ANNALES SCIENTIFIQUES DE L'É.N.S.

ÉTIENNE FOUVRY
PHILIPPE MICHEL

Sur certaines sommes d'exponentielles sur les nombres premiers

Annales scientifiques de l'É.N.S. 4^e série, tome 31, n° 1 (1998), p. 93-130
<http://www.numdam.org/item?id=ASENS_1998_4_31_1_93_0>

Ann. scient. Éc. Norm. Sup.,
4e série, t. 31, 1998, p. 93 à 130.

SUR CERTAINES SOMMES D'EXPONENTIELLES SUR LES NOMBRES PREMIERS

PAR ÉTIENNE FOUVRY ET PHILIPPE MICHEL

RÉSUMÉ. – Par des méthodes de géométrie algébrique, nous donnons des majorations pour les sommes d'exponentielles de la forme suivante $\sum_{p\leq x} \exp\left(2\pi i \frac{f(p)}{q}\right)$, où q désigne un nombre premier (grand), $f(X)$ est une fraction rationnelle à coefficients entiers et p décrit les nombres premiers plus petits que $x(\leq q)$. Nous raffinons également la méthode dans le cas où $f(X)$ est de la forme $f(X) = X^k + uX$ (k un entier différent de 0 et de 1). © Elsevier, Paris

Mots-clés : Sommes d'exponentielles, nombres premiers

ABSTRACT. – Using methods inherited from algebraic geometry, we give bounds for exponential sums of the type $\sum_{p\leq x} \exp\left(2\pi i \frac{f(p)}{q}\right)$, where q is a large prime number, $f(X)$ is a general rational function over $\mathbf{Z}$ and the sum is performed over primes less than $x(\leq q)$. Some extensions of the method are given when $f(X)$ is of the form $f(X) = X^k + uX$ (k integer different from 0 and 1). © Elsevier, Paris

Keywords: Exponential sums, prime numbers.

I. Introduction

L'idée de ce travail nous est venue en étudiant l'article de Friedlander et Iwaniec ([Fr-I1]) : faire appel à des méthodes profondes de géométrie algébrique, héritées des célèbres travaux de Deligne ([De1], [De3]) sur la conjecture de Weil, pour majorer certaines sommes d'exponentielles apparaissant naturellement en théorie analytique des nombres. Parmi la multitude de choix possibles, notre attention s'est portée sur la situation suivante :

Soient q un nombre premier, $\psi(.)$ caractère additif non trivial sur $\mathbb{F}_q$,

† *$f(X)$ est de la forme $f(X) = \frac{P(X)}{Q(X)}$ où $P(X)$ et $Q(X)$ sont deux polynômes unitaires de $\mathbb{Z}[X]$ premiers entre eux. On suppose en outre, que f n'est ni un polynôme constant, ni un polynôme de degré* 1.

Classification AMS 11L03, 11L20

On cherche à majorer la somme trigonométrique :

$$S(f;q,x)=\sum_{p<x}\psi(f(p)),$$

faite sur les nombres premiers p tels que $f(p)$ soit défini, ayant pour but de donner des majorations non triviales de cette somme lorsque x est d'ordre de grandeur assez proche de q.

Notre premier résultat est le

THÉORÈME 1.1. – *Soient $\varepsilon>0$, q un nombre premier, x un réel vérifiant $1\leq x\leq q$, f une fraction rationnelle comme dans (†). Il existe alors une constante C, dépendant au plus de ε, de* $\deg P$ *et* $\deg Q$*, telle que, pour tout caractère additif ψ non trivial de $\mathbb{F}_q$, on ait l'inégalité*

$$|S(f;q,x)|\leq Cq^{\frac{3}{16}+\varepsilon}x^{\frac{25}{32}}. \tag{1.1}$$

Il est bon de mettre en avant le caractère universel des exposants $\frac{3}{16}$ et $\frac{25}{32}$ apparaissant dans (1.1) et l'inexactitude de cette majoration lorsque $f(X)\equiv 1$ ou $f(X)\equiv X$.

L'étude de $S(f;q,x)$ pour f polynôme, entre dans le cadre plus général de celles des sommes

$$S=\sum_{p\leq x}e(f(p)),$$

avec f polynôme de $\mathbb{R}[X]$ et $e(.)=\exp(2\pi i.)$. Cette étude fut inaugurée par Vinogradov ([Vi]) dans le cas où $f(X)=X$ et explorée par de nombreux auteurs : pour résumer, lorsque $f(X)$ est un polynôme de degré k avec un coefficient de plus haut degré jouissant d'une approximation rationnelle adéquate, on obtient une majoration non triviale de S en combinant les méthodes classiques de majorations de sommes d'exponentielles sur les polnômes (Weyl, Hardy–Littlewood, Vinogradov) et les identités combinatoires sur la fonction caractéristique des nombres premiers (Vinogradov, Vaughan). De telles démarches, appliquées à l'étude de notre somme $S(f;q,x)$, pour f polynôme de degré $k\geq 2$ sont efficaces pour x petit ($x\geq q^{\frac{1}{k}+\varepsilon}$) –ce qui n'est pas le cas de (1.1). Par contre, ces résultats ne donnent que des majorations $S(f;q,q)=O(q^{1-\vartheta_k})$ avec $\vartheta_k>0$ tendant vers 0, lorsque k tend vers l'infini (voir Lemme 6.1 ci-dessous). Toutes ces méthodes sont totalement inadaptées pour f fraction rationnelle, non polynomiale de $\mathbb{Z}(X)$. Pour l'abondante littérature sur ce sujet, on se reportera avec profit aux introductions de [Hu], [Gh], [Harm], [Ba–H]...

Il existe un autre abord de $S(f;q,x)$ par les caractères de Dirichlet. En adoptant les notations classiques de la théorie des nombres premiers ([Da] Chap.20), au risque d'une ambiguïté passagère sur la signification de la lettre ψ, on a, en suivant la démonstration

de ([Va] Corollary 2.1), les relations

$$\begin{aligned}\tilde{S}(f;q,x): &= \sum_{n<x}\Lambda(n)\psi(f(n)) = \sum_{a=0}^{q-1}\psi(f(a)) \sum_{\substack{n<x\\ n\equiv a(\mathrm{mod}\ q)}}\Lambda(n)\\ &= \frac{1}{\varphi(q)}\sum_{a=1}^{q-1}\psi(f(a)) \sum_{\chi(\mathrm{mod}\ q)}\overline{\chi}(a)\psi(x,\chi) + O\big(\log(2qx)\big)\\ &\ll \frac{1}{\varphi(q)}\sum_{\chi(\mathrm{mod}\ q)}\Big|\sum_{a=1}^{q-1}\psi(f(a))\overline{\chi}(a)\Big||\psi(x,\chi)| + O\big(\log(2qx)\big).\end{aligned}$$

Que χ soit principal ou non, on a la relation

$$\sum_{a=1}^{q-1}\psi(f(a))\overline{\chi}(a) = O_{\deg P,\deg Q}(q^{\frac{1}{2}}),$$

([Schm] Theorem 2G, Page 45, pour f polynôme), d'où, en appliquant ([Va] Theorem 2), on a finalement pour $\tilde{S}(f;q,x)$ et, par conséquent pour $S(f;q,x)$ la majoration

$$|S(f;q,x)| \leq C(q^{-\frac{1}{2}}x + q^{\frac{1}{8}}x^{\frac{3}{4}} + q^{\frac{1}{2}}x^{\frac{1}{2}})q^{\varepsilon},$$

majoration qui n'a d'intérêt que pour $x > q$. Cette majoration est due à Vaughan lorsque $f(X) = X$ et est évoquée par Harman ([Harm]) lorsque $f(X) = X^k$, k entier positif, l'entier q n'étant pas nécessairement premier. En conclusion, on perçoit bien le caractère critique de l'étude de $S(f;q,x)$ pour $x = q$

Signalons que, pour $x = q$, longueur de l'intervalle qui nous intéresse essentiellement dans ce travail (voir la discussion à la fin du paragraphe VI), et pour tout f vérifiant (†), le gain par rapport à la majoration triviale $O(q/\log q)$ est une puissance de q – plus précisément $q^{\frac{1}{32}-\varepsilon}$–alors que les méthodes de [Mi] ne fourniraient qu'un gain en $O(\log q/\log\log q)$ si elles étaient appliquées à la somme $S(f;q,q)$. Remarquons aussi que l'inégalité (1.1) est intéressante pour $q^{\frac{6}{7}+\varepsilon} \leq x \leq q$.

En fait notre méthode s'applique tout aussi bien à des sommes

$$\sum_{n<x} g(n)\psi(f(n)),$$

où $g(n)$ est une fonction arithmétique ayant les propriétés de convolution suffisantes pour conduire à deux types de sommes

$$S_{\mathrm{I}}(f,q;M,N) = \sum_{m\leq M}\alpha_m\sum_{n\in\mathcal{I}}\psi(f(mn))$$

et

$$S_{\mathrm{II}}(f,q;M,N) = \sum_{m\leq M}\alpha_m\sum_{n\in\mathcal{I}}\beta_n\psi(f(mn)),$$

où

– α_m et β_n sont deux suites de nombres complexes inférieurs à 1 en module,

– $\mathcal{I}$ un intervalle non spécifié, contenant N entiers,

– M et $N \geq 1$ vérifient d'autres inégalités impliquées par la nature de la décomposition combinatoire de g.

