm{geom}, \mathcal{L}}$ est semisimple d'après [9, Cor. 1.3.9].

Supposons que \mathcal{L} est ι -pur de poids zéro et $G_{\mathrm{geom}, \mathcal{L}} = G_{\mathrm{arith}, \mathcal{L}}$, de sorte que la représentation ρ se factorise par $G_{\mathrm{geom}, \mathcal{L}}(\overline{\mathbf{Q}}_\ell)$. Choisissons un sous-groupe compact maximal K de $G_{\mathrm{geom}, \mathcal{L}}(\mathbf{C})$ et notons $K^\#$ l'ensemble de ses classes de conjugaison. Le but est d'associer à chaque point de X à valeurs dans une extension finie E de k un élément de $K^\#$ dont la trace soit égale à $\mathrm{Tr}(\mathrm{Frob}_{E,x} | \mathcal{L})$. Soient x un tel point et $\mathrm{Frob}_{E,x}$

la classe de conjugaison qu'il définit dans $\pi_1(X, \bar{\eta})$. Son image par la représentation ρ est une classe de conjugaison

$$\rho(\text{Frob}_{E,x}) \in G_{\text{geom}, \mathcal{L}}(\overline{\mathbf{Q}}_\ell)^\# \subset G_{\text{geom}, \mathcal{L}}(\mathbf{C})^\#.$$

Soit $\rho(\text{Frob}_{E,x})^{\text{ss}}$ sa semisimplification au sens de la décomposition de Jordan. Puisque \mathcal{L} est ι -pur de poids zéro, chaque élément g dans $\rho(\text{Frob}_{E,x})^{\text{ss}}$ est semi-simple avec des valeurs propres *unitaires*, et l'adhérence de $\langle g \rangle$ est donc un sous-groupe compact de $G_{\text{geom}, \mathcal{L}}(\mathbf{C})$. Il s'ensuit que g appartient à un sous-groupe compact maximal et, comme ils sont tous conjugués, qu'il existe des éléments h dans K et s dans $G_{\text{geom}, \mathcal{L}}(\mathbf{C})$ tels que $g = s^{-1}hs$. On affirme que h est bien défini à conjugaison près par un élément de K . En effet, par le théorème de Peter–Weyl, les traces des représentations irréductibles de dimension finie Λ_K de K séparent les classes de conjugaison. Or Λ_K correspond d'après le théorème 3.1 à une unique représentation Λ du $\overline{\mathbf{Q}}_\ell$ -groupe algébrique $G_{\text{geom}, \mathcal{L}}$ et, quel que soit le choix de h , on a

$$\text{Tr}(\Lambda_K(h)) = \text{Tr}(\Lambda(\rho(\text{Frob}_{E,x})^{\text{ss}})) = \text{Tr}(\Lambda(\rho(\text{Frob}_{E,x}))).$$

On notera $\theta_{E,x}$ la classe de conjugaison dans K ainsi obtenue.

Finalement, soit $\pi: K \rightarrow K^\#$ la projection canonique. Muni de la topologie quotient, l'espace $K^\#$ est compact et l'application $f \mapsto f_{\text{cent}} = f \circ \pi$ permet d'identifier $\mathcal{C}(K^\#)$ aux fonctions *centrales* continues sur K . L'image directe par π de la mesure de Haar normalisée μ_K est une mesure de probabilité $\mu_{K^\#}$ sur $K^\#$ telle que

$$\int_{K^\#} f \mu_{K^\#} = \int_K f_{\text{cent}} \mu_K.$$

THÉORÈME 3.3 (Deligne). — *Soit \mathcal{L} un faisceau ℓ -adique lisse sur X . Supposons que \mathcal{L} est ι -pur de poids zéro et que les groupes $G_{\text{arith}, \mathcal{L}}$ et $G_{\text{geom}, \mathcal{L}}$ coïncident. Lorsque le degré des extensions E/k tend vers l'infini, les classes de conjugaison $\{\theta_{E,x}\}_{x \in X(E)}$ s'équirépartissent dans $K^\#$ selon la mesure $\mu_{K^\#}$.*

DÉMONSTRATION — Soit $f: K \rightarrow \mathbf{C}$ une fonction centrale continue. Il faut démontrer que, quand E parcourt les extensions de k de degré assez grand pour que l'ensemble $X(E)$ soit non vide, on a l'égalité

$$(10) \quad \int_K f \mu_K = \lim_{|E| \rightarrow \infty} \frac{1}{|X(E)|} \sum_{x \in X(E)} f(\theta_{E,x}).$$

D'après le théorème de Peter–Weyl, f est limite uniforme de combinaisons linéaires finies de traces de représentations irréductibles de dimension finie Λ_K de K ; il suffit de traiter le cas d'une telle représentation. Comme μ_K a masse totale un, la fonction constante $f = 1$ vérifie (10) même sans passer à la limite. On peut donc supposer que Λ_K n'est pas triviale, auquel cas l'intégrale du membre gauche s'annule :

$$\int_K \text{Tr}_{\Lambda_K} \mu_K = 0.$$

Démontrons que le membre droit de (10) est également nul (critère d'équirépartition de Weyl). Invoquant à nouveau le théorème 3.1, Λ_K correspond à une unique représentation irréductible non triviale Λ du groupe algébrique $G_{\text{geom}, \mathcal{L}}$ sur $\overline{\mathbf{Q}}_\ell$. Compte tenu de l'hypothèse $G_{\text{arith}, \mathcal{L}} = G_{\text{geom}, \mathcal{L}}$, on peut composer Λ avec

$$\pi_1(X, \bar{\eta}) \xrightarrow{\rho} G_{\text{geom}, \mathcal{L}}(\overline{\mathbf{Q}}_\ell)$$

et penser à $\Lambda \circ \rho$ comme à un système local ℓ -adique sur X . Notons-le $\Lambda(\mathcal{L})$ et regardons ses traces de Frobenius dans \mathbf{C} via ι . On a alors $\text{Tr}_{\Lambda_K}(\theta_{E,x}) = \text{Tr}(\text{Frob}_{E,x} | \Lambda(\mathcal{L}))$, et la formule des traces de Grothendieck donne l'égalité

$$\sum_{x \in X(E)} \text{Tr}_{\Lambda_K}(\theta_{E,x}) = \sum_{i=0}^{2d} (-1)^i \text{Tr}(F_E | H_c^i(X_{\bar{k}}, \Lambda(\mathcal{L}))).$$

Comme le groupe $G_{\text{geom}, \mathcal{L}}$ est réductif, ρ est une représentation fidèle et Λ est une représentation irréductible, il existe des entiers $a, b \geq 0$ tels que $\Lambda(\mathcal{L})$ soit sous-objet du système local $\mathcal{L}^{\otimes a} \otimes (\mathcal{L}^\vee)^{\otimes b}$. On en déduit que $\Lambda(\mathcal{L})$ est encore ι -pur de poids zéro. La cohomologie à support compact $H_c^i(X_{\bar{k}}, \Lambda(\mathcal{L}))$ est donc ι -mixte de poids $\leq i$ d'après le théorème principal de Weil II. Par ailleurs, on a l'annulation

$$H_c^{2d}(X_{\bar{k}}, \Lambda(\mathcal{L})) = (\Lambda(\mathcal{L})_{\bar{\eta}})_{\pi_1(X_{\bar{k}}, \bar{\eta})} = 0$$

car $\Lambda(\mathcal{L})_{\bar{\eta}}$ est une représentation irréductible non triviale de $\pi_1(X_{\bar{k}}, \bar{\eta})$. Combinant ces informations, il vient

$$\begin{aligned} \left| \sum_{x \in X(E)} \text{Tr}_{\Lambda_K}(\theta_{E,x}) \right| &\leq \sum_{i=0}^{2d-1} \dim_{\overline{\mathbf{Q}}_\ell} H_c^i(X_{\bar{k}}, \Lambda(\mathcal{L})) \cdot |E|^{i/2} \\ (11) \qquad \qquad \qquad &\leq \left(\sum_{i=0}^{2d-1} \dim_{\overline{\mathbf{Q}}_\ell} H_c^i(X_{\bar{k}}, \Lambda(\mathcal{L})) \right) |E|^{(2d-1)/2}. \end{aligned}$$

Par les inégalités de Lang–Weil, on a $2|X(E)| \geq |E|^d$ dès que le degré de l'extension E est assez grand pour que $|E|^{1/2} > 2 \sum_{i \leq 2d-1} b_c^i(X)$ et, en particulier, l'ensemble $X(E)$ n'est pas vide. Joint à ce qui précède, ceci fournit la majoration

$$\left| \frac{1}{|X(E)|} \sum_{x \in X(E)} \text{Tr}_{\Lambda_K}(\theta_{E,x}) \right| \leq \frac{2}{\sqrt{|E|}} \sum_{i=0}^{2d-1} \dim_{\overline{\mathbf{Q}}_\ell} H_c^i(X_{\bar{k}}, \Lambda(\mathcal{L})).$$

La limite du membre gauche est donc zéro lorsque le degré de E tend vers l'infini. \square

Remarque 3.4. — Dans [27, Thm. 9.2.6 (3)], Katz et Sarnak démontrent qu'il existe une constante $C(X_{\bar{k}}, \mathcal{L})$, ne dépendant que de la variété $X_{\bar{k}}$ et du système local \mathcal{L} , telle que

$$(12) \qquad \sum_{i=0}^{2d} \dim_{\overline{\mathbf{Q}}_\ell} H_c^i(X_{\bar{k}}, \Lambda(\mathcal{L})) \leq \dim(\Lambda) C(X_{\bar{k}}, \mathcal{L})$$

pour toute $\overline{\mathbf{Q}}_\ell$ -représentation de dimension finie Λ de $G_{\text{geom}, \mathcal{L}}$. Si X est une courbe, on peut d'après [18, (3.6.2.1)] prendre

$$C(X_{\bar{k}}, \mathcal{L}) = 2g - 2 + N + \sum_{i=1}^N r_i$$

où g est le genre de la compactification lisse de X , N le nombre de \bar{k} -points x_1, \dots, x_N à l'infini et r_i le plus grand saut dans la décomposition (7) de la monodromie locale de \mathcal{L} en x_i .