Les sommes S_{I} et S_{II} sont, dans la dénomination de Vaughan de type I ou de type II, et apparaissent dans la décomposition des fonctions de diviseurs généralisées τ_k, la fonction de Möbius μ et de quantité d'autres fonctions arithmétiques raisonnables. Ainsi, pouvons–nous écrire l'inégalité

$$\Big| \sum_{1 \leq n \leq x} \mu(n)\psi(f(n)) \Big| \leq C_{k,\varepsilon} q^{\frac{3}{16}+\varepsilon} x^{\frac{25}{32}},$$

sous les conditions du Théorème 1.1. Une telle relation montre, pour ainsi dire, une quasi–orthogonalité entre une fonction de nature *arithmétique* (la fonction $\mu(n)$) et une fonction de nature *algébrique* (la fonction $\psi(f(n))$). Autrement dit, les oscillations de l'une sont indépendantes des oscillations de l'autre.

Une agréable conséquence du Théorème 1.1 est la suivante :

Soit $f_1, \cdots, f_{33}$, trente–trois fractions rationnelles du type (†). *Alors, l'équation en les nombres premiers $p_i \leq q$,*

$$N = f_1(p_1) + \cdots + f_{33}(p_{33}) (\mathrm{mod}\ q),$$

a, pour $q \longrightarrow \infty$, comme nombre de solutions : $\dfrac{\pi(q)^{33}}{q}\big(1 + O(q^{-1/33})\big)$, uniformément sur l'entier N.

Ceci se démontre en détectant la congruence étudiée par les caractères ψ^h avec $0 \leq h < q$, le terme $h = 0$ fournissant le terme principal, les autres termes étant traités par le Théorème 1.1.

Dans cette étude, joueront un rôle particulier, tant par les résultats que par les méthodes, les f *quasi–monômes*. On dira que f est un *quasi–monôme* de degré k (k entier relatif différent de 0 est 1), si f est de la forme $f(X) \equiv X^k + uX$ avec $u \in \mathbb{Z}$.(Observons que si $k < 0$ et $u \neq 0, 1$, f n'est pas exactement de la forme (†) ; lorsque q-u, il suffit évidemment de remplacer ψ par ψ^u).

La preuve du Théorème 1.1 passera d'abord par la

PROPOSITION 1.2. – *Soient $\varepsilon > 0$, $\ell \geq 1$ un entier, (α_m) une suite de nombres complexes de module inférieurs à 1, M et N deux nombres réels supérieurs à 1 vérifiant*

$$(MN)^\ell \leq q^{\ell+1}, \quad M \leq N^\ell,$$

et $\mathcal{I}$ un intervalle contenant N entiers. Soit f vérifiant (†).

On a alors les trois majorations

$$(1.2.1) \qquad S_{\mathrm{I}}(f, q; M, N) = O\Big(q^{\frac{1}{2\ell}+\varepsilon} M^{\frac{2\ell+1}{2\ell+2}} N^{\frac{2\ell^2-1}{2\ell^2+2\ell}} + q^{\frac{1}{4\ell}+\varepsilon} M^{\frac{2\ell^2+2\ell-1}{2\ell(\ell+1)}} N^{\frac{2\ell^2+\ell-2}{2\ell(\ell+1)}}\Big);$$

si f n'est pas un polynôme (autrement dit, si $\deg Q \geq 1$);

$$S_{\mathrm{I}}(f,q;M,N) = O\Big(q^{\frac{1}{2\ell}+\varepsilon} M^{\frac{2\ell+1}{2\ell+2}} N^{\frac{2\ell^2-1}{2\ell^2+2\ell}} + q^{\frac{1}{4\ell}+\varepsilon} M^{\frac{2\ell^2+2\ell-2}{2\ell(\ell+1)}} N^{\frac{2\ell^2+\ell-3}{2\ell(\ell+1)}}\Big), \tag{1.2.2}$$

si f est un polynôme unitaire de degré strictement supérieur à 2 et à ℓ ;

$$S_{\mathrm{I}}(f,q;M,N) = O\Big(q^{\frac{1}{2\ell}+\varepsilon} M^{\frac{2\ell+1}{2\ell+2}} N^{\frac{2\ell^2-1}{2\ell^2+2\ell}}\Big), \tag{1.2.3}$$

si f est un quasi–monôme de degré k avec $k < 0$ ou avec $k \geq 3$ et $\ell < \min\{p, p|(k, q-1)\}$. Chacune des relations (1.2.1), (1.2.2) *et* (1.2.3) *est uniforme sur l'ensemble des caractères additifs ψ modulo q, non triviaux, la constante O, suivant les situations, dépendant au plus de ε, ℓ, $\deg P$, $\deg Q$ et k.*

Les relations (1.2.1), (1.2.2) et (1.2.3) sont de précision croissante, les deuxièmes termes à droite de (1.2.1) et (1.2.2) s'effaceront devant les premiers car on appliquera ces estimations avec $\ell = 3$ et $MN \leq q$ lors de la preuve du Théorème 1.1. Lorsque $f(X) = X^{-1}$, en fixant $\ell = 2$, on retrouve le Theorem 3 de [Fr–I1]. Pour apprécier la force de cette majoration, il suffit de constater que dans le cas où α_m est constamment égal à 1, une application directe du théorème de Deligne ne donnerait rien d'intéressant pour $M = N = \sqrt{q}$. Par contre la technique d'allongement de l'intervalle de sommation (voir le début du paragraphe IV), nous permet de gagner $q^{1/24-\varepsilon}$ par rapport à la majoration triviale.

Nous abordons maintenant le cas des sommes de type II. Nous montrerons la

PROPOSITION 1.3. – *Soient $\varepsilon > 0$, (α_m) et (β_n) deux suites de nombres complexes de modules inférieurs à 1, M et N deux nombres réels vérifiant $1 \leq M, N \leq q$. Alors, pour tout f vérifiant* (†), *on a la majoration*

$$S_{\mathrm{II}}(f,q;M,N) = \sum_{m\leq M} \alpha_m \sum_{n\leq N} \beta_n \psi(f(mn)) = O_{\deg P, \deg Q}\Big(MN^{\frac{1}{2}} + q^{\frac{1}{4}} M^{\frac{1}{2}} N (\log q)^{\frac{1}{2}}\Big),$$

uniformément sur l'ensemble des caractères additifs ψ modulo q, non triviaux.

Ce résultat très général et facile à obtenir à partir de la majoration de Weil des sommes d'exponentielles en une variable (voir paragraphe V), ne donne rien dans le cas parfaitement symétrique $M = N = \sqrt{q}$. Par contre si f est un polynôme de degré $k \geq 3$, on obtient aussi un résultat, en appliquant à la somme (5.1), la majoration de Weyl, déjà évoquée plus haut, mais la qualité de cette majoration décroît lorsque k augmente.

Par une autre méthode beaucoup plus élaborée de géométrie algébrique, nous pouvons traiter le cas des quasi–monômes, où nous utilisons de façon cruciale la multiplicativité du morphisme monôme. Notre technique fait appel aux résultats très profonds de Katz sur la détermination des groupes de monodromie géométrique attachés à certaines familles de sommes d'exponentielles à un paramètre, obtenues par la transformée de Fourier–Deligne–Laumon. Bien que, apparemment cette étude soit sans influence sur le Théorème 1.1, nous montrerons le

THÉORÈME 1.4. – *Soient $k \in \mathbb{Z} - \{0,1,2\}$, f le quasi–monôme de degré k défini par $f(X) = X^k + uX$, ℓ un entier, (α_m) et (β_n) deux suites à supports inclus dans $]M, 2M]$ et $]N, 2N]$, vérifiant $|\alpha_m|$ et $|\beta_n| \leq 1$. On a alors, pour tout $\varepsilon > 0$, la majoration*

$$\sum_m \sum_n \alpha_m \beta_n \psi(f(mn)) \ll_{k,\ell,\varepsilon} MNq^{\varepsilon}\big(M^{-\frac{1}{2}} + q^{\frac{3\ell+5}{8\ell(\ell+2)}} (MN)^{-\frac{\ell+1}{2\ell(\ell+2)}}\big), \tag{1.3}$$

uniformément sur ψ non trivial modulo q, $u \in \mathbb{Z}$ et sous les conditions

$$N \leq q, \quad q^{\frac{1}{4}} \leq MN \leq q^{\frac{3\ell+4}{4\ell}} \text{ et } q^{\frac{1}{2}} N^{\ell} \geq M^2,$$

le paramètre ℓ devant vérifier

$$\ell \geq 1 \quad \text{si} \quad k < 0 \quad \text{ou} \quad \text{si} \quad (k, q-1) = 1$$

et

$$1 \leq \ell < \min\{p; p|(k, q-1)\} \quad \text{si} \quad k \geq 3.$$

Ainsi, si $k < 0$ ou si $k \geq 3$ est impair, la somme précédente est, pour $M = N = \sqrt{q}$ en $O(q^{\frac{63}{64}})$; il suffit de fixer $\ell = 2$. Si on peut choisir des valeurs de ℓ très grandes, on accède à des suites (α_m) et (β_n) à supports très courts. À titre d'illustration, nous nous restreignons au cas où $k < 0$, on a le

COROLLAIRE 1.5. – *Soit $k < 0$, $f(X)$ le quasi–monôme $f(X) = X^k + uX$, (α_m) et (β_n) deux suites à supports inclus dans $]M, 2M]$ et $]N, 2N]$, vérifiant $|\alpha_m|$ et $|\beta_n| \leq 1$. Pour tout $\delta > 0$, il existe $\eta(\delta) > 0$, tel qu'on ait la relation*

$$\sum_m \sum_n \alpha_m \beta_n \psi(f(mn)) \ll_{\delta,k} (MN)^{1-\eta},$$

sous les conditions

$$q^{\frac{3}{4}+\delta} \leq MN \leq q^{\frac{5}{4}-\delta} \quad \text{et} \quad q^{\delta} \leq M, \ N \leq q,$$

uniformément sur ψ non trivial modulo q et $u \in \mathbb{Z}$.

Démonstration. – Quitte à intervertir les rôles de M et N, la relation $q^{\frac{1}{2}} N^{\ell} \geq M^2$ est toujours satisfaite pour $\ell \geq 2$. On constate que la relation (1.3) est non triviale dès qu'on a $MN > q^{(3\ell+5)/(4\ell+4)+\varepsilon}$ et $M \geq q^{\delta}$. Il reste donc à trouver $\ell \geq 2$ tel qu'on ait l'encadrement

$$q^{\frac{3\ell+5}{4\ell+4}+\varepsilon} < MN < q^{\frac{3\ell+4}{4\ell}-\varepsilon}.$$

Un tel entier existe puisque les intervalles $\mathcal{I}_\ell = \left]\dfrac{3\ell+5}{4\ell+4}, \dfrac{3\ell+4}{4\ell}\right[$ vérifient : $\bigcup_{\ell=2}^{\infty} \mathcal{I}_\ell = \left]\dfrac{3}{4}, \dfrac{5}{4}\right[$. ■

Le Corollaire 1.5 a une intéressante application à la somme $S(f; q, x)$ définie précédemment :

COROLLAIRE 1.6. – *Soit f un quasi–monôme de degré $k < 0$. Alors pour tout $\delta > 0$, il existe $\eta(\delta) > O$, tel qu'on ait la relation*

$$S(f; q, x) \ll_{\delta,k} x^{1-\eta},$$

sous la condition $q^{3/4+\delta} \leq x \leq q$, uniformément sur ψ non trivial modulo q et $u \in \mathbb{Z}$.

Démonstration. – La philosophie pour traiter une somme sur des nombres premiers est, par des identités combinatoires, de se ramener à des sommes de type I ou II (voir paragraphe VI pour de plus amples détails). Le Corollaire 1.5 traite non trivialement toutes les sommes de type II $S_{\mathrm{II}}(f,q;M,N)$, pour $MN<x$ et $M,\ N\geq x^{\delta}$, pourvu que $q^{3/4+\delta}\leq x\leq q$. Il reste donc des sommes de type I : $S_{\mathrm{I}}(f,q;M,N)$, pour M minuscule, à savoir $M<x^{\delta}$. Un développement en série de Fourier de la fonction caractéristique de $]N,2N]$ et une application directe de la majoration de Weil pour les sommes exponentielles sur des fonctions rationnelles (voir les méthodes du paragraphe IV et le Lemme 4.3), conduisent directement à l'inégalité

$$S_{\mathrm{I}}(f,q;M,N)\ll M\left(\frac{N}{q}+1\right)q^{\frac{1}{2}+\varepsilon},$$

qui suffit largement à notre exigence, car non triviale pour δ assez petit. Il n'est nullement nécessaire de faire appel à (1.2.3). À titre d'application, le Corollaire 1.6 entraîne, pour $q\longrightarrow\infty$, l'équirépartition modulo 1, des fractions $\frac{\bar{p}^k}{q}$ ($2\leq p\leq q^{3/4+\delta}$ et $\bar{p}$ inverse de p modulo q), pour k entier positif fixé.

Le corollaire suivant est, en quelque sorte, l'analogue du Théorème 3 et du Corollaire 1 de [Fr–I2], qui donnent des majorations de la somme de caractères

$$\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\chi(a+b)$$

où χ est un caractère multiplicatif, non principal modulo q, et $\mathcal{A}$ et $\mathcal{B}$ sont des ensembles assez denses, d'entiers sans propriété particulière, inclus dans $[1,\sqrt{q}]$, et qui montrent ainsi la régularité des sommes d'éléments de deux suites quelconques. Au lieu de caractères multiplicatifs, nous envisageons des caractères additifs, et au lieu d'additionner des éléments, nous les multiplions, d'où le

COROLLAIRE 1.7. – *Soient $\mathcal{A}$ et $\mathcal{B}$ deux ensembles d'entiers inclus dans $[1,\sqrt{q}]$. Alors, pour tout $\varepsilon>0$, tout caractère ψ non trivial modulo q, on a la majoration*

$$\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\psi(f(ab))=O_{k,\varepsilon}(q^{\frac{59}{60}+\varepsilon}),$$

pour f quasi–monôme de degré k, avec $k\geq 5$ et $(k,6)=1$ ou $k<0$, et

$$\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\psi(f(ab))=O_{\varepsilon}(q^{\frac{63}{64}+\varepsilon}),$$

pour f quasi–monôme de degré $k\geq 3$, impair.

Cet énoncé est une application directe du Théorème 1.4, pour de petites valeurs de ℓ, à savoir $\ell=3$ et $\ell=2$. ■

Lorsque f est un polynôme de degré $k\geq 3$, on a directement comme conséquence de la remarque suivant la Proposition 1.3, une majoration en $O(q^{1-\vartheta_k})$ où $\vartheta_k>0$ tend vers 0 lorsque k tend vers l'infini. On peut regretter que le Théorème 1.4 soit muet sur le cas ou f est une fraction rationnelle générale. En effet notre technique donne naissance à des sommes trigonométriques (dépendant de 2ℓ paramètres) en trois variables, pour lesquelles on peut espérer appliquer ([B–S] Theorem 1). Mais il nous a semblé délicat de traiter la condition *iii)* d'irréductibilité de fibres, en toute généralité pour la famille de sommes rencontrées.

II. Irréductibilité de certaines variétés

a. Un résultat général

Il ne nous a pas été possible de trouver explicitement l'énoncé de la proposition suivante dans la littérature. Toutefois cet énoncé existe de façon sous–jacente dans différents articles que nous a signalés A.Schinzel (...,[Schi1], [D–S], [Fr], [Schi2],...) où est traité le cas où f est un polynôme. Afin d'être complets, nous en donnons une démonstration dans un langage moderne, démonstration dont les principes nous ont été aimablement communiqués par J–L. Colliot–Thélène. Remarquons que dans toutes ces démonstrations, le Théorème de Lüroth joue un rôle décisif et que cette proposition se généralise directement à des polynômes de $k[X_1, \ldots, X_n]$. On a

PROPOSITION 2.1. – *Soit k un corps parfait, $g(X,Y)$ et $h(X,Y)$ deux polynômes de $k[X,Y]$, premiers entre eux, tels que la fraction $f(X,Y) = g(X,Y)/h(X,Y)$ soit non constante sur l'ouvert $\mathbb{A}^2_k - \{z\acute{e}ros \quad de \quad h(X,Y)\}$.*

On a alors l'équivalence entre les deux propriétés

i) *$g(X,Y) - Th(X,Y)$ est réductible sur $\overline{k(T)}[X,Y]$;*

ii) *Il existe $u(V) \in k(V)$ une fraction rationnelle non homographie et $v(X,Y) \in k(X,Y)$ tels que $f(X,Y) = u(v(X,Y))$.*

Si l'une ou l'autre des propriétés précédentes est vérifiée, on peut faire les normalisations suffisantes

- *si $h(X,Y) \in k^*$ (f est donc un polynôme), alors $u(V) \in k[V]$ et $v(X,Y) \in k[X,Y]$,*
- si k est algébriquement clos et si h n'est pas une constante, alors u est une fraction de degré strictement positif.

(on appelle *degré* d'une fraction rationnelle la différence des degrés du numérateur et du dénominateur, soit encore l'ordre du pôle à l'infini.)

Démonstration. – Il est clair que la seconde propriété entraîne la première : écrivant $u(V) = p(V)/q(V)$, il suffit de factoriser $p(V) - Tq(V)$ dans $\overline{k(T)}$ (Dans les paragraphes IIa, IIb et IIc les lettres f, p et q ont une signification différente de celle du paragraphe I, aucune confusion n'est possible).

Montrons l'implication réciproque. Notons encore f le morphisme rationnel

$$\begin{array}{ccc} \mathbb{A}^2_k & \to & \mathbb{A}^1_k \\ (x,y) & \to & f(x,y), \end{array}$$

entre les corps de fonctions, f est décrit par l'injection $k(T) \hookrightarrow k(X,Y) : T \to t = f(X,Y)$. Il s'agit donc de montrer que f admet une factorisation rationnelle de la forme

$$\mathbb{A}^2_k \xrightarrow{v} \mathbb{P}^1_k \xrightarrow{u} \mathbb{P}^1_k,$$

où u n'est pas une homographie. Soit K la clôture algébrique de $k(t)$ dans $k(X,Y)$.