Remarque 3.5. — Le théorème 3.3 est un énoncé d'équirépartition verticale. Supposons maintenant que l'on se donne un schéma lisse X sur un ouvert S de $\text{Spec}(\mathbf{Z}[1/\ell])$ et un système local ℓ -adique ι -pur de poids zéro \mathcal{L} sur X tel que, pour chaque premier p dans S , les groupes de monodromie géométrique et arithmétique du système local \mathcal{L}_p sur $X_{\mathbf{F}_p}$ obtenu par réduction modulo p coïncident et qu'ils sont tous égaux à un même groupe réductif. Au vu de la borne (12), la question si les classes de conjugaison $\{\theta_{\mathbf{F}_p, x}\}_{x \in X(\mathbf{F}_p)}$ s'équirépartissent horizontalement est intimement liée au difficile problème de trouver des estimées explicites de la constante $C(X_{\overline{\mathbf{F}}_p}, \mathcal{L}_p)$, par exemple de la majorer indépendamment de p , cf. [19, App.] et [27, §9.6].

3.3. Retour aux sommes de Kloosterman

On donne maintenant l'application du théorème d'équirépartition de Deligne aux sommes de Kloosterman. En plus des références originales de Deligne [8] et Katz [18], le lecteur pourra consulter avec profit le survol [36] de Laumon. Soient $\psi: \mathbf{F}_q \rightarrow \overline{\mathbf{Q}}_\ell^\times$ un caractère additif non trivial et \mathcal{L}_ψ le faisceau d'Artin-Schreier correspondant. Pour un entier $n \geq 2$, notons $\sigma: \mathbb{G}_m^n \rightarrow \mathbb{A}^1$ et $\pi: \mathbb{G}_m^n \rightarrow \mathbb{G}_m$ les morphismes somme et produit des coordonnées, respectivement, et posons

$$\mathcal{K}l_n = R^{n-1} \pi_! \sigma^* \mathcal{L}_\psi.$$

D'après Deligne, $\mathcal{K}l_n$ est un faisceau ℓ -adique lisse de rang n sur $\mathbb{G}_{m, \mathbf{F}_q}$ ayant pour trace de Frobenius en un point $a \in \mathbf{F}_q^\times$ la somme de Kloosterman au signe près :

$$\text{Tr}(\text{Frob}_{\mathbf{F}_q, a} | \mathcal{K}l_n) = (-1)^{n-1} \text{Kl}_n(a, q).$$

De plus, la flèche d'oubli des supports $R^{n-1} \pi_! \sigma^* \mathcal{L}_\psi \rightarrow R^{n-1} \pi_* \sigma^* \mathcal{L}_\psi$ est un isomorphisme [8, Thm. 7.8]. Comme $\sigma^* \mathcal{L}_\psi$ est ι -pur de poids zéro, le théorème principal de Weil II entraîne que $\mathcal{K}l_n$ est ι -pur de poids $n-1$, d'où la majoration qui nous a permis de démontrer l'équirépartition des angles des sommes de Gauss dans l'introduction :

$$|\text{Kl}_n(a, q)| \leq nq^{\frac{n-1}{2}}.$$

Soit $\mathcal{L}_n = \mathcal{K}l_n(\frac{n-1}{2})$ le système local ℓ -adique ι -pur de poids zéro obtenu en demitordant $\mathcal{K}l_n$ à la Tate. On sait que le déterminant $\det \mathcal{L}_n = \wedge^n \mathcal{L}_n$ est le système local trivial de rang un sur $\mathbb{G}_{m, \mathbf{F}_q}$ et que, pour n pair ou pour $p = 2$ et n impair, on dispose d'un accouplement parfait $\mathcal{L}_n \otimes \mathcal{L}_n \rightarrow \overline{\mathbf{Q}}_\ell$ qui est alterné dans le premier cas et symétrique

dans le second. Il s'ensuit que le groupe de monodromie arithmétique $G_{\text{arith}, \mathcal{L}_n}$ est inclus dans $\text{SL}(n)$. Si n est pair, c'est un sous-groupe du groupe symplectique $\text{Sp}(n)$ et, si $p = 2$ et n est impair, du groupe spécial orthogonal $\text{SO}(n)$. Dans [18, Thm. 11.1], Katz démontre que la monodromie est aussi grande que possible⁽⁶⁾ en calculant

$$G_{\text{geom}, \mathcal{L}_n} = \begin{cases} \text{Sp}(n) & n \text{ pair,} \\ \text{SL}(n) & n \text{ impair et } p \neq 2, \\ \text{SO}(n) & n \text{ impair } \neq 7 \text{ et } p = 2, \\ G_2 & n = 7 \text{ et } p = 2, \end{cases}$$

où $G_2 \subset \text{SO}(7)$ est l'un des groupes algébriques exceptionnels, défini comme le stabilisateur d'une certaine forme trilinéaire dans la représentation standard de dimension 7 de $\text{SO}(7)$. Avec un petit argument additionnel pour traiter le dernier cas [18, §11.3], on en déduit l'égalité des groupes $G_{\text{geom}, \mathcal{L}_n} = G_{\text{arith}, \mathcal{L}_n}$.

Supposons $p \neq 2$ et notons G le groupe de monodromie de \mathcal{L}_n , qui est donc égal à $\text{Sp}(n)$ si n est pair et à $\text{SL}(n)$ si n est impair. L'intersection $K = G(\mathbf{C}) \cap U(n)$ avec le groupe unitaire est un sous-groupe compact maximal de $G(\mathbf{C})$. Pour le système local \mathcal{L}_n , le nombre $C(\mathbb{G}_{m, \bar{k}}, \mathcal{L}_n)$ de la remarque 3.4 vaut $1/n$ car \mathcal{L}_n a ramification modérée en 0 et ramification sauvage en ∞ avec $\text{Sw}_\infty(\mathcal{L}_n) = 1$ et tous les sauts égaux à $1/n$. Par conséquent, (11) et (12) donnent la majoration

$$\left| \frac{1}{q-1} \sum_{a \in \mathbf{F}_q^\times} \text{Tr}_{\Lambda_K}(\theta_{\mathbf{F}_q, a}) \right| \leq \frac{\dim(\Lambda_K)}{n} \frac{\sqrt{q}}{q-1}$$

pour toute représentation continue irréductible non triviale Λ_K de K . Le résultat suivant, qui généralise le théorème 1.3 dans l'introduction, en découle :

THÉORÈME 3.6 (Katz). — *Lorsque q tend vers l'infini parmi n'importe quelle suite de puissances de nombres premiers impairs, les sommes de Kloosterman normalisées*

$$\{\text{Kl}_n(a, q)/q^{\frac{n-1}{2}}\}_{a \in \mathbf{F}_q^\times}$$

se répartissent comme les traces de matrices aléatoires dans K .

Il résulte de ce théorème que, pour chaque entier $r \geq 1$, la limite des moments

$$\lim_{q \rightarrow \infty} \frac{1}{q^{\frac{r(n-1)}{2}}(q-1)} \sum_{a \in \mathbf{F}_q^\times} \text{Kl}_n(a, q)^r$$

est égale à la multiplicité de la représentation triviale dans la puissance tensorielle r -ième de la représentation standard de G correspondant à \mathcal{L}_n . Par exemple, cette multiplicité

6. D'après un théorème récent de Perret-Gentil [38], améliorant des résultats de Gabber [18, Ch. 12], c'est encore le cas pour les groupes de monodromie *entière*, qui sont des sous-groupes de $\text{Sp}(n)$ ou $\text{SL}(n)$ sur la complétion de l'anneau des entiers d'un corps cyclotomique en une place au-dessus de ℓ , pourvu que ℓ soit plus grand qu'une constante effective dépendant de n .

vaut 2 si $n = 2$ et $r = 4$, ce qui explique le terme dominant dans le calcul (3) du quatrième moment des sommes de Kloosterman en une variable.

3.4. Le cas du groupe additif

Dans ce paragraphe, on explique comment le théorème 3.3 permet d'étudier la répartition des transformées de Fourier, relatives à des caractères variables, de la fonction trace d'un faisceau ℓ -adique sur la droite affine ; c'est le pendant du théorème d'équirépartition de Katz pour le groupe additif.

Soit $\mathbb{A}_k^1 = \text{Spec } k[x]$ et soit M un objet de la catégorie dérivée $D_c^b(\mathbb{A}_k^1, \overline{\mathbf{Q}}_\ell)$. Pour chaque extension finie E de k et chaque caractère additif $\rho : E \rightarrow \overline{\mathbf{Q}}_\ell^\times$, on pose

$$S(M, E, \rho) = \sum_{x \in E} \rho(x) \text{Tr}(\text{Frob}_{E,x} | M).$$

Comment ces sommes se répartissent-elles lorsque le degré de E tend vers l'infini ?

Moyennant le choix d'un caractère non trivial $\psi : k \rightarrow \overline{\mathbf{Q}}_\ell^\times$, tous les caractères additifs de E sont de la forme $x \mapsto \psi(\text{Tr}_{E/k}(xy))$ pour un seul $y \in E$, de sorte que l'on peut récrire les sommes ci-dessus comme

$$S(M, E, y) = \sum_{x \in E} \psi(\text{Tr}_{E/k}(xy)) \text{Tr}(\text{Frob}_{E,x} | M)$$

et les regarder comme étant paramétrées par la droite affine duale $\mathbb{A}_k^1 = \text{Spec } k[y]$.