Puisque la fonction f est non constante, on peut choisir deux points fermés M_1 et $M_2 \in \mathbb{A}^2_k$ tels que $h(M_1) \neq 0$, $h(M_2) \neq 0$ et $f(M_1) \neq f(M_2)$. La restriction de f à la droite L passant par M_1 et M_2 est non constante, on en déduit que $k(t)$ puis K s'injectent

dans $k(L)$. Donc K est une extension transcendante pure de degré 1 de k et, par le théorème de Lüroth ([Hart] Ex 2.5.5. p.303–304, par exemple), il existe $v \in k(X,Y)$ tel que $K = k(v)$ et t s'écrit donc sous la forme $t = u(v)$ avec $u \in k(V)$. Le fait que u n'est pas une homographie, c'est–à–dire $K \neq k(t)$, est assuré par le lemme suivant :

LEMME 2.2. – *Si $g(X,Y) - Th(X,Y)$ est réductible dans $\overline{k(T)}[X,Y]$, alors $K \neq k(t)$.*

Démonstration. – Le polynôme $g(X,Y) - Th(X,Y)$ est irréductible dans $k[X,Y,T]$ (c'est un polynôme de degré 1 en T et $g(X,Y)$ et $h(X,Y)$ sont premiers entre eux). Par le lemme de Gauss, la $k[T]$–algèbre $k(T)[X,Y]/\big(g(X,Y) - Th(X,Y)\big)$ est donc intègre. D'après ([Mu] Prop.4 p.142), la réductibilité de $g(X,Y) - Th(X,Y)$ dans $\overline{k}(T)$ implique que $k(T)$ n'est pas séparablement clos dans $\mathrm{Frac}\Big(k(T)[X,Y]/\big(g(X,Y) - Th(X,Y)\big)\Big)$, ce qui signifie que $k(t)$ n'est pas séparablement clos dans $k(X,Y)$. ■

Supposons maintenant que $f(X,Y) = g(X,Y)$. On va montrer qu'on peut choisir $v \in k[X,Y]$: écrivons v et t sous la forme

$$v = \frac{P_1(X,Y)}{P_2(X,Y)},\ P_1,\ P_2 \in k[X,Y],\ \text{et } t = \frac{Q_1(v)}{Q_2(v)},\ Q_1,\ Q_2 \in k[V],\ (Q_1,Q_2) = 1.$$

Supposons que $P_2 \notin k$ et $Q_2 \notin k$; soit λ une racine de Q_2 dans $\bar{k}$ (alors $Q_1(\lambda) \neq 0$), si $P_1 - \lambda P_2$ est non constant, le polynôme $t = f(X,Y)$ a des pôles dans $\mathbb{A}^2_{\bar{k}}$ ce qui est absurde. Dans le cas contraire, soit $\lambda' \neq \lambda$ une autre racine de $Q_2(V)$, c'est alors le polynôme $P_1 - \lambda' P_2$ qui est non constant. On est donc dans le cas où $Q_2(V)$ est de la forme $(V-\lambda)^q$, comme k est parfait $\lambda \in k$; v s'écrit alors sous la forme $v = \lambda + c/P_2(X,Y)$, $c \in k^*$. En faisant le changement de variable $v' = c(v-\lambda)^{-1}$ (on remarque que $k(v') = k(v) = K$), on est ramené au cas $v = P_1(X,Y) \in k[X,Y]$. On voit alors que $P_1 - \lambda$ est non constant, par conséquent Q_2 est de degré 0. ■

Supposons enfin k algébriquement clos, $u(V)$ s'écrit sous la forme $u(V) = Q_1(V)/Q_2(V)$ avec Q_1 et Q_2 deux polynômes premiers entre eux. On peut supposer $\deg Q_1 > \deg Q_2$, en effet, si tel n'est pas le cas, on fait un changement de variable homographique $V = \mu + 1/V'$, où μ est un zéro de Q_2, qui existe puisque u n'est pas une homographie. ■

b. Opérateurs de décalage

Soit ℓ un entier au moins égal à 1 et soit $\mathbf{b} = (b_1, \cdots, b_\ell, b'_1, \cdots, b'_\ell)$ un vecteur de $\mathbb{Z}^{2\ell}$. On définit alors l'opérateur de décalage $\Delta_{\mathbf{b}}$ pour $f \in \mathbb{Z}(X)$, par la formule

$$\big(\Delta_{\mathbf{b}} f\big)(X,Y) = \sum_{i=1}^{\ell} \Big(f((X+b_i)Y) - f((X+b'_i)Y) \Big),$$

et, pour $m \in \mathbb{Z}$, on pose aussi

$$\big(\Delta_{\mathbf{b},m} f\big)(X,Y) = \big(\Delta_{\mathbf{b},m} f\big)(X,Y) - mY.$$

Il est clair que les définitions des opérateurs $\Delta_{\mathbf{b}}$ et $\Delta_{\mathbf{b},m}$ s'étendent au cas où les b_i et m appartiennent à un corps k et f à $k(X)$.

Ces opérateurs apparaîtront naturellement lors de traitement des sommes d'exponentielles, après un shift et l'inégalité de Hölder pour $\Delta_{\mathbf{b}}$ et un développement en série de Fourier pour $\Delta_{\mathbf{b},m}$. Afin d'appliquer un résultat dû à Hooley (voir Lemme 4.1 ci–dessous) sur des majorations de sommes d'exponentielles, nous montrerons que pour la plupart des $\mathbf{b}$, une variété, naturellement associée à $(\Delta_{\mathbf{b},m})$ est absolument irréductible pour tout m.

Soit k un corps et $f(X,Y) \in k(X,Y)$. On dit que f est *composée* s'il existe $u(V) \in k(V)$ qui n'est pas une homographie et $v(X,Y) \in k(X,Y)$, telle que $f(X,Y) = u(v(X,Y))$. On a

PROPOSITION 2.3. – *Soit k un corps algébriquement clos. Soient P, $Q \in k[X]$ deux polynômes premiers entre eux tels que la fraction P/Q ne soit pas un polynôme de degré ≤ 1. Soient $\ell \geq 1$ et $\mathbf{b}$ un vecteur de $k^{2\ell}$, noté indifféremment $\mathbf{b} = (b_1, \cdots, b_\ell, b'_1, \cdots, b'_\ell)$ ou $\mathbf{b} = (b_1, \cdots, b_{2\ell})$. On suppose que $\mathbf{b}$ vérifie les relations*

$$b_i \neq b_j \ (1 \leq i < j \leq 2\ell) \tag{2.1}$$

et

$$b_1 + \cdots + b_\ell - b'_1 - \cdots - b'_\ell \neq 0. \tag{2.2}$$

Alors, si la caractéristique de k est nulle ou si cette caractéristique est supérieure à une certaine fonction des degrés de P et Q, la fraction $(\Delta_{\mathbf{b},m} P/Q)(X,Y)$ n'est composée pour aucun $m \in k$, et la courbe définie sur $\overline{k(T)}$ par l'équation $(\Delta_{\mathbf{b},m} P/Q)(X,Y) - T = 0$ est irréductible sur $\overline{k(T)}$.

La dernière partie de l'énoncé précédent est une conséquence directe de la Proposition 2.1.

Avant de passer à la démonstration, nous énumérons quelques conventions :

• On peut supposer que P et Q sont unitaires, c'est une conséquence de la relation $(\Delta_{\mathbf{b},m})(\lambda f) = \lambda(\Delta_{\mathbf{b},m\lambda^{-1}})(f)$, valable pour tout λ de k^*.

• Si $A(X,Y)$ est un polynôme de $k[X,Y]$, l'égalité $A(X,Y) = cX^aY^b + \cdots$ où $c \neq 0$, signifie que $A(X,Y)$, en tant que polynôme en Y est de degré b et que le coefficient du terme Y^b est un polynôme en X de degré a de terme dominant cX^a.

• Si $S(X)$ est un polynôme de $k[X]$ et $\alpha \in k$, on note s le degré de S et $s(\alpha)$ la multiplicité du zéro α.

• On pose $\varepsilon_i = +1$ ou -1 suivant que $1 \leq i \leq \ell$ ou $\ell + 1 \leq i \leq 2\ell$.

• On écrit $Q(X)$ sous la forme

$$Q(X) = X^{q(0)} R(X),$$

avec $R(X) \in k(X)$ et $R(0) \neq 0$. Avec ces conventions, on pose

$$(\Delta_{\mathbf{b},m} P/Q)(X,Y) \ := \frac{\mathrm{NUM}(X,Y)}{\mathrm{DEN}(X,Y)},$$

avec

$$\begin{aligned}\mathrm{NUM}(X,Y) &= \sum_{i=1}^{2\ell}\varepsilon_i P((X+b_i)Y)\prod_{j=1,j\neq i}^{2\ell}(X+b_j)^{q(0)}R((X+b_j)Y)\\ &\quad -mY^{q(0)+1}\prod_{j=1}^{2\ell}(X+b_j)^{q(0)}R((X+b_j)Y),\\ \mathrm{DEN}(X,Y) &= Y^{q(0)}\prod_{j=1}^{2\ell}(X+b_j)^{q(0)}R((X+b_j)Y).\end{aligned}$$

c. Démonstration de la Proposition 2.3

c.1. Cas où $q(0) \geq 1$

Les polynômes $\mathrm{NUM}(X,Y)$ et $\mathrm{DEN}(X,Y)$ sont premiers entre eux. En effet, les facteurs irréductibles de $\mathrm{DEN}(X,Y)$ sont Y, $X+b_i$ et $(X+b_i)Y-\rho$, où ρ décrit l'ensemble des racines (non nulles) $\mathcal{R}$ de R. Le fait que $X+b_i$ ne divise pas $\mathrm{NUM}(X,Y)$ est une conséquence de (2.1). Puisque P et Q ont des racines différentes, on voit que $(X+b_i)Y-\rho$ ne divise pas $\mathrm{NUM}(X,Y)$. Enfin, en remarquant, d'après (2.2) et la non–nullité de $q(0)P(0)Q(0)$, que $\mathrm{NUM}(X,0)$ a pour terme de plus haut degré $-q(0)P(0)R(0)^{2\ell-1}(b_1+\cdots+b_\ell-b'_1-\cdots-b'_\ell)X^{(2\ell-1)q(0)-1}$, ce qui entraîne que Y ne divise pas $\mathrm{NUM}(X,Y)$.