L'avantage de ce point de vue est que $y \mapsto -S(M, E, y)$ devient alors la fonction trace de la *transformation de Fourier*

$$\begin{aligned} \text{FT}_\psi : D_c^b(\mathbb{A}_k^1, \overline{\mathbf{Q}}_\ell) &\longrightarrow D_c^b(\mathbb{A}_k^1, \overline{\mathbf{Q}}_\ell) \\ M &\longmapsto R\text{pr}_{2,!}(\text{pr}_1^* M \otimes \mathcal{L}_{\psi(xy)}[1]), \end{aligned}$$

où pr_1 et pr_2 désignent les projections de $\mathbb{A}_k^2 = \text{Spec } k[x, y]$ sur les deux facteurs. Introduite par Deligne dans les années 70, cette construction a été systématiquement étudiée par Brylinski, Katz et Laumon [4], [16], [26], [35], [37]. À l'instar de la transformation de Fourier classique, le foncteur FT_ψ est essentiellement involutif

$$(13) \quad \text{FT}_{\psi^{-1}} \circ \text{FT}_\psi = (-1)$$

et échange le produit de convolution additive $M \star N = R\text{s}_!(M \boxtimes N)$, où $s : \mathbb{A}_k^2 \rightarrow \mathbb{A}_k^1$ désigne l'application somme, et le produit tensoriel :

$$(14) \quad \text{FT}_\psi(M \star N) = \text{FT}_\psi(M) \otimes \text{FT}_\psi(N)[-1].$$

On a défini la transformation de Fourier à l'aide de l'image directe à support compact car c'est celle-ci qui s'interprète en termes de sommes exponentielles par le biais de la formule des traces, mais on aurait pu également utiliser l'image directe usuelle. Le

« miracle de la transformation de Fourier » [26, Thm. 2.1.3] est qu'il n'y en a qu'une seule, c'est-à-dire que la flèche d'oubli des supports

$$R\mathrm{pr}_{2,1}(\mathrm{pr}_1^*M \otimes \mathcal{L}_{\psi(xy)}[1]) \longrightarrow R\mathrm{pr}_{2,*}(\mathrm{pr}_1^*M \otimes \mathcal{L}_{\psi(xy)}[1])$$

est un isomorphisme. Voici quelques propriétés qui en résultent aussitôt :

- (a) Le foncteur FT_ψ commute à la dualité : $\mathbb{D} \circ \mathrm{FT}_\psi = \mathrm{FT}_{\psi^{-1}} \circ \mathbb{D}(1)$.
- (b) Le foncteur FT_ψ induit une équivalence de catégories sur le faisceaux pervers :

$$\mathrm{FT}_\psi : \mathbf{Perv}(\mathbb{A}_k^1, \overline{\mathbb{Q}}_\ell) \xrightarrow{\sim} \mathbf{Perv}(\mathbb{A}_k^1, \overline{\mathbb{Q}}_\ell).$$

- (c) Le foncteur FT_ψ augmente de 1 le poids des objets ι -purs.

DÉMONSTRATION — La propriété (a) découle du fait que la dualité échange $R\mathrm{pr}_{2,1}$ et $R\mathrm{pr}_{2,*}$, ainsi que pr_1^* et $\mathrm{pr}_1^! = \mathrm{pr}_1^*(1)[2]$. Grâce à l'involutivité (13), pour établir (b) il suffit de démontrer que la transformation de Fourier préserve les faisceaux pervers. Si M est pervers, alors $\mathrm{pr}_1^*M[1] \otimes \mathcal{L}_{\psi(xy)}$ est un faisceau pervers sur \mathbb{A}_k^2 , et $\mathrm{FT}_\psi(M)$, vu comme image directe usuelle, est semipervers car le morphisme pr_2 est affine ; puisque son dual est égal à $\mathrm{FT}_{\psi^{-1}}(\mathbb{D}(M)(1))$, il est aussi semipervers. Enfin, si M est ι -pur de poids w , alors $\mathrm{pr}_1^*M \otimes \mathcal{L}_{\psi(xy)}[1]$ est ι -pur de poids $w + 1$ et, comme les images directe usuelle et à support compact par la projection pr_2 son isomorphes, (c) résulte du théorème principal de Weil II. \square

La propriété (b) implique en particulier que la transformation de Fourier envoie des objets simples vers des objets simples. De plus, si M n'est pas géométriquement isomorphe à un faisceau d'Artin–Schreier décalé $\mathcal{L}_{\psi(ax)}[1]$, sa transformée de Fourier est de la forme $(j_*\mathcal{L})[1]$ pour un système local ℓ -adique sur un ouvert $j : U \hookrightarrow \mathbb{A}_k^1$ et

$$S(M, E, y) = \mathrm{Tr}(\mathrm{Frob}_{E,y} | \mathcal{L})$$

pour tout $y \in U(E)$. Compte tenu de tout ce qui précède, le théorème d'équirépartition de Deligne se traduit en l'énoncé suivant :

THÉORÈME 3.7. — *Soit M un faisceau pervers géométriquement simple et ι -pur de poids zéro sur \mathbb{A}_k^1 qui n'est pas de la forme $\mathcal{L}_{\psi(ax)}[1]$ et soit $(j_*\mathcal{L})[1]$ sa transformée de Fourier, où \mathcal{L} est un système local ℓ -adique sur un ouvert U de la droite affine duale. Supposons que les groupes de monodromie arithmétique et géométrique de \mathcal{L} coïncident et choisissons un sous-groupe compact maximal K de ce groupe. Alors, les sommes $\{S(M, E, y)\}_{y \in U(E)}$ se répartissent comme les traces de matrices aléatoires dans K lorsque le degré des extensions E/k tend vers l'infini.*

Si l'on essaye d'adapter ces techniques à l'étude de la répartition des transformées de Fourier des fonctions trace d'un faisceau pervers sur le groupe multiplicatif $\mathbb{G}_{m,k}$, on est tout de suite confronté à l'obstacle qu'il n'y a pas de variété algébrique sur k dont les E -points paramètrent les caractères multiplicatifs $\chi : E^\times \rightarrow \overline{\mathbb{Q}}_\ell$, ni *a fortiori*

de système local ℓ -adique incarnant la transformation de Fourier relative à ces caractères⁽⁷⁾. Par ailleurs, on a vu avec les sommes de Gauss que leur répartition peut être gouvernée par des groupes comme $GL(1)$ qui, contrairement aux groupes de monodromie géométrique d'un système local, ne sont pas semisimples. Katz a eu la belle idée de remplacer les points sur une variété algébrique par des foncteurs fibre sur une catégorie tannakienne comme espace de paramètres. Se rappelant que les systèmes locaux forment une catégorie tannakienne dans laquelle le groupe associé à un objet n'est rien d'autre que son groupe de monodromie, l'égalité (14) suggère de considérer à la place la catégorie des faisceaux pervers sur $\mathbb{G}_{m,k}$ munie du produit de convolution multiplicative.

4. LE THÉORÈME D'ÉQUIRÉPARTITION DE KATZ

Ce numéro est consacré aux résultats de la monographie [22]. On introduit d'abord une catégorie tannakienne de faisceaux pervers sur le groupe multiplicatif \mathbb{G}_m suivant Gabber et Loeser [11], ce qui permettra d'associer à ces objets des groupes algébriques sur $\overline{\mathbf{Q}}_\ell$ jouant le rôle des groupes de monodromie. Sous les bonnes hypothèses, il s'agit de groupes réductifs et l'on peut définir des classes de conjugaison $\theta_{E,\chi}$ dans un sous-groupe compact maximal K de leurs points complexes. Le théorème de Katz affirme que les $\theta_{E,\chi}$ s'équirépartissent selon la mesure induite par la mesure de Haar normalisée. Après l'avoir démontré, on donnera quelques exemples de calcul du groupe tannakien.

4.1. Bons caractères

Dans ce paragraphe et le suivant, on se place sur un corps algébriquement clos de caractéristique p , que l'on omettra de la notation. Soit $j: \mathbb{G}_m \hookrightarrow \mathbb{P}^1$ l'inclusion.

DÉFINITION 4.1. — *Soient M un faisceau pervers sur \mathbb{G}_m et \mathcal{L}_χ le faisceau de Kummer associé à un caractère continu χ du groupe fondamental modéré $\pi_1^{\text{mod}}(\mathbb{G}_m)$. On dit que χ est bon pour M si la flèche canonique d'oubli des supports*

$$Rj_!(M \otimes \mathcal{L}_\chi) \longrightarrow Rj_*(M \otimes \mathcal{L}_\chi)$$

est un isomorphisme dans $D_c^b(\mathbb{P}^1, \overline{\mathbf{Q}}_\ell)$. Autrement, on dira que χ est mauvais pour M .

LEMME 4.2. — *Pour un objet donné M , il y a au plus $2\text{rg}(M)$ mauvais caractères, où $\text{rg}(M)$ désigne le rang générique du faisceau constructible $\mathcal{H}^{-1}(M)$.*

7. Par contre, le groupe des caractères ℓ -adiques continus de $\pi_1^{\text{mod}}(\mathbb{G}_{m,\bar{k}})$ est muni d'une structure de $\overline{\mathbf{Q}}_\ell$ -schéma à une infinité dénombrable de composantes connexes isomorphes à $\text{Spec}(\overline{\mathbf{Q}}_\ell \otimes_{\mathbf{Z}_\ell} \mathbf{Z}_\ell[[X]])$, et l'on dispose d'un foncteur de $D_c^b(\mathbb{G}_{m,\bar{k}}, \overline{\mathbf{Q}}_\ell)$ vers la catégorie des modules à cohomologie bornée et cohérente sur ce schéma envoyant M vers un objet dont la fibre en un caractère χ est $\text{R}\Gamma(\mathbb{G}_{m,\bar{k}}, M \otimes \mathcal{L}_\chi)$. C'est ce point de vue qui permet à Gabber et Loeser de démontrer certains des résultats du numéro suivant.

DÉMONSTRATION — Si M est ponctuel, tous les caractères sont bons. En dévissant M en sa partie ponctuelle et non ponctuelle comme dans (9), on peut donc supposer que M est de la forme $\mathcal{F}[1]$ pour un faisceau constructible \mathcal{F} sur \mathbb{G}_m qui n'a pas de sections ponctuelles. Posons $\mathcal{G} = \mathcal{F} \otimes \mathcal{L}_\chi$. Comme le foncteur $j_!$ est exact, le caractère χ est bon pour \mathcal{F} si et seulement si $j_!\mathcal{G} \cong j_*\mathcal{G}$ et $R^1j_*\mathcal{G} = 0$. Compte tenu de la description des foncteurs $j_!$, j_* et R^1j_* dans l'exemple 2.7, ces isomorphismes reviennent à dire que \mathcal{G} , en tant que représentation des groupes d'inertie $I_{\bar{0}}$ et I_{∞} , n'a pas d'invariants ni de coinvariants. Or, si $j_0: \mathbb{G}_m \hookrightarrow \mathbb{A}^1$ désigne l'inclusion, les suites exactes

$$(15) \quad 0 \longrightarrow \mathcal{G}^{I_{\bar{0}}} \longrightarrow H^0(\mathbb{A}^1, j_{0!}\mathcal{G}[1]) \longrightarrow H^0(\mathbb{G}_m, \mathcal{G}[1]) \longrightarrow \mathcal{G}_{I_{\bar{0}}} \longrightarrow 0,$$

$$(16) \quad 0 \longrightarrow \mathcal{G}^{I_{\infty}} \longrightarrow H_c^0(\mathbb{G}_m, \mathcal{G}[1]) \longrightarrow H^0(\mathbb{A}^1, j_{0!}\mathcal{G}[1]) \longrightarrow \mathcal{G}_{I_{\infty}} \longrightarrow 0$$

montrent que ces invariants et coinvariants ont même dimension [22, p. 22]. Il suffit donc d'éviter les inverses des caractères modérés χ apparaissant dans la monodromie locale de \mathcal{F} autour de 0 et ∞ et il y en a au plus $2\mathrm{rg}(M)$. \square

4.2. Une catégorie tannakienne de faisceaux pervers sur \mathbb{G}_m

Soit $m: \mathbb{G}_m \times \mathbb{G}_m \rightarrow \mathbb{G}_m$ la loi de multiplication. La catégorie dérivée $D_c^b(\mathbb{G}_m, \overline{\mathbf{Q}}_\ell)$ est munie de deux *produits de convolution*

$$M \star_! N = Rm_!(M \boxtimes N), \quad M \star N = Rm_*(M \boxtimes N),$$

qui sont échangés par la dualité de Verdier. En combinant la suite spectrale de Leray pour le morphisme m , l'identité $m^*\mathcal{L}_\chi = \mathcal{L}_\chi \otimes \mathcal{L}_\chi$ et la formule de Künneth [20, §2.5], on obtient des isomorphismes

$$(17) \quad \mathrm{R}\Gamma_c(\mathbb{G}_m, (M \star_! N) \otimes \mathcal{L}_\chi) = \mathrm{R}\Gamma_c(\mathbb{G}_m, M \otimes \mathcal{L}_\chi) \otimes \mathrm{R}\Gamma_c(\mathbb{G}_m, N \otimes \mathcal{L}_\chi),$$

$$(18) \quad \mathrm{R}\Gamma(\mathbb{G}_m, (M \star N) \otimes \mathcal{L}_\chi) = \mathrm{R}\Gamma(\mathbb{G}_m, M \otimes \mathcal{L}_\chi) \otimes \mathrm{R}\Gamma(\mathbb{G}_m, N \otimes \mathcal{L}_\chi).$$

En général, aucun des produits de convolution ne préserve les objets pervers. Par exemple, le carré de convolution d'un objet de Kummer $\mathcal{L}_\chi[1]$ est égal à $\mathcal{L}_\chi[2]$ qui n'est pas pervers; dans un sens que l'on précisera ci-dessous, c'est la seule obstruction. Si M et N sont pervers, il en va de même pour $M \boxtimes N$ et, le morphisme m étant affine, l'objet $M \star N$ est semipervers. Comme $\mathbb{D}(M \star_! N) = \mathbb{D}(M) \star \mathbb{D}(N)$ est également semipervers, si la flèche d'oubli des supports $M \star_! N \rightarrow M \star N$ est un isomorphisme, le produit de convolution de M et N est pervers. Nous allons introduire une localisation de la catégorie $\mathbf{Perv}(\mathbb{G}_m, \overline{\mathbf{Q}}_\ell)$ sur laquelle cette flèche devient toujours un isomorphisme.

LEMME 4.3. — *Soit M un faisceau pervers sur \mathbb{G}_m .*

(a) *On a $\chi(\mathbb{G}_m, M) \geq 0$.*

(b) *Si $\chi(\mathbb{G}_m, M) = 0$, alors M est de la forme $\mathcal{F}[1]$ pour un faisceau lisse \mathcal{F} qui est extension successive de faisceaux de Kummer \mathcal{L}_χ .*

DÉMONSTRATION — La caractéristique d’Euler étant additive par rapport aux suites exactes, le dévissage (9) de M en sa partie ponctuelle et non ponctuelle donne

$$\chi(\mathbb{G}_m, M) = \chi(\mathbb{G}_m, M_{\text{pct}}) + \chi(\mathbb{G}_m, M_{\text{npct}}).$$

Le premier terme est la dimension de $H^0(\mathbb{G}_m, M_{\text{pct}})$. Puisque $M_{\text{npct}} = \mathcal{F}[1]$ pour un faisceau constructible \mathcal{F} sur \mathbb{G}_m et que la caractéristique d’Euler de \mathbb{G}_m est nulle, la formule de Grothendieck–Ogg–Shafarevich est dans ce cas l’égalité

$$(19) \quad \chi(\mathbb{G}_m, M_{\text{npct}}) = \text{Sw}_0(\mathcal{F}) + \text{Sw}_\infty(\mathcal{F}) + \sum_{x \in \mathbb{G}_m(\bar{k})} [\text{dr}_x(\mathcal{F}) + \text{Sw}_x(\mathcal{F})]$$

dont tous les termes sont positifs car \mathcal{F} n’a pas de sections ponctuelles.

Supposons maintenant $\chi(\mathbb{G}_m, M) = 0$. On a alors $H^0(\mathbb{G}_m, M_{\text{pct}}) = 0$, d’où $M_{\text{pct}} = 0$ vu qu’un faisceau ponctuel sans sections globales est nul. Par suite, $M = \mathcal{F}[1]$ et tous les termes du membre droit de (19) s’annulent. Puisque \mathcal{F} n’a pas de sections ponctuelles et que $\text{dr}_x(\mathcal{F}) = 0$ pour tout x , il s’agit d’un faisceau lisse sur \mathbb{G}_m . Comme $\text{Sw}_0(\mathcal{F})$ et $\text{Sw}_\infty(\mathcal{F})$ sont nuls, \mathcal{F} a ramification modérée à l’infini et correspond donc à une représentation continue de $\pi_1^{\text{mod}}(\mathbb{G}_m)$. Or ce groupe est abélien, comme on l’a vu dans le paragraphe 2.4, et ses caractères sont précisément les faisceaux de Kummer \mathcal{L}_χ . \square

On dira qu’un faisceau pervers est *négligeable* si sa caractéristique d’Euler est nulle. Soit $\mathbf{Nég}(\mathbb{G}_m)$ la sous-catégorie pleine de $\mathbf{Perv}(\mathbb{G}_m, \overline{\mathbf{Q}}_\ell)$ formée des objets négligeables. Par le lemme 4.3, elle est *épaisse* : dans une suite exacte $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$, l’objet B est négligeable si et seulement si A et C sont négligeables. On peut donc, d’après Gabber et Loeser, réaliser la construction suivante : soit $\overline{\mathbf{Nég}}$ la sous-catégorie pleine de $D_c^b(\mathbb{G}_m, \overline{\mathbf{Q}}_\ell)$ formée des objets M dont tous les faisceaux pervers de cohomologie ${}^p\mathcal{H}^i(M)$ sont négligeables. Alors $\overline{\mathbf{Nég}}$ est une sous-catégorie épaisse, et la localisation

$$(20) \quad \mathbf{Perv}(\mathbb{G}_m, \overline{\mathbf{Q}}_\ell) / \mathbf{Nég}(\mathbb{G}_m)$$

est équivalente à une sous-catégorie abélienne de la localisation de $D_c^b(\mathbb{G}_m, \overline{\mathbf{Q}}_\ell)$ relativement à $\overline{\mathbf{Nég}}$, en fait le cœur d’une t -structure [11, §3.6].

PROPOSITION 4.4. — Soient M et N deux faisceaux pervers sur \mathbb{G}_m . La flèche naturelle $M \star_! N \rightarrow M \star N$ dans $D^b(\mathbb{G}_m, \overline{\mathbf{Q}}_\ell)$ est un isomorphisme modulo $\overline{\mathbf{Nég}}$.

DÉMONSTRATION — Grâce au lemme 4.2, il existe un caractère modéré χ tel que les complexes $\text{R}\Gamma_c(\mathbb{G}_m, \cdot)$ et $\text{R}\Gamma(\mathbb{G}_m, \cdot)$ soient isomorphes pour les trois objets $M \otimes \mathcal{L}_\chi$, $N \otimes \mathcal{L}_\chi$ et $(M \star_! N) \otimes \mathcal{L}_\chi$. En particulier, la flèche naturelle

$$\text{R}\Gamma_c(\mathbb{G}_m, M \otimes \mathcal{L}_\chi) \otimes \text{R}\Gamma_c(\mathbb{G}_m, N \otimes \mathcal{L}_\chi) \rightarrow \text{R}\Gamma(\mathbb{G}_m, M \otimes \mathcal{L}_\chi) \otimes \text{R}\Gamma(\mathbb{G}_m, N \otimes \mathcal{L}_\chi)$$

est un isomorphisme. Or cette flèche s’identifie à

$$\text{R}\Gamma_c(\mathbb{G}_m, (M \star_! N) \otimes \mathcal{L}_\chi) \longrightarrow \text{R}\Gamma(\mathbb{G}_m, (M \star N) \otimes \mathcal{L}_\chi)$$

d'après (17) et (18) et, comme la source est isomorphe à $\mathrm{R}\Gamma(\mathbb{G}_m, (M \star! N) \otimes \mathcal{L}_\chi)$ par le choix de χ , on en déduit que l'oubli des supports induit un isomorphisme

$$\mathrm{R}\Gamma(\mathbb{G}_m, (M \star! N) \otimes \mathcal{L}_\chi) \longrightarrow \mathrm{R}\Gamma(\mathbb{G}_m, (M \star N) \otimes \mathcal{L}_\chi).$$

Soit C le cône du morphisme $M \star! N \rightarrow M \star N$. Quitte à remplacer C par $C \otimes \mathcal{L}_\chi$, ce qui précède implique l'annulation $\mathrm{R}\Gamma(\mathbb{G}_m, C) = 0$. Dans la suite spectrale

$$E_2^{a,b} = H^a(\mathbb{G}_m, {}^p\mathcal{H}^b(C)) \implies H^{a+b}(\mathbb{G}_m, C \otimes \mathcal{L}_\chi),$$

qui calcule la cohomologie d'un objet de la catégorie dérivée à partir de celle de ses faisceaux pervers de cohomologie, tous les termes $E_2^{a,b}$ avec $a \neq 0, 1$ s'annulent car \mathbb{G}_m est une courbe affine. La suite spectrale dégénère donc à la deuxième page, et la condition $\mathrm{R}\Gamma(\mathbb{G}_m, C) = 0$ équivaut à $\mathrm{R}\Gamma(\mathbb{G}_m, {}^p\mathcal{H}^b(C)) = 0$ pour tout b . Par conséquent, les faisceaux pervers ${}^p\mathcal{H}^b(C)$ sont négligeables. \square

Il sera utile de disposer de représentants explicites des classes d'équivalence dans (20). Katz considère la sous-catégorie $\mathbf{P}(\mathbb{G}_m)$ de $\mathbf{Perv}(\mathbb{G}_m, \overline{\mathbf{Q}}_\ell)$ formée des faisceaux pervers n'ayant pas de sous-objets ni de quotients du type Kummer décalé $\mathcal{L}_\chi[1]$. Dans [20, §2.6], il démontre que, pour un tel M , les objets $M \star! N$ et $M \star N$ sont pervers quel que soit le faisceau pervers N sur \mathbb{G}_m . On peut alors parler de l'image de la flèche d'oubli des supports dans $\mathbf{P}(\mathbb{G}_m)$ et définir la *convolution intermédiaire*

$$M \star_{\mathrm{int}} N = \mathrm{im}(M \star! N \longrightarrow M \star N).$$

En composant l'inclusion de $\mathbf{P}(\mathbb{G}_m)$ dans $\mathbf{Perv}(\mathbb{G}_m, \overline{\mathbf{Q}}_\ell)$ avec le passage à la localisation on obtient, d'après [11, §3.7], une équivalence de catégories

$$\mathbf{P}(\mathbb{G}_m) \cong \mathbf{Perv}(\mathbb{G}_m, \overline{\mathbf{Q}}_\ell) / \mathbf{Nég}(\mathbb{G}_m)$$

qui envoie la convolution intermédiaire \star_{int} sur le produit de convolution. En particulier, chaque classe d'équivalence dans la localisation a un unique représentant dans $\mathbf{P}(\mathbb{G}_m)$.