Supposons donc que $(\Delta_{\mathbf{b},m}P/Q)$ soit composée : on écrit cette fraction sous la forme $(\Delta_{\mathbf{b},m}P/Q) = cQ_1(v)/Q_2(v)$ avec $c\in k^*$, $Q_1(V)=\prod_\lambda(V-\lambda)$, $Q_2(V)=\prod_\mu(V-\mu)$, $(Q_1,Q_2)=1$, Q_1/Q_2 n'étant pas une homographie et $v=P_1(X,Y)/P_2(X,Y)$ avec P_1 et P_2 premiers entre eux. Ainsi les λ comptés avec multiplicité, sont au nombre de q_1 et sont tous distincts des μ, qui, eux, sont au nombre de q_2. Par le même argument que celui situé à la fin de la Proposition 2.1, on peut supposer $q_1>q_2$. Puisque les polynômes $P_1-\lambda P_2$ et $P_1-\mu P_2$ sont premiers entre eux, on a, par identification, pour certains ξ, $\xi'\in k^*$ les deux égalités

$$\mathrm{NUM}(X,Y)=\xi\prod_\lambda(P_1-\lambda P_2)(X,Y),$$

$$\mathrm{DEN}(X,Y)=\xi' P_2^{q_1-q_2}\prod_\mu(P_1-\mu P_2)(X,Y).$$

• Cas où $q_2=0$. Ainsi $\mathrm{DEN}(X,Y)=\xi' P_2^{q_1}$, donc P_2 est divisible par Y. En confrontant les deux expressions de $\mathrm{NUM}(X,Y)$, on parvient à l'égalité

$$\begin{aligned}\mathrm{NUM}(X,0) &= q(0)P(0)R(0)^{2\ell-1}(b_1+\cdots+b_\ell-b'_1-\cdots-b'_\ell)X^{(2\ell-1)q(0)-1}+\cdots\\ &= \xi(P_1(X,0))^{q_1},\end{aligned}$$

donc $q_1|(2\ell-1)q(0)-1$, mais $q_1|q(0)$, d'où $q_1=1$, donc Q_1/Q_2 est une homographie, ce qui est interdit.

• Cas où $q_2>0$. Dans ce cas, on voit que Y divise un et un seul des polynômes suivants : P_2, $P_2-\mu P_1$, μ parcourant l'ensemble des racines de Q_2. Ainsi, quitte à faire

éventuellement un changement de variables $v' = v - \mu$, qui transforme $P_1 - \mu P_2$ en un nouveau P_1, on peut supposer que 0 est racine de Q_2 de multiplicité $q_2(0) > 0$ et que Y divise soit P_1 soit P_2(signalons que ce changement de variables n'affecte en rien la condition $q_1 > q_2$). Pour traiter simultanément ces cas, nous introduisons un entier κ qui vaut soit 0 soit 1. Les polynômes P_1 et P_2 sont alors de la forme

$$P_1(X,Y) = \xi_1 Y^{\kappa q(0)/q_2(0)} \prod_{b\in\mathcal{B}_1} (X+b)^{q(0)/q_2(0)} \prod_{(b,\rho)\in\mathcal{A}_1} ((X+b)Y-\rho)^{q(\rho)/q_2(0)}$$

et

$$P_2(X,Y) = \xi_2 Y^{(1-\kappa)q(0)/(q_1-q_2)} \prod_{b\in\mathcal{B}_2} (X+b)^{q(0)/(q_1-q_2)} \prod_{(b,\rho)\in\mathcal{A}_2} ((X+b)Y-\rho)^{q(\rho)/(q_1-q_2)};$$

où $\mathcal{B}_1$ et $\mathcal{B}_2$ sont deux sous–ensembles disjoints de $\{b_1,\cdots,b_{2\ell}\}$, $\mathcal{A}_1$ et $\mathcal{A}_2$ sont deux sous–ensembles disjoints de $\{b_1,\cdots,b_{2\ell}\}\times\mathcal{R}$ (rappelons que tous les b_i sont distincts).

Remarquons maintenant que, pour tout $\nu \in k$, on a l'égalité suivante, valable pour certains ξ_1' et ξ_2' de k^* :

$$(P_1 - \nu P_2)(X,0) = (1-\kappa)\xi_1' \prod_{b\in\mathcal{B}_1} (X+b)^{q(0)/q_2(0)} - \nu\kappa\xi_2' \prod_{b\in\mathcal{B}_2} (X+b)^{q(0)/(q_1-q_2)}.$$

En donnant à ν la valeur λ d'une racine de Q_1, on voit que $\mathrm{NUM}(X,0)$ est divisible par $\prod_{b\in\mathcal{B}_{1+\kappa}}(X+b)$. Or, on a l'égalité

$$\mathrm{NUM}(X,0) = P(0)R(0)^{2\ell-1} \sum_{i=1}^{2\ell} \varepsilon_i \prod_{j=1;j\neq i}^{2\ell} (X+b_j)^{q(0)};$$

qui implique donc $\mathcal{B}_{1+\kappa}$ est vide. En conclusion, nous aurions, pour tout λ racine de Q_1, l'égalité $(P_1-\lambda P_2)(X,0) = (1-\kappa)\xi_1' - \lambda\kappa\xi_2'$, donc $\mathrm{NUM}(X,0) = \xi\prod_\lambda (P_1-\lambda P_2)(X,0)$ serait constant, ce qui est une contradiction, puisque ce polynôme a un terme de degré $(2\ell-1)q(0)-1$, calcul déjà rencontré plus haut.

c.2. Cas où $q(0) = 0$ et $q \geq 1$

L'idée est de se ramener au cas précédent. Puisque Q n'est pas constant, il admet au moins une racine α. Posons $P'(X) = P(X+\alpha)$, $Q'(X) = Q(X+\alpha)$ (donc $Q'(0) = 0$), et $X' = X - \alpha/Y$. La relation triviale

$$\left(\Delta_{\mathbf{b},m}\frac{P}{Q}\right)(X,Y) = \left(\Delta_{\mathbf{b},m}\frac{P'}{Q'}\right)(X',Y)$$

montre que la fraction $(\Delta_{\mathbf{b},m}\frac{P}{Q})(X,Y)$ est composée si et seulement si la fraction $(\Delta_{\mathbf{b},m}\frac{P'}{Q'})(X,Y)$ l'est. ■

c.3. Cas où $q = 0$

Le polynôme $Q(X)$ est ainsi constant, on peut même supposer $Q(X) = 1$ et $P(X)$ est un polynôme de degré p au moins 2. D'après la Proposition 2.1, nous sommes ramenés à chercher l'écriture de $(\Delta_{\mathbf{b},m}P)(X,Y)$ sous la forme $(\Delta_{\mathbf{b},m}P)(X,Y) = Q_1(P_1(X,Y))$ avec P_1 et Q_1 polynômes en une ou deux variables. Avec nos conventions, on a, pour un certain ξ, les égalités

$$\begin{aligned}(\Delta_{\mathbf{b},m}P)(X,Y) &= \textstyle\sum_{i=1}^{2\ell} \varepsilon_i P((X+b_i)Y) - mY \\ &= p(b_1 + \cdots + b_\ell - b'_1 - \cdots - b'_\ell)X^{p-1}Y^p + \cdots \\ &= \xi \textstyle\prod_\lambda (P_1(X,Y) - \lambda).\end{aligned}$$

Si on écrit $P_1(X,Y) = cX^aY^b + \cdots$, des égalités de degrés donnent $q_1 b = p$, $q_1 a = p-1$, ce qui implique $q_1 = 1$, par conséquent, le polynôme $(\Delta_{\mathbf{b},m}P)(X,Y)$ n'est pas composé. ■

d. Raffinement dans le cas où f est un polynôme

Dans cette partie, f est un polynôme unitaire à coefficients entiers, de degré au moins 3, on se propose dans ce cas particulier d'améliorer notre connaissance de l'ensemble des $\mathbf{b}$ pour lesquels $(\Delta_{\mathbf{b},m}f)(X,Y)$ est composé. On a

PROPOSITION 2.4. – *Soit $f(X)$ un polynôme unitaire de $\mathbb{Z}[X]$, de degré au moins 3 et q un nombre premier. Soit $\mathcal{E}(B,q,f)$ l'ensemble des $\mathbf{b}$ avec $0 \leq b_i, b'_i < B (1 \leq i \leq \ell)$, tels qu'il existe $m \in \mathbb{Z}$ tel que la variété, définie modulo q par l'équation*

$$(\Delta_{\mathbf{b},m}f)(X,Y) - T = 0,$$

ne soit pas une courbe absolument irréductible. Alors pour $1 \leq B \leq q$ et $\ell \geq 2$, on a la relation

$$|\mathcal{E}(B,q,f)| = O_{\deg f}(B^{2\ell-2}).$$

La Proposition 2.3 donnerait pour majoration $O(B^{2\ell-1})$.

d.1. Démonstration de la Proposition 2.4.

D'après la Proposition 2.1, la démonstration se ramène à majorer le cardinal de l'ensemble des $\mathbf{b}$ avec $0 \leq b_i, b'_i \leq B$ tels qu'il existe $m \in \mathbb{Z}$, $u \in \mathbb{F}_q[X]$, $v \in \mathbb{F}_q[X,Y]$ avec $\deg u \geq 2$ tels que

$$\big(\Delta_{\mathbf{b},m}f\big)(X,Y) = u\big(v(X,Y)\big).$$

Soit $\mathcal{F}(B,q,f)$ l'ensemble des $\mathbf{b}$, avec chaque b_i et b'_i compris entre 1 et B, tels qu'on ait

$$k(b_1 + \cdots - b'_1 \cdots) = 0 \quad \text{et} \quad \frac{k(k-1)}{2}(b_1^2 + \cdots - b_1'^2 - \cdots) = 0 (\mathrm{mod}\ q),$$

où k est le degré de f. Il est clair que l'ensemble $\mathcal{F}(B,q,f)$ est de cardinal en $O(B^{2\ell-2})$ (puisqu'on a $\ell \geq 2$ et qu'on peut supposer $q > k$). Ceci nous permet de nous restreindre à majorer le cardinal de l'ensemble

$$\mathcal{E}(B,q,f) - \mathcal{F}(B,q,f).$$

Soit $\mathbf{b} \notin \mathcal{F}(B,q,f)$. On a l'égalité $\deg_Y\big(\Delta_{\mathbf{b},m}f\big)(X,Y) = k$ dans tous les cas, et, suivant les situations

$$\deg_X\big(\Delta_{\mathbf{b},m}f\big)(X,Y) = k-1,$$

si

$$k(b_1+\cdots+b_\ell-b'_1\cdots-b'_\ell) \not\equiv 0 (\mathrm{mod}\ q) \tag{2.3}$$

ou

$$\deg_X\big(\Delta_{\mathbf{b},m}f\big)(X,Y) = k-2$$

si

$$k(b_1+\cdots+b_\ell-b'_1-\cdots-b'_\ell) = 0 \quad et \quad \frac{k(k-1)}{2}(b_1^2+\cdots+b_\ell^2-{b'_1}^2-\cdots-{b'_\ell}^2) \not\equiv 0 (\mathrm{mod}\ q). \tag{2.4}$$

Les relations de divisibilité $(\deg u)|k$ et $(\deg u)|\deg_X\big(\Delta_{\mathbf{b},m}f\big)(X,Y)$, conduisent, dans le cas de (2.3), à $\deg u = 1$ –ce qui est exclu– et, dans le cas de (2.4) à l'égalité $\deg u = 2$.