THÉORÈME 4.5 (Gabber–Loeser, Katz, Deligne)

- (a) Munie du produit de convolution intermédiaire \star_{int} , de l'objet neutre δ_1 et de la dualité $M^\vee = [x \mapsto x^{-1}]^*\mathbb{D}(M)$, la catégorie $\mathbf{P}(\mathbb{G}_m)$ est tannakienne.
- (b) Notons $j_0: \mathbb{G}_m \hookrightarrow \mathbb{A}_m^1$ l'inclusion. Pour n'importe quel faisceau de Kummer \mathcal{L}_χ sur \mathbb{G}_m , la correspondance

$$M \longmapsto H^0(\mathbb{A}^1, j_{0!}(M \otimes \mathcal{L}_\chi))$$

définit un foncteur fibre ω_χ sur la catégorie tannakienne $\mathbf{P}(\mathbb{G}_m)$.

DÉMONSTRATION — La première assertion est le théorème 3.7.5 de Gabber–Loeser [11] et la deuxième, que Katz attribue à Deligne, est démontrée dans l'appendice à [22]. \square

Remarque 4.6. — Quel que soit le faisceau pervers M sur \mathbb{G}_m , la cohomologie $H^i(\mathbb{A}^1, j_{0!}M)$ s'annule en degré non nul. En effet, on peut supposer que M est ou bien ponctuel, auquel cas l'assertion est évidente, ou bien extension intermédiaire $\mathcal{F}[1]$,

auquel cas les groupes $H^i(\mathbb{A}^1, j_{0!}M) = H^{i+1}(\mathbb{A}^1, j_{0!}\mathcal{F})$ s'annulent en degré $i = 1$ car \mathbb{A}^1 est une courbe affine et en degré $i = -1$ car \mathcal{F} n'a pas de sections globales ponctuelles non nulles. Comme les caractéristiques d'Euler usuelle et à support compact d'un faisceau ℓ -adique coïncident, on en déduit l'égalité $\dim H^0(\mathbb{A}^1, j_{0!}M) = \chi(\mathbb{G}_m, M)$. En particulier, la dimension tannakienne d'un objet M de $\mathbf{P}(\mathbb{G}_m)$ est donnée par sa caractéristique d'Euler.

4.3. Les classes de conjugaison $\theta_{E,\chi}$

Plaçons-nous maintenant sur un corps fini k . Soit $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$ la sous-catégorie pleine de $\mathbf{Perv}(\mathbb{G}_{m,k}, \overline{\mathbf{Q}}_\ell)$ formée des objets M tels que le faisceau pervers $M_{\bar{k}}$ sur $\mathbb{G}_{m,\bar{k}}$ déduit de M par extension des scalaires appartienne à la sous-catégorie $\mathbf{P}(\mathbb{G}_m)$ du paragraphe précédent. La convolution intermédiaire et le foncteur fibre

$$M \mapsto \omega(M) = H^0(\mathbb{A}_k^1, j_{0!}M)$$

munissent $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$ d'une structure de catégorie tannakienne.

LEMME 4.7. — *La sous-catégorie pleine de $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$ formée des faisceaux pervers ι -purs de poids zéro est stable par le produit de convolution intermédiaire.*

DÉMONSTRATION — Si M et N sont des faisceaux ι -purs de poids zéro sur $\mathbb{G}_{m,k}$, leur produit extérieur $M \boxtimes N$ est également ι -pur de poids zéro sur $\mathbb{G}_{m,k} \times \mathbb{G}_{m,k}$. D'après le résultat principal de Weil II (théorème 2.14), $M \star_! N = Rm_!(M \boxtimes N)$ est ι -mixte de poids ≤ 0 . Puisque tout quotient d'un tel faisceau pervers est encore ι -mixte de poids ≤ 0 par [2, Prop. 5.3.1], on en déduit que $M \star_{\text{int}} N$ est ι -mixte de poids ≤ 0 . Or le dual $\mathbb{D}(M \star_{\text{int}} N)$ s'identifie à la convolution intermédiaire $\mathbb{D}(M) \star_{\text{int}} \mathbb{D}(N)$ et est donc ι -mixte de poids ≤ 0 aussi. Par conséquent, $M \star_{\text{int}} N$ est ι -pur de poids zéro. \square

Soit M un faisceau pervers dans $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$ semisimple et ι -pur de poids zéro. En combinant les suites exactes (15) et (16) dans la preuve du lemme 4.2, on voit que $Rj_!M \rightarrow Rj_*M$ est un isomorphisme si et seulement si les applications

$$H_c^0(\mathbb{G}_{m,\bar{k}}, M) \longrightarrow \omega(M) \longrightarrow H^0(\mathbb{G}_{m,\bar{k}}, M)$$

d'oubli des supports et de restriction sont des isomorphismes [22, Thm. 4.1]. Si c'est le cas, $\omega(M)$ est ι -pur de poids zéro d'après le théorème principal de Weil II, c'est-à-dire que les valeurs propres de Frobenius agissant sur $\omega(M)$ sont unitaires.

Étant donné une extension finie E de k et un caractère multiplicatif $\chi: E^\times \rightarrow \overline{\mathbf{Q}}_\ell^\times$, notons \mathcal{L}_χ le système local de Kummer sur $\mathbb{G}_{m,E}$ défini dans l'exemple 2.5. Si L est une extension finie de E , le tiré en arrière de \mathcal{L}_χ sur $\mathbb{G}_{m,L}$ est le faisceau de Kummer associé au caractère $\chi \circ N_{L/E}$. Vus comme des faisceaux lisses sur $\mathbb{G}_{m,\bar{k}}$, les \mathcal{L}_χ sont donc les caractères *d'ordre fini* du groupe fondamental modéré

$$\pi_1^{\text{mod}}(\mathbb{G}_{m,\bar{k}}) = \varprojlim_{E/k \text{ finie}} E^\times,$$

où les applications de transition sont données par la norme. On dira que le caractère χ est *bon* ou *mauvais* pour M si χ est bon ou mauvais pour l'objet $M_{\bar{k}}$ sur $\mathbb{G}_{m,\bar{k}}$ au sens de la définition 4.1. Quitte à identifier (E, χ) avec $(L, \chi \circ N_{L/E})$ pour toute extension finie L de E , le lemme 4.2 entraîne qu'il y a au plus $2\text{rg}(M)$ mauvais caractères pour M .

En remplaçant M par $M \otimes \mathcal{L}_\chi$ dans ce qui précède, la caractérisation de bons caractères en termes du foncteur ω implique le résultat suivant :

PROPOSITION 4.8. — *Soient M un faisceau pervers dans $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$ et $\langle M \rangle^\otimes$ la sous-catégorie tannakienne qu'il engendre. Supposons que M est semisimple et ι -pur de poids zéro. Si un caractère $\chi: E^\times \rightarrow \overline{\mathbf{Q}}_\ell^\times$ est bon pour M , alors χ est bon pour n'importe quel objet N dans $\langle M \rangle^\otimes$ et la correspondance*

$$N \mapsto \omega_\chi(N) = H_c^0(\mathbb{G}_{m,\bar{k}}, M \otimes \mathcal{L}_\chi)$$

définit un foncteur fibre sur $\langle M \rangle^\otimes$. Le groupe $\omega_\chi(N)$ est ι -pur de poids zéro et le Frobenius géométrique F_E est un automorphisme tensoriel de ω_χ .

Fixons un foncteur fibre ω sur la catégorie tannakienne $\mathbf{P}(\mathbb{G}_m)$, par exemple

$$\omega(M) = H^0(\mathbb{A}_{\bar{k}}^1, j_{0!}M).$$

Soient M un faisceau pervers dans $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$ et $M_{\bar{k}}$ l'objet correspondant de $\mathbf{P}(\mathbb{G}_m)$. Par le théorème principal des catégories tannakiennes, ω induit des équivalences

$$\langle M \rangle^\otimes \cong \mathbf{Rep}_{\overline{\mathbf{Q}}_\ell}(G_{\text{arith},M}) \quad \langle M_{\bar{k}} \rangle^\otimes \cong \mathbf{Rep}_{\overline{\mathbf{Q}}_\ell}(G_{\text{geom},M})$$

entre la catégorie engendrée par M (*resp.* $M_{\bar{k}}$) et la catégorie des $\overline{\mathbf{Q}}_\ell$ -représentations de dimension finie du groupe des automorphismes tensoriels $G_{\text{arith},M}$ (*resp.* $G_{\text{geom},M}$) de la restriction de ω à $\langle M \rangle^\otimes$ (*resp.* à $\langle M_{\bar{k}} \rangle^\otimes$). Il s'agit dans les deux cas de sous-groupes de $\text{GL}(\omega(M))$. Concrètement, $G_{\text{arith},M}$ est le sous-groupe des automorphismes linéaires γ tels que, pour toute construction tensorielle $M^{t:s} = \bigoplus M^{\otimes r_i} \otimes (M^\vee)^{\otimes s_i}$, l'action de γ sur $\omega(M^{t:s})$ laisse globalement stables toutes les images des sous-quotients de $M^{t:s}$. Comme l'objet $M_{\bar{k}}$ a plus de sous-quotients à respecter, on a l'inclusion

$$G_{\text{geom},M} \subseteq G_{\text{arith},M}.$$

Le corps de coefficients $\overline{\mathbf{Q}}_\ell$ étant algébriquement clos, n'importe quel autre choix de foncteur fibre sur $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$ donne lieu à un groupe isomorphe à $G_{\text{arith},M}$ par un isomorphisme unique à un automorphisme intérieur près. Tout élément dans le groupe associé à un autre foncteur fibre définit donc une classe de conjugaison dans $G_{\text{arith},M}$. En particulier, pour une extension finie E de k et un caractère multiplicatif $\chi: E^\times \rightarrow \overline{\mathbf{Q}}_\ell^\times$, le Frobenius géométrique F_E est un automorphisme tensoriel de ω_χ , d'où des classes de conjugaison dans le groupe $G_{\text{arith},M}(\overline{\mathbf{Q}}_\ell) \subset G_{\text{arith},M}(\mathbf{C})$ que l'on notera $\text{Frob}_{E,\chi}$.