Il reste donc à traiter le cas de la condition (2.4), pour lequel nous écrivons explicitement les polynômes en cause. Puisque le degré de f est pair, on pose, en modifiant la définition de k :

$$f(X) = \sum_{i=0}^{2k} f_i X^i,$$

$$u(X) = u_2X^2 + u_1X + u_0,$$

$$v(X,Y) = \sum_{i=0}^{k} P_i(X)Y^i,$$

avec f_{2k} et u_2 non divisibles par q. L'égalité $f = u\circ v$ implique, en égalant les coefficients de Y^{2k}, la relation

$$f_{2k}\big\{(X+b_1)^{2k}+\cdots+(X+b_\ell)^{2k}-(X+b'_1)^{2k}-\cdots-(X+b'_\ell)^{2k}\big\} = u_2P_k^2(X). \tag{2.5}$$

On affaiblit la relation (2.5) en constatant qu'elle entraîne la nullité, modulo q, du discriminant du polynôme

$$(X+b_1)^{2k}+\cdots+(X+b_\ell)^{2k}-(X+b'_1)^{2k}-\cdots-(X+b'_\ell)^{2k},$$

qui est de degré au moins 2, d'après (2.4) et les hypothèses sur le degré de f. Ce discriminant est un polynôme $D_k(\mathbf{b})$, à coefficients entiers, à 2ℓ variables. En opérant, dans D_k, la substitution $b'_\ell = b_1+b_2\cdots+b_\ell-b'_1-\cdots-b'_{\ell-1}$, on obtient un poynôme D_k^* en $2\ell-1$ variables. Montrons d'abord le

LEMME 2.5. – *Le polynôme à coefficients entiers D_k^* n'est pas formellement nul.*

d.2. Démonstration du Lemme 2.5

Raisonnons par l'absurde. Si D^* était formellement nul, cela entraînerait, en choisissant $\mathbf{b} = (1, -1, 0, \ldots, 0)$, que le polynôme

$$Q_k(X) = (X+1)^{2k} + (X-1)^{2k} - 2X^{2k}$$

aurait une racine double notée ξ qui serait ainsi, aussi racine de

$$Q'_k(X) = (2k)\big((X+1)^{2k-1} + (X-1)^{2k-1} - 2X^{2k-1}\big).$$

Pour q assez grand, on aurait donc $2\xi^{2k-1} = (\xi+1)^{2k-1} + (\xi-1)^{2k-1}$, d'où en reportant dans $Q_k(\xi)$, on obtient l'égalité $(\xi-1)^{2k-1} = (\xi+1)^{2k-1}$. On a donc $\xi = (1+\lambda)/(1-\lambda)$, où λ est une racine $(2k-1)$–ième de l'unité, différente de 1. En reportant dans la relation $Q_k(\xi) = 0$, on a

$$2^{2k} + (2\lambda)^{2k} - 2(1+\lambda)^{2k} = 2(1+\lambda)\{2^{2k-1} - (1+\lambda)^{2k-1}\} = 0.$$

Ainsi λ vérifierait simultanément $\lambda^{2k-1} - 1 = 0$ et $(1+\lambda)^{2k-1} - 2^{2k-1} = 0$. Ces deux équations ont pour seule racine commune $\lambda = 1$, d'où la contradiction. ■

Pour terminer, il reste à majorer le cardinal des $\mathbf{b}$ vérifiant (2.4) et (2.5). Un tel $\mathbf{b}$ est donc tel que $D_k^*(b_1, \cdots, b_\ell, b'_1, \cdots, b'_{\ell-1}) = 0 (\mathrm{mod}\ q)$. Pour q assez grand, D_k^* n'est pas formellement nul d'après le Lemme 2.5, et a donc $O(B^{2\ell-2})$ racines de taille inférieure à B, ce qui termine la preuve de la Proposition 2.4. ■

III. Indépendance de faisceaux

L'objet de ce paragraphe est d'étudier le comportement de la somme

$$S_k(x, m; q) := \sum_{\substack{y \in \mathbb{F}_q \\ y^k \neq \infty}} \psi(xy^k + my),$$

pour k entier différent de 0, 1 et 2 et m entier. Nous montrerons le

THÉORÈME 3.1. – *Soit k un entier différent de 0, 1 et 2, ψ un caractère additif non trivial de $(\mathbb{F}_q, +)$, $r(X)$ une fraction rationnelle non constante de $\mathbb{Z}(X)$ vérifiant la condition*

$$r(X) \text{ n'est pas de la forme } r(X) = c\big(s(X)\big)^d (\mathrm{mod}\ q),$$

(3.∗) *avec $c \in \mathbb{F}_q$, $d | (k, q-1)$, $d > 1$ et $s(X) \in \mathbb{F}_q(X)$.*

On a les égalités

$$\sum_{\substack{x \in \mathbb{F}_q \\ r(x) \neq 0, \infty}} S_k(r(x), m; q) = O(q) \quad \text{pour} \quad m \in \mathbb{Z}, \tag{3.1}$$

(3.2)
$$\sum_{\substack{x\in\mathbf{F}_q\\ r(x)\neq 0,\infty}} S_k(r(x),m_1;q)\overline{S_k(r(x),m_2;q)} = q^2 + O(q^{\frac{3}{2}}) \quad \text{pour} \quad m_1^k = m_2^k \neq 0(\mathrm{mod}\ q),$$

(3.3)
$$\sum_{\substack{x\in\mathbf{F}_q\\ r(x)\neq 0,\infty}} |S_k(r(x),0;q)|^2 = \big((k,q-1)-1\big)q^2 + O(q^{\frac{3}{2}})$$

et

(3.4)
$$\sum_{\substack{x\in\mathbf{F}_q\\ r(x)\neq 0,\infty}} S_k(r(x),m_1;q)\overline{S_k(r(x),m_2;q)} = O(q^{3/2}) \quad \text{pour} \quad m_1^k \neq m_2^k(\mathrm{mod}\ q).$$

En outre, les constantes impliquées par les O dépendent au plus de k et du degré du numérateur et du dénominateur de $r(X)$.

(En fait, l'hypothèse (3.$*$) n'est utilisée que pour (3.3) et pour (3.1) lorsque $m = 0$). Remarquons que si $m_1^k = m_2^k(\mathrm{mod}\ q)$, les sommes $S_k(r(x),m_1;q)$ et $S_k(r(x),m_2;q)$ sont égales ; la relation (3.2) couplée à la majoration de Weil : $S_k(r(x),m_1;q) = O(q^{1/2})$, entraînent que la somme en question vaut en moyenne $q^{1/2}$. En revanche, la relation (3.4)–qui envisage le cas d'une somme en trois variables– s'interprète comme une relation d'orthogonalité approchée. En d'autres termes, quand x varie dans $\mathbb{F}_q$, les fonctions $S_k(r(x),m_1;q)$ et $S_k(r(x),m_2;q)$ sont relativement indépendantes l'une de l'autre : ceci est conséquence d'un résultat d'indépendance de deux faisceaux ℓ–adiques, d'où le titre de ce paragraphe. Des résultats de même nature sont déjà apparus dans la littérature. Citons ([Fr–I] Appendix Theorem 1), où est traité le cas de

$$\sum_{\substack{x\in\mathbf{F}_q\\ x\neq 0,\ 1}} S_{-1}(r_1(x),m_1;q)S_{-1}(r_2(x),m_2;q),$$

avec $r_1(x) = 1/x$ et $r_2(x) = 1/(1-x)$ et aussi ([Fo–I] Appendix Theorem 1) où est étudiée de la somme

$$\sum_{\substack{x\in\mathbf{F}_q\\ x\neq 0,\ 1,\beta/\alpha}} S_{-1}(r_1(x),1;q)S_{-1}(r_2(x),1;q)S_{-1}(r_3(x),1;q)S_{-1}(r_4(x),1;q),$$

avec $r_1(x) = \alpha(x-1)^2$, $r_2(x) = (x-1)(\alpha x - \beta)$, $r_3(x) = \beta(1/x-1)^2$ et $r_4(x) = (1/x-1)(\beta/x-\alpha)$ avec $\alpha\beta(\alpha-\beta) \neq 0(\mathrm{mod}\ q)$. Il faut constater que dans les deux exemples précédents les fonctions rationnelles r_i sont notablement distinctes (elles n'ont pas les mêmes singularités), notre cas est donc plus délicat à traiter car les sommes paraissent *plus proches.*

La preuve du Théorème 3.1 est une étude précise de la famille à un paramètre x, de sommes d'exponentielles $S_k(x,m;q)$. Pour ce faire nous utilisons la théorie quasi–exhaustive développée dans ([Ka2] Chap. 7), où des analogues de ces sommes sont traités avec grand soin.

a. Étude des sommes $S_k(x,m;q)$ pour $m \neq 0$

Pour $n \in \mathbb{Z}^*$, on notera $[n]$ le morphisme de $\mathbb{A}^1_{\mathbb{F}_q}$ sur lui–même défini par $x \to x^n$. Pour $n \in \mathbb{N}^*$, on notera ψ_{q^n} le caractère de $(\mathbb{F}_{q^n},+)$ obtenu par composition de $\psi_q = \psi$ avec $tr_{\mathbb{F}_{q^n}/\mathbb{F}_q}$.