Si le faisceau pervers M est ι -pur de poids zéro, alors il est géométriquement semi-simple d'après [2, Thm. 5.3.8]. Comme la représentation fidèle $G_{\text{geom},M} \rightarrow \text{GL}(\omega(M))$ correspondant à $M_{\bar{k}}$ est complètement réductible, $G_{\text{geom},M}$ est un groupe algébrique

réductif. Dorénavant, on supposera que M est *arithmétiquement* semisimple, c'est-à-dire semisimple en tant qu'objet de $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$. Ceci signifie que M est un faisceau pervers semisimple sur $\mathbb{G}_{m,k}$ qui, géométriquement, n'admet pas de faisceaux de Kummer décalés comme sous-objets ni comme quotients. Dans ce cas, le groupe $G_{\text{arith},M}$ est réductif aussi. Si le caractère χ est bon pour M , la classe de conjugaison $\text{Frob}_{E,\chi}$ a des valeurs propres unitaires d'après la proposition 4.8. Choisissons un sous-groupe compact maximal K du groupe de Lie réductif $G_{\text{arith},M}(\mathbf{C})$. Reprenant mot par mot l'argument du paragraphe 3.2, on associe à chaque $\text{Frob}_{E,\chi}$ une classe de conjugaison $\theta_{E,\chi}$ dans $K^\#$.

4.4. Le théorème principal

THÉORÈME 4.9 (Katz). — *Soit M un faisceau pervers dans $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$. Supposons que M est ι -pur de poids zéro, semisimple, et que les groupes $G_{\text{geom},M}$ et $G_{\text{arith},M}$ sont égaux. Choisissons un sous-groupe compact maximal K de $G_{\text{arith},M}(\mathbf{C})$. Lorsque le degré des extensions E/k tend vers l'infini, les classes de conjugaison $\{\theta_{E,\chi}\}_{\chi \text{ bon}}$ s'équirépartissent dans $K^\#$ selon la mesure $\mu_{K^\#}$ induite par la mesure de Haar sur K .*

DÉMONSTRATION — Soit $\text{Bon}(E, M)$ l'ensemble de bons caractères $\chi: E^\times \rightarrow \overline{\mathbf{Q}}_\ell^\times$ pour l'objet M ; d'après le lemme 4.2, il est non vide dès que le degré de E est assez grand. Démontrons que, pour toute fonction centrale continue $f: K \rightarrow \mathbf{C}$, on a

$$(21) \quad \frac{1}{|\text{Bon}(E, M)|} \sum_{\chi \in \text{Bon}(E, M)} f(\theta_{E,\chi}) \longrightarrow \int_K f \mu_K$$

lorsque le degré de E tend vers l'infini. En utilisant le théorème de Peter–Weyl, on se réduit à prouver que le membre gauche de (21) converge vers zéro lorsque f est la trace d'une représentation irréductible non triviale de dimension finie Λ_K de K .

Soit Λ la seule $\overline{\mathbf{Q}}_\ell$ -représentation irréductible non triviale de $G_{\text{arith},M}$ associée à Λ_K par le théorème 3.1. Par le biais de l'équivalence $\langle M \rangle^\otimes \simeq \mathbf{Rep}_{\overline{\mathbf{Q}}_\ell}(G_{\text{arith},M})$, elle correspond à un faisceau pervers *simple* N dans la sous-catégorie tannakienne de $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$ engendrée par M . De plus, l'hypothèse $G_{\text{geom},M} = G_{\text{arith},M}$ entraîne que N est *géométriquement simple*, et la non-trivialité de Λ se traduit par le fait que $N_{\bar{k}}$ n'est pas isomorphe à l'objet neutre δ_1 . En termes de N , la trace $\text{Tr}_{\Lambda_K}(\theta_{E,\chi})$ est égale à

$$S(N, E, \chi) = \sum_{x \in E^\times} \chi(x) \text{Tr}(\text{Frob}_{E,x} | N)$$

par la formule des traces de Grothendieck. Le résultat découlerait donc de l'estimée suivante lorsque le degré de E tend vers l'infini :

$$\frac{1}{|\text{Bon}(E, M)|} \sum_{\chi \in \text{Bon}(E, M)} S(N, E, \chi) = O\left(1/\sqrt{|E|}\right).$$

Pour la démontrer, remarquons d'abord qu'il suffit d'estimer la moyenne des sommes $S(N, E, \chi)$ sur *tous* les caractères multiplicatifs. En effet, en notant $\text{Mauv}(E, M)$

le complémentaire de $\text{Bon}(E, M)$ dans E^\times , on a :

$$(22) \quad \frac{1}{|\text{Bon}(E, M)|} \sum_{\chi \in \text{Bon}(E, M)} S(N, E, \chi) = \left(1 + \frac{|\text{Mauv}(E, M)|}{|\text{Bon}(E, M)|} \right) \frac{1}{|E^\times|} \sum_{\chi} S(N, E, \chi) - \frac{1}{|\text{Bon}(E, M)|} \sum_{\chi \in \text{Mauv}(E, M)} S(N, E, \chi).$$

Or il y a au plus $2\text{rg}(M)$ mauvais caractères pour l'objet M et la majoration

$$|S(N, E, \chi)| \leq \dim \omega(N)$$

est valable quel que soit χ . En effet, comme N appartient à la catégorie tannakienne engendrée par M , c'est un faisceau pervers semisimple et ι -pur de poids zéro dans $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$; il en va de même pour $N \otimes \mathcal{L}_\chi$. La cohomologie à support compact d'un tel faisceau est concentrée en degré zéro et $H_c^0(\mathbb{G}_{m, \bar{k}}, N \otimes \mathcal{L}_\chi)$ est ι -mixte de poids ≤ 0 , d'où l'inégalité voulue par la formule des traces et la remarque 4.6.

Estimons donc la moyenne des $S(N, E, \chi)$. Par orthogonalité des caractères,

$$\frac{1}{|E^\times|} \sum_{\chi} S(N, E, \chi) = \frac{1}{|E^\times|} \sum_{x \in E^\times} \text{Tr}(\text{Frob}_{E, x} | N) \sum_{\chi} \chi(x) = \text{Tr}(\text{Frob}_{E, 1} | N).$$

D'après la classification des faisceaux pervers simples sur une courbe (exemple 2.16), on sait que N est de l'un de ces deux types :

- Si N est ponctuel, alors il existe un point $t \in k^\times \setminus \{1\}$ et une unité ℓ -adique α tels que $N = \alpha^{\deg} \otimes \delta_t$, la possibilité $t = 1$ étant exclue par l'hypothèse que $N_{\bar{k}}$ n'est pas isomorphe à δ_1 . Dans ce cas, $\text{Tr}(\text{Frob}_{E, 1} | N) = 0$.

- Si N n'est pas ponctuel, alors il est de la forme $\mathcal{F}[1]$ pour un faisceau extension intermédiaire \mathcal{F} sur \mathbb{G}_m . Comme N est ι -pur de poids zéro, \mathcal{F} est ι -pur de poids -1 , d'où les inégalités

$$|\text{Tr}(\text{Frob}_{E, 1} | N)| = |-\text{Tr}(\text{Frob}_{E, 1} | \mathcal{F})| \leq \frac{\dim(\mathcal{F}_{\bar{1}})}{\sqrt{|E|}} \leq \frac{\text{rg}(\mathcal{F})}{\sqrt{|E|}},$$

où la dernière provient du fait que, le faisceau \mathcal{F} étant une extension intermédiaire, la fibre $\mathcal{F}_{\bar{1}} = (\mathcal{F}_{\bar{\eta}})^{I_{\bar{1}}}$ a dimension plus petite ou égale au rang générique de \mathcal{F} .

Dans les deux cas, on a $|\text{Tr}(\text{Frob}_{E, 1} | N)| \leq \text{rg}(N) / \sqrt{|E|}$. Compte tenu de (22), on en déduit la majoration

$$(23) \quad \left| \frac{1}{|\text{Bon}(E, M)|} \sum_{\chi \in \text{Bon}(E, M)} S(N, E, \chi) \right| \leq \frac{2(\text{rg}(N) + \dim \omega(N))}{\sqrt{|E|}}$$

pour toute extension E/k de degré assez grand pour que $|\text{Mauv}(E, M)| \leq \sqrt{|E|} - 1$. C'est ce qu'il fallait pour conclure la démonstration. \square

En prenant l'image directe de la mesure de Haar normalisée par la trace $\text{Tr}: K \rightarrow \mathbf{C}$, on trouve immédiatement le corollaire suivant :

COROLLAIRE 4.10. — *Sous les hypothèses du théorème 4.9, les sommes exponentielles $\{S(M, E, \chi)\}_{\chi \text{ bon}}$ se répartissent comme les traces de matrices aléatoires dans K lorsque le degré des extensions E/k tend vers l’infini.*

Remarque 4.11. — Dans [22, Thm. 7.2], Katz établit un résultat un peu plus général. Si M est semisimple, $G_{\text{geom}, M}$ est un sous-groupe *distingué* de $G_{\text{arith}, M}$ et il suffit de supposer que le quotient $G_{\text{arith}, M}/G_{\text{geom}, M}$ est isomorphe à un groupe cyclique $\mathbf{Z}/n\mathbf{Z}$. Dans ce cas, on choisit un sous-groupe compact maximal K_{arith} de $G_{\text{arith}, M}(\mathbf{C})$ et l’on note K_{geom} son intersection avec $G_{\text{geom}, M}(\mathbf{C})$. C’est un sous-groupe distingué de K_{arith} avec quotient $K_{\text{arith}}/K_{\text{geom}} = \mathbf{Z}/n\mathbf{Z}$, d’où une application $K_{\text{arith}}^{\#} \rightarrow \mathbf{Z}/n\mathbf{Z}$. Étant donné un entier d modulo n , soient $K_{\text{arith}, d}^{\#} \subset K_{\text{arith}}^{\#}$ l’image inverse de d par cette application et $\mu_d^{\#}$ la mesure de probabilité sur $K_{\text{arith}, d}^{\#}$ déduite de la mesure de Haar normalisée sur K_{geom} . Le résultat est le suivant : pour n’importe quelle suite d’extensions E/k de degré congru à d modulo n dont les cardinaux tendent vers l’infini, les classes de conjugaison $\{\theta_{E, \chi}\}_{\chi \text{ bon}}$ s’équirépartissent dans $K_{\text{arith}, d}^{\#}$ selon la mesure $\mu_d^{\#}$.

En présence de bornes uniformes pour les constantes intervenant dans l’estimée (23), le théorème d’équirépartition de Katz admet la variante horizontale suivante :

THÉORÈME 4.12 (Katz). — *Soient G un groupe réductif sur $\overline{\mathbf{Q}}_{\ell}$ muni d’une représentation fidèle de dimension n et K un sous-groupe compact maximal de $G(\mathbf{C})$. Soit (k_i) une suite de corps finis de caractéristique distincte de ℓ dont les cardinaux tendent vers l’infini. Pour chaque i , soit M_i un objet semisimple et ι -pur de poids zéro de la catégorie $\mathbf{P}_{\text{arith}}(\mathbb{G}_{m, k_i})$ ayant dimension tannakienne n . Supposons que l’égalité $G_{\text{geom}, M_i} = G_{\text{arith}, M_i} = G$ soit satisfaite, l’objet M_i correspondant à la représentation fidèle de G , et qu’il existe un nombre réel $C \geq n$ tel que $\text{rg}(M_i) \leq C$ pour tout i . Alors les classes de conjugaison $\{\theta_{k_i, \chi}\}_{\chi \in \text{Bon}(k_i, M_i)}$ s’équirépartissent dans $K^{\#}$.*

ESQUISSE DE DÉMONSTRATION — Soient Λ une représentation irréductible non triviale de G et N_i l’objet correspondant dans la sous-catégorie $\langle M_i \rangle^{\otimes}$ de $\mathbf{P}_{\text{arith}}(\mathbb{G}_{m, k_i})$. D’après le critère d’équirépartition de Weyl, il suffit de démontrer que

$$\frac{1}{|\text{Bon}(k_i, M_i)|} \sum_{\chi \in \text{Bon}(k_i, M_i)} S(N_i, k_i, \chi)$$

converge vers zéro lorsque i tend vers l’infini. Comme il y a au plus $2\text{rg}(M_i)$ mauvais caractères, (23) donne l’inégalité

$$(24) \quad \left| \frac{1}{|\text{Bon}(k_i, M_i)|} \sum_{\chi \in \text{Bon}(k_i, M_i)} S(N_i, k_i, \chi) \right| \leq \frac{2(\text{rg}(N_i) + \dim \omega(N_i))}{\sqrt{|k_i|}}$$

pour tout i tel que $2C \leq \sqrt{|k_i|} - 1$. Le groupe $G \subset \text{GL}(V)$ étant réductif, il existe des entiers a et b tels que Λ soit sous-représentation de $V^{\otimes a} \otimes (V^{\vee})^{\otimes b}$. Chaque faisceau

pervers N_i est donc sous-objet de la construction tensorielle $M_i^{\otimes a} \otimes (M_i^\vee)^{\otimes b}$ et

$$\dim \omega(N_i) \leq \dim(M_i^{\otimes a} \otimes (M_i^\vee)^{\otimes b}) = n^{a+b} \leq C^{a+b}.$$

Par ailleurs, une analyse fine de la formule de Grothendieck–Ogg–Shafarevich montre que, pour tous faisceaux pervers semisimples K et L dans $\mathbf{P}_{\text{arith}}(\mathbb{G}_{m,k_i})$, l’inégalité

$$\text{rg}(K \star_{\text{int}} L) \leq \text{rg}(K) \dim \omega(L) + \text{rg}(L) \dim \omega(K)$$

est satisfaite [22, Thm. 28.2]. Par récurrence sur $a + b$, on en déduit l’inégalité

$$\text{rg}(M_i^{\otimes a} \otimes (M_i^\vee)^{\otimes b}) \leq (a + b)(\dim \omega(M_i))^{a+b-1} \text{rg}(M_i)$$

et donc $\text{rg}(N_i) \leq (a + b)C^{a+b}$, ce qui permet de conclure que le membre gauche de (24) converge vers zéro lorsque i tend vers l’infini. \square

4.5. Exemples

Dans ce dernier paragraphe, nous expliquons comment déduire du théorème d’équirépartition de Katz les résultats annoncés dans l’introduction.

Exemple 4.13 (Sommes de Gauss). — Soit $\psi: k \rightarrow \overline{\mathbf{Q}}_\ell^\times$ un caractère additif non trivial. Alors $M = j_0^* \mathcal{L}_\psi(1/2)[1]$ est un faisceau pervers simple sur $\mathbb{G}_{m,k}$, pur de poids zéro, qui n’est pas géométriquement isomorphe à un faisceau de Kummer décalé (par exemple, car il a ramification sauvage à l’infini). Par la formule de Grothendieck–Ogg–Shafarevich, sa dimension tannakienne vaut

$$\chi(\mathbb{G}_m, M) = -\chi(\mathbb{G}_m, j_0^* \mathcal{L}_\psi) = \text{Sw}_\infty(\mathcal{L}_\psi) = 1,$$

d’où des inclusions $G_{\text{geom},M} \subseteq G_{\text{arith},M} \subseteq \text{GL}(1)$. Comme aucune puissance de convolution de $M_{\bar{k}}$ n’est l’objet neutre, le groupe $G_{\text{geom},M}$ est égal à $\text{GL}(1)$ tout entier. Il s’ensuit que M est un objet de $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$ vérifiant les hypothèses du théorème. Soit E une extension de k à q éléments et posons $\psi_q = \psi \circ \text{Tr}_{E/k}$. Pour tout caractère multiplicatif $\chi: E^\times \rightarrow \overline{\mathbf{Q}}_\ell^\times$, on a

$$S(M, E, \chi) = -\frac{1}{\sqrt{q}} \sum_{x \in E^\times} \chi(x) \psi_q(x) = -\frac{g(\psi_q, \chi)}{\sqrt{q}},$$

de sorte que $\omega_\chi(M)$ est pur de poids zéro si χ n’est pas trivial et de poids -1 si χ est trivial. Les bons caractères pour M sont donc les caractères non triviaux. Comme le compact maximal est $K = S^1$, le corollaire 4.10 est l’énoncé que les sommes de Gauss normalisées sont équiréparties dans S^1 selon la mesure de Haar.

Pour traiter les exemples des sommes d’Evans et de Rudnick, on aura besoin d’un résultat en théorie des représentations [22, Thm. 14.1] :

PROPOSITION 4.14. — *Soit M un faisceau pervers dans $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$ de dimension tannakienne deux. Supposons que M est pur de poids zéro, autodual et géométriquement semisimple. Si M n’est géométriquement isomorphe à aucun de ses translatés non triviaux $[x \mapsto ax]^* M$, où $a \in \bar{k} \setminus \{1\}$, alors $G_{\text{geom},M} = G_{\text{arith},M} = \text{SL}(2)$.*

Exemple 4.15 (Sommes d’Evans). — Soit $\psi: k \rightarrow \overline{\mathbf{Q}}_\ell^\times$ un caractère additif non trivial. L’objet $M = \mathcal{L}_{\psi(x-x^{-1})}(1/2)[1]$ est pur de poids zéro. Comme $\mathcal{L}_{\psi(x-x^{-1})}$ est un faisceau de rang un à ramification sauvage à l’infini, M est un objet géométriquement simple dans $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$. Par la formule de Grothendieck–Ogg–Shafarevich, il a dimension

$$\chi(\mathbb{G}_{m,\bar{k}}, M) = \text{Sw}_0(\mathcal{L}_{\psi(x-x^{-1})}) + \text{Sw}_\infty(\mathcal{L}_{\psi(x-x^{-1})}) = 2.$$

En écrivant $\mathcal{L}_{\psi(x-x^{-1})}$ comme $\mathcal{L}_{\psi(x)} \otimes \mathcal{L}_{\psi(-1/x)}$, on voit que le dual de ce système local est $\mathcal{L}_{\psi(x^{-1}-x)}$, d’où $M^\vee = M$ pour le dual tannakien. De plus, le translaté

$$[x \mapsto ax]^* M = \mathcal{L}_{\psi(ax-(ax)^{-1})}(1/2)[1]$$

n’est géométriquement isomorphe à M pour aucun $a \neq 1$ (si tel était le cas, l’objet $\mathcal{L}_{\psi((a-1)x+(1-a^{-1})x^{-1})}(1/2)[1]$ serait géométriquement trivial, mais le système local sous-jacent a ramification sauvage à l’infini pour tout $a \neq 1$). Les hypothèses de la proposition 4.14 sont donc satisfaites et $G_{\text{geom},M} = G_{\text{arith},M} = \text{SL}(2)$. Comme $\mathcal{L}_{\psi(x-x^{-1})}$ a ramification totalement sauvage en 0 et ∞ , il résulte de la preuve du lemme 4.2 que tous les caractères sont bons pour M . Le théorème d’équirépartition de Katz est dans ce cas l’énoncé que les angles $\{\theta_{q,\chi}\}_\chi$ des sommes d’Evans s’équirépartissent dans l’intervalle $[0, \pi]$ selon la mesure de Sato–Tate lorsque q tend vers l’infini.