Enfin, partant d'un caractère additif (*resp.* multiplicatif) non trivial ψ(*resp.* χ) de $(\mathbb{F}_q,+)$ (*resp.* $(\mathbb{F}_q^*,\times)$), on note $\mathcal{L}_\psi$ (*resp.* $\mathcal{L}_\chi$) le $\mathbb{Q}_\ell$–faisceau de rang 1, lisse sur $\mathbb{A}^1_{\mathbb{F}_q}$ (*resp.* $\mathbb{G}_{m,\mathbb{F}_q}$) qui lui est associé ([Ka1] Chap.2).

a.1. Le cas $k > 2$

Pour $m \neq 0$, Katz a construit, grâce à l'aide de la transformée de Fourier–Deligne–Laumon, un $\mathbb{Q}_\ell$–faisceau $\mathcal{G}_m$, lisse sur $\mathbb{G}_{m,\mathbb{F}_q}$, qui vérifie, pour $x \in \mathbb{F}^*_{q^n}/\mathbb{F}^*_{q^{n-1}}$, l'égalité (qui en fait le caractérise à isomorphisme près) :

$$tr(\mathrm{Frob}_x, \mathcal{G}_m) = \sum_{\substack{y \in \mathbb{F}_{q^n} \\ y^k \neq \infty}} \psi_{q^n}(xy^k + my) := S_k(x,m;q^n).$$

Ce faisceau a les propriétés suivantes ([Ka2] 7.7, 7.12, 7.13) : $\mathcal{G}_m$ est lisse sur $\mathbb{G}_{m,\mathbb{F}_q}$, de rang $k-1$, pur de poids 1, modérément ramifié en ∞, sauvage en 0 avec $\mathrm{Swan}_0(\mathcal{G}_m) = 1$ (donc avec $1/(k-1)$ pour seule pente en 0), enfin si q ne divise pas un certain entier non nul Q_k, le théorème général 7.7.6 de [Ka2] donne les diverses possibilités pour la composante neutre du groupe de monodromie géométrique de $\mathcal{G}_m$, notée $\mathrm{G}^0_{\mathrm{geom}}(\mathcal{G}_m)$.

Dans ce cas particulier, on peut être plus précis : on remarque que le *pull-back* $[-(k-1)]^*\mathcal{G}_m$ est isomorphe au $\mathbb{Q}_\ell$–faisceau $\mathcal{G}'_m$ construit en ([Ka2]7.10.5) en considérant $f(y) = y^k - my$ qui est une *supermorse function* au sens de 7.10. Cet isomorphisme peut être prouvé formellement et plus simplement en notant que les deux faisceaux ont les mêmes traces de frobenius : pour tout $x \in \mathbb{F}^*_{q^n}/\mathbb{F}^*_{q^{n-1}}$, on a

$$tr(\mathrm{Frob}_x,\ [-(k-1)]^*\mathcal{G}_m) = S_k(x^{1-k},m;\ q^n) = \sum_{y \in \mathbb{F}_{q^n}} \psi_{q^n}(x(y^k - my)) = tr(\mathrm{Frob}_x, \mathcal{G}'_m).$$

D'après ([Ka2] Theorem 7.10.5), pour q ne divisant pas Q_k, on a l'égalité

$$\begin{aligned} \mathrm{G}^0_{\mathrm{geom}}(\mathcal{G}'_m) &= Sp_{k-1}(\mathbb{Q}_\ell) \quad \text{si } k \text{ est impair} \\ &= \pm Sl_{k-1}(\mathbb{Q}_\ell) \quad \text{si } k \text{ est pair.} \end{aligned}$$

Le point fondamental dans la preuve du Théorème 3.1 est la

PROPOSITION 3.2. – *Pour tout k entier au moins égal à 2, il existe un entier non nul Q_k tel que, si q ne divise pas Q_k et si $m_1^k \neq m_2^k$, on a les égalités*

$$\begin{aligned} \mathrm{G}^0_{\mathrm{geom}}(\mathcal{G}_{m_1} \oplus \mathcal{G}_{m_2}) &= \mathrm{G}^0_{\mathrm{geom}}(\mathcal{G}_{m_1}) \times \mathrm{G}^0_{\mathrm{geom}}(\mathcal{G}_{m_2}) \\ &= Sp_{k-1} \times Sp_{k-1}(\mathbb{Q}_\ell) \qquad \textit{si } k \textit{ est impair,} \\ &= Sl_{k-1} \times Sl_{k-1}(\mathbb{Q}_\ell) \qquad \textit{si } k \textit{ est pair.} \end{aligned}$$

On voit donc que la composante neutre du groupe de monodromie géométrique de la somme des deux faisceaux $\mathcal{G}_{m_1}$ et $\mathcal{G}_{m_2}$ est aussi grosse que possible (*i.e.* le produit des composantes neutres de chacun des deux groupes de monodromie géométrique) ; c'est en ce sens qu'on peut parler de faisceaux indépendants (ou plutôt Lie–indépendants).

Preuve. – C'est une conséquence du critère de Goursat–Kolchin–Ribet ([Ka2]), critère qui a déjà été appliqué en d'autres lieux ([Fo–I] par exemple). Mais dans notre cas, les faisceaux $\mathcal{G}_{m_1}$ et $\mathcal{G}_{m_2}$, ne se distinguent géométriquement que par la structure précise de leur monodromie locale en 0, structure qui est élucidée par Katz grâce au théorème de la *phase stationnaire* de Laumon. Les arguments présentés ici ont déjà été utilisés dans ([Mi] Chap 2).

Partons d'un isomorphisme géométrique

$$\mathcal{G}_{m_1} \otimes \mathcal{L} \simeq \mathcal{G}_{m_2};$$

il se restreint aux représentations du groupe d'inertie sauvage en 0 noté P_0; on a donc un isomorphisme de P_0–modules

$$\mathcal{G}_{m_1|P_0} \otimes \mathcal{L}_{|P_0} \simeq \mathcal{G}_{m_2|P_0};$$

or $\mathcal{L}$ est de rang 1 et les pentes de $\mathcal{G}_{m|P_0}$ sont < 1, par conséquent, $\mathcal{L}$ est modéré en 0 et on a l'isomorphisme

$$\mathcal{G}_{m_1|P_0} \simeq \mathcal{G}_{m_2|P_0}.$$

En prenant le *pull–back* par $[-(k-1)]$, on a un isomorphisme de P_∞–modules :

$$\mathcal{G}'_{m_1|P_\infty} \simeq \mathcal{G}'_{m_2|P_\infty}. \tag{3.5}$$

La monodromie locale à l'infini de $\mathcal{G}'$ a été calculée explicitement par Katz ([Ka2] Theorem 7.9.4) : on a l'égalité

$$\mathcal{G}'_{m|P_\infty} = \bigoplus_{s\in\mathcal{S}} \mathcal{L}_{\psi_q}(sx),$$

où s parcourt l'ensemble $\mathcal{S}$ des valeurs critiques de $f(y) = y^k - my$. En faisant le choix dans $\overline{\mathbb{F}_q}$ d'une racine $(k-1)$–ième de m/k, on a $\mathcal{S} = (1-k)(\frac{m}{k})^{k/(k-1)}\mathcal{M}_{k-1}$ (où $\mathcal{M}_{k-1}$ désigne l'ensemble des racines $(k-1)$–ièmes de 1 dans $\overline{\mathbb{F}_q}$) et l'isomorphisme (3.5) implique que $m_1^k = m_2^k$.

Il reste à traiter le cas d'un isomorphisme $\mathcal{G}_{m_1} \otimes \mathcal{L} \simeq \mathcal{G}_{m_2}^\vee$: si k est impair $\mathcal{G}_{m_2}$ est isomorphe à son dual et par la discussion précédente, on a $m_1^k = m_2^k$; si k est impair, l'isomorphisme de P_∞–modules

$$\bigoplus_{\xi^{k-1}=1} \mathcal{L}_{\psi_q(sx)} \simeq \bigoplus_{\xi'^{k-1}=1} \mathcal{L}_{\psi_q(s'x)},$$

(avec $s = (1-k)(\frac{m_1}{k})^{k/(k-1)}\xi$ et $s' = -(1-k)(\frac{m_2}{k})^{k/(k-1)}\xi'$) implique encore l'égalité $m_1^k = m_2^k$.