Exemple 4.16 (Sommes de Rudnick). — Dans cet exemple, on suppose que la caractéristique de k est impaire et on note $j_1: \mathbb{G}_{m,k} \setminus \{1\} \hookrightarrow \mathbb{G}_{m,k}$ l’inclusion. Les sommes de Rudnick sont associées à l’objet

$$M = j_{1!} \mathcal{L}_{\psi(\frac{x+1}{x-1})}(1/2)[1]$$

de la catégorie $\mathbf{P}_{\text{arith}}(\mathbb{G}_m)$, qui est géométriquement simple et pur de poids zéro, par exemple parce que le faisceau $\mathcal{L}_{\psi(\frac{x+1}{x-1})}$ a ramification totalement sauvage en 1 et son prolongement par zéro coïncide donc avec l’image directe usuelle. La formule de Grothendieck–Ogg–Shafarevich donne dans ce cas l’égalité

$$\chi(\mathbb{G}_{m,\bar{k}}, M) = \text{dr}_1(j_{1!} \mathcal{L}_{\psi(\frac{x+1}{x-1})}) + \text{Sw}_1(j_{1!} \mathcal{L}_{\psi(\frac{x+1}{x-1})}) = 1 + 1 = 2$$

car $j_{1!} \mathcal{L}_{\psi(\frac{x+1}{x-1})}$ s’étend en un faisceau lisse en 0 et ∞ . De plus, l’identité $\frac{x^{-1}+1}{x^{-1}-1} = -\frac{x+1}{x-1}$ implique que M est autodual. Comme 1 est le seul point de $\mathbb{G}_m(\bar{k})$ en lequel le faisceau $j_{1!} \mathcal{L}_{\psi(\frac{x+1}{x-1})}$ n’est pas lisse, M n’est géométriquement isomorphe à aucun translaté non trivial, d’où $G_{\text{geom},M} = G_{\text{arith},M} = \text{SL}(2)$ par la proposition 4.14. La monodromie de $j_{1!} \mathcal{L}_{\psi(\frac{x+1}{x-1})}$ autour de 0 et ∞ étant triviale, tout caractère *non trivial* χ est bon pour M et le théorème d’équirépartition de Katz répond positivement à la question de Rudnick.

RÉFÉRENCES

- [1] *Revêtements étales et groupe fondamental (SGA 1)* – Documents Mathématiques, vol. 3, Société Mathématique de France, Paris, 2003, Séminaire de géométrie algébrique du Bois Marie 1960–61 dirigé par A. Grothendieck.
- [2] A. A. BEĬLISON, J. BERNSTEIN, P. DELIGNE & O. GABBER – « Faisceaux pervers », Analysis and topology on singular spaces, I (Luminy, 1981), Astérisque, vol. 100, Soc. Math. France, Paris, 1982, p. 5–171.
- [3] V. BLOMER, E. FOUVRY, E. KOWALSKI, P. MICHEL, D. MILIĆEVIĆ & W. SAWIN – « The second moment theory of families of L -functions the case of twisted Hecke L -functions », <https://arxiv.org/abs/1804.01450>.
- [4] J.-L. BRYLINSKI – « Transformations canoniques, dualité projective, théorie de Lefschetz, transformations de Fourier et sommes trigonométriques », *Astérisque* **140-141** (1986), p. 3–134.
- [5] B. COLLAS, M. DETTWEILER, S. REITER & W. SAWIN – « Monodromy of elliptic curve convolution, seven-point sheaves of G_2 -type and motives of Beauville type », <https://arxiv.org/abs/1803.05883>.
- [6] B. CONRAD – « Reductive group schemes », Autour des schémas en groupes. Vol. I, Panor. Synthèses, vol. 42/43, Soc. Math. France, Paris, 2014, p. 93–444.
- [7] H. DAVENPORT – « On certain exponential sums », *J. reine angew. Math.* **169** (1933), p. 158–176.
- [8] P. DELIGNE – « Applications de la formule des traces aux sommes trigonométriques », Cohomologie étale, Lecture Notes in Math., vol. 569, Springer-Verlag, 1977, Séminaire de Géométrie Algébrique du Bois-Marie SGA 4 $\frac{1}{2}$.
- [9] ———, « La conjecture de Weil. II », *Publ. Math. IHÉS* (1980), no. 52, p. 137–252.
- [10] E. FOUVRY & P. MICHEL – « Sur le changement de signe des sommes de Kloosterman », *Ann. of Math.* **165** (2007), no. 3, p. 675–715.
- [11] O. GABBER & F. LOESER – « Faisceaux pervers ℓ -adiques sur un tore », *Duke Math. J.* **83** (1996), no. 3, p. 501–606.
- [12] C. GAUSS – « Summatio serierum quarundam singularium », *Comment. Soc. regiae sci. Göttingen* (1811), Werke II, p. 9–45.
- [13] A. GROTHENDIECK – « Formule de Lefschetz et rationalité des fonctions L », Dix exposés sur la cohomologie des schémas, vol. 3, North-Holland, Amsterdam, 1968, p. 31–45.
- [14] C. HALL, J. P. KEATING & E. RODITTY-GERSHON – « Variance of arithmetic sums and L -functions in $\mathbb{F}_q[t]$ », *Algebra Number Theory* **13** (2019), no. 1, p. 19–92.
- [15] H. HASSE – « Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper », *J. reine angew. Math.* **172** (1935), p. 37–54.

- [16] L. ILLUSIE – « Deligne’s ℓ -adic Fourier transform », Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985), Proc. Sympos. Pure Math., vol. 46, Amer. Math. Soc., Providence, RI, 1987, p. 151–163.
- [17] N. M. KATZ – *Sommes exponentielles*, Astérisque, vol. 79, Société Mathématique de France, Paris, 1980, Cours à Orsay, automne 1979, rédigé par G. Laumon.
- [18] ———, *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Mathematics Studies, vol. 116, Princeton University Press, Princeton, NJ, 1988.
- [19] ———, « Exponential sums over finite fields and differential equations over the complex numbers : some interactions », *Bull. Amer. Math. Soc.* **23** (1990), no. 2, p. 269–309.
- [20] ———, *Rigid local systems*, Annals of Mathematics Studies, vol. 139, Princeton University Press, Princeton, NJ, 1996.
- [21] ———, « L -functions and monodromy : four lectures on Weil II », *Adv. Math.* **160** (2001), no. 1, p. 81–132.
- [22] ———, *Convolution and equidistribution. Sato-Tate theorems for finite-field Mellin transforms*, Annals of Mathematics Studies, vol. 180, Princeton University Press, Princeton, NJ, 2012.
- [23] ———, « On a question of Keating and Rudnick about primitive Dirichlet characters with squarefree conductor », *Int. Math. Res. Not.* (2013), no. 14, p. 3221–3249.
- [24] ———, « Elliptic convolution, G_2 , and elliptic surfaces », *Astérisque* **370** (2015), p. 197–205.
- [25] ———, « On two questions of Entin, Keating, and Rudnick on primitive Dirichlet characters », *Int. Math. Res. Not.* (2015), no. 15, p. 6044–6069.
- [26] N. M. KATZ & G. LAUMON – « Transformation de Fourier et majoration de sommes exponentielles », *Publ. Math. IHÉS* (1985), no. 62, p. 361–418.
- [27] N. M. KATZ & P. SARNAK – *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.
- [28] J. P. KEATING & Z. RUDNICK – « The variance of the number of prime polynomials in short intervals and in residue classes », *Int. Math. Res. Not.* (2014), no. 1, p. 259–288.
- [29] H. D. KLOOSTERMAN – « On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$ », *Acta Math.* **49** (1927), no. 3-4, p. 407–464.
- [30] E. KOWALSKI – « Book review of *Convolution and equidistribution : Sato-Tate theorems for finite fields Mellin transforms* », *Bull. Amer. Math. Soc.* **51** (2014), no. 1, p. 141–149.
- [31] T. KRÄMER & R. WEISSAUER – « Vanishing theorems for constructible sheaves on abelian varieties », *J. Algebraic Geom.* **24** (2015), no. 3, p. 531–568.

- [32] P. KURLBERG & Z. RUDNICK – « Hecke theory and equidistribution for the quantization of linear maps of the torus », *Duke Math. J.* **103** (2000), no. 1, p. 47–77.
- [33] ———, « On the distribution of matrix elements for the quantum cat map », *Ann. of Math. (2)* **161** (2005), no. 1, p. 489–507.
- [34] S. LANG & A. WEIL – « Number of points of varieties in finite fields », *Amer. J. Math.* **76** (1954), p. 819–827.
- [35] G. LAUMON – « Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil », *Publ. Math. IHÉS* **65** (1987), p. 131–210.
- [36] ———, « Exponential sums and ℓ -adic cohomology : A survey », *Israel Journal of Mathematics* **120** (2000), no. 1, p. 225–257.
- [37] G. LAUMON – « La transformation de Fourier géométrique et ses applications », *Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990)*, Math. Soc. Japan, Tokyo, 1991, p. 437–445.
- [38] C. PERRET-GENTIL – « Integral monodromy groups of Kloosterman sheaves », *Mathematika* (2018), no. 3, p. 652–678.
- [39] H. POINCARÉ – « Fonctions modulaires et fonctions fuchsienues », *Ann. Fac. Sci. Toulouse Sci. Math. Sci. Phys. (3)* **3** (1911), p. 125–149.
- [40] M. RAYNAUD – « Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes », *Séminaire Bourbaki (17e année : 1964/65)*, Vol. 9, exp. no. 286, 129–147, Société Mathématique de France, Paris, 1995.
- [41] L. ROSENZWEIG – « On the fluctuations of matrix elements of the quantum cat map », *Int. Math. Res. Not.* (2011), no. 21, p. 4884–4933.
- [42] Z. RUDNICK – « The arithmetic theory of quantum maps », *Equidistribution in number theory, an introduction*, NATO Sci. Ser. II Math. Phys. Chem., vol. 237, Springer, Dordrecht, 2007, p. 331–342.
- [43] H. SALIÉ – « Über die Kloostermanschen Summen $S(u, v; q)$ », *Math. Z.* **34** (1932), no. 1, p. 91–109.
- [44] W. SAWIN – « A tannakian category and a horizontal equidistribution conjecture for exponential sums », *Thèse*, Princeton University, 2016.
- [45] J.-P. SERRE – *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979.
- [46] A. WEIL – « On some exponential sums », *Proc. Nat. Acad. Sci. U. S. A.* **34** (1948), p. 204–207.
- [47] R. WEISSAUER – « Vanishing theorems for constructible sheaves on abelian varieties over finite fields », *Math. Ann.* **365** (2016), no. 1-2, p. 559–578.
- [48] H. WEYL – « Über die Gleichverteilung von Zahlen mod. Eins », *Math. Ann.* **77** (1916), no. 3, p. 313–352.

- [49] P. XI – « Large sieve inequalities for algebraic trace functions », *Int. Math. Res. Not.* (2017), no. 16, p. 4840–4881, avec un appendice de É. Fouvry, E. Kowalski et P. Michel.

Javier FRESÁN

CMLS, École Polytechnique

F-91128 Palaiseau Cedex

E-mail : javier.fresan@polytechnique.edu