Soit $r(X)$ une fraction rationnelle non constante de $\mathbb{F}_q(X)$, on note encore r le morphisme fini de $\mathbb{P}^1_{\mathbb{F}_q}$ correspondant. On forme alors les faisceaux $r^*\mathcal{G}_m$ qui sont lisses sur l'ouvert U, complémentaire dans $\mathbb{P}^1_{\mathbb{F}_q}$ de l'ensemble des zéros et des pôles de $r(X)$. Comme il a déjà été dit, le *pull–back* d'un faisceau par un morphisme fini ne modifie pas la composante neutre du groupe de monodromie géométrique, la Proposition 3.2 admet le corollaire suivant

COROLLAIRE 3.3. – *Soit $r(X)$ une fraction rationnelle non constante de $\mathbb{F}_q(X)$. Pour $k > 1$, pour q ne divisant pas Q_k et pour $m_1^k \neq m_2^k$ on a les égalités*

$$\begin{aligned} \mathrm{G}^0_{\mathrm{geom}}(r^*\mathcal{G}_{m_1} \oplus r^*\mathcal{G}_{m_2}) &= Sp_{k-1} \times Sp_{k-1}(\mathbb{Q}_\ell) \quad \textit{si } k \textit{ est impair,} \\ &= Sl_{k-1} \times Sl_{k-1}(\mathbb{Q}_\ell) \quad \textit{si } k \textit{ est pair.} \end{aligned}$$

a.2. Le cas $k < 0$

Indiquons les modifications à apporter dans ce cas : on construit de la même façon les faisceaux $\mathcal{G}_m$ qui correspondent aux sommes $S_k(x, m; q)$ qui sont lisses sur $\mathbb{G}_m$, de rang $-(k-1)$, modérés en ∞, sauvages en 0, de conducteur de Swan 1 (donc de pente $-1/(k-1)$ en 0). D'après ([Ka2] Theorem 7.12.3.1), si q ne divise pas Q_k, la composante neutre du *pull–back* $[-k]^*\mathcal{G}_m$ vaut $Sp_{|k-1|}(\mathbb{Q}_\ell)$ ou $Sl_{|k-1|}(\mathbb{Q}_\ell)$ suivant la parité de k.

On vérifie ensuite que si $m_1^k \neq m_2^k$, les faisceaux $\mathcal{G}_{m_1}$ et $\mathcal{G}_{m_2}$ satisfont au critère de Goursat–Kolchin–Ribet en considérant encore les *pull–back* $[-(k-1)]^*\mathcal{G}_{m_i}$ et en notant que la fonction $f(y) = y^k - my$ est une *super–morse function*. La théorie développée en ([Ka2] 7.9 et 7.10) permet alors de conclure. On a donc en toute généralité la

PROPOSITION 3.4. – *Soit $k \in \mathbb{Z} - \{0, 1, 2\}$. Alors, il existe un entier positif Q_k tel que si q ne divise pas Q_k et si $m_1^k \neq m_2^k$, on a l'égalité*

$$\begin{aligned} \mathrm{G}^0_{\mathrm{geom}}(r^*\mathcal{G}_{m_1} \oplus r^*\mathcal{G}_{m_2}) &= Sp_{|k-1|} \times Sp_{|k-1|}(\mathbb{Q}_\ell) \quad \textit{si } k \textit{ est impair,} \\ &= Sl_{|k-1|} \times Sl_{|k-1|}(\mathbb{Q}_\ell) \quad \textit{si } k \textit{ est pair,} \end{aligned}$$

pour toute fraction rationnelle $r(X)$ non constante de $\mathbb{F}_q(X)$.

b. Étude des sommes $S_k(x, m; q)$ pour $m = 0$

Si $m = 0$, les sommes à étudier sont beaucoup plus simples puisque ce sont des sommes de Gauss

$$S_k(x, 0; q) = \sum_{\substack{y \in \mathbb{F}_q \\ y^k \neq \infty}} \psi_q(xy^k) = \sum_{\substack{y \in \mathbb{F}_q \\ y^k \neq \infty}} \psi_q(xy^{k'}),$$

avec $k' = (k, q-1)$, de sorte qu'on a les égalités (pour x non divisible par q) :

– Si $k' = 1$, on a $S_k(x, 0; q) = 0$ ou -1 suivant que k est positif ou négatif

– Si $k' > 1$, on a

$$(3.6)\qquad \begin{aligned} S_k(x,0;q) &= \sum_{\chi^{k'}=\chi_0} \overline{\chi}(x) G_{\chi,\psi_q} + 1 \quad \text{si } k>0, \\ &= \sum_{\chi^{k'}=\chi_0} \overline{\chi}(x) G_{\chi,\psi_q} \quad \text{si } k<0, \end{aligned}$$

avec χ_0 caractère trivial et G_{χ,ψ_q} désigne la somme de Gauss correspondante : $G_{\chi,\psi_q} = \sum_{t\in\mathbb{F}_q} \chi(t)\psi_q(t)$.

c. Preuve du Théorème 3.1

Commençons par le cas $m_1^k \neq m_2^k$, $m_1 m_2 \neq 0$. La formule de Grothendieck–Lefschetz donne l'égalité

$$\begin{aligned} \Sigma_k(m_1,m_2;q) &:= \sum_{\substack{x\in\mathbb{F}_q \\ r(x)\neq 0,\infty}} S_k(r(x),m_1;q)\overline{S_k(r(x),m_2;q)} \\ &= \sum_{\substack{x\in\mathbb{F}_q \\ r(x)\neq 0,\infty}} tr(\mathrm{Frob}_x, r^*\mathcal{G}_{m_1}\otimes r^*\mathcal{G}_{m_2}^\vee) \\ &= \sum_{i=0}^{2}(-1)^i tr(\mathrm{Frob}_q, H_c^i(U\otimes\overline{\mathbb{F}}_q, r^*\mathcal{G}_{m_1}\otimes r^*\mathcal{G}_{m_2}^\vee)). \end{aligned}$$

Le premier groupe de cohomologie $H_c^0(\cdots)$ est nul car U est affine. Si $m_1^k \neq m_2^k$, la Proposition 3.4 implique que la représentation du groupe fondamental géométrique de $U\otimes\overline{\mathbb{F}}_q$ associée au faisceau $r^*\mathcal{G}_{m_1}\otimes r^*\mathcal{G}_{m_2}^\vee$ est irréductible, donc $H_c^2(\cdots)=0$ (puisque H_c^2 s'identifie aux coinvariants du faisceau sous l'action du groupe fondamental géométrique de U). Ensuite par le théorème fondamental de Deligne, le $\mathbb{Q}_\ell$–vectoriel $H_c^1(U\otimes\overline{\mathbb{F}}_q, r^*\mathcal{G}_{m_1}\otimes r^*\mathcal{G}_{m_2}^\vee)$ est mixte de poids ≤ 3 et a pour dimension la valeur absolue de la caractéristique d'Euler–Poincaré du faisceau : on a donc la majoration

$$|\Sigma_k(m_1,m_2;q)| \leq |\chi_c(U\otimes\overline{\mathbb{F}}_q, r^*\mathcal{G}_{m_1}\otimes r^*\mathcal{G}_{m_2}^\vee)| q^{3/2}.$$

Enfin, la formule de Grothendieck–Ogg–Shafarevitch ([Ka1]2.3.1) et une majoration facile des conducteurs de Swan permettent de majorer la caractéristique d'Euler–Poincaré $\chi_c(\cdots)$ en fonction de k et des ordres des zéros et des pôles de $r(X)$ (premiers à q par hypothèse) : on a les majorations ([Ka1] 1.14)

$$\mathrm{Swan}_{x_0} r^*\mathcal{G}_{m_1}\otimes r^*\mathcal{G}_{m_2}^\vee \leq \mathrm{ord}_{x=x_0}(r(x))|k-1|^2/|k-1|, \text{ si } x_0 \text{ est un zéro de } r(x)$$

et

$$\mathrm{Swan}_{x_\infty} r^*\mathcal{G}_{m_1}\otimes r^*\mathcal{G}_{m_2}^\vee = 0, \text{ si } x_\infty \text{ est un pôle de } r(x),$$

ce qui donne donc (3.4) dans le cas où $m_1 m_2 \neq 0 (\mathrm{mod}\ q)$.

Maintenant, si $m_1 \neq 0$ et $m_2 = 0$, la majoration de $\Sigma_k(m_1, m_2; q)$ est beaucoup plus facile, en effet

– si $k' = (k, q-1) = 1$, on a

$$\Sigma_k(m_1, 0; q) = 0 \qquad \text{si } k > 0$$

$$\Sigma_k(m_1, 0; q) = \Big| \sum_{\substack{x \in \mathbf{F}_q \\ r(x) \neq 0, \infty}} S_k(r(x), m_1; q) \Big| \leq |\chi_c(U \otimes \overline{\mathbb{F}}_q, r^* \mathcal{G}_{m_1})| q, \qquad \text{si } k < 0$$

– si $k' > 1$, on doit majorer k' sommes de la forme

$$\overline{G_{\chi, \psi_q}} \sum_{\substack{x \in \mathbf{F}_q \\ r(x) \neq 0, \infty}} \chi(r(x)) S_k(r(x), m_1; q),$$

et étudier le faisceau $r^* \mathcal{L}_\chi \otimes r^* \mathcal{G}_{m_1}$; or $r^* \mathcal{G}_{m_1}$ est géométriquement irréductible et $r^* \mathcal{L}_\chi$ est de rang 1 : le faisceau $r^* \mathcal{L}_\chi \otimes r^* \mathcal{G}_{m_1}$ reste donc géométriquement irréductible, on a alors la majoration

$$\sum_{\substack{x \in \mathbf{F}_q \\ r(x) \neq 0, \infty}} \chi(r(x)) S_k(r(x), m_1; q) = O(q),$$

La formule précédente, pour $\chi = \chi_0$, permet de majorer la contribution à $\Sigma_k(m_1, 0; q)$ du terme constant 1 de (3.6) par $O(q)$. Les majorations (3.1) et (3.4) pour $m_2 = 0$ en résultent, notons que le cas où $m = 0$ dans (3.1) requiert l'hypothèse (3.*).

Il reste donc le cas $m_1^k = m_2^k$. Pour $m_1 \neq 0$ modulo q, on étudie ici la somme associée au faisceau pur de poids 0 : $r^* \mathcal{G}_{m_1} \otimes r^* \mathcal{G}_{m_1}^\vee = \mathrm{End}(r^* \mathcal{G}_{m_1})$. Comme le faisceau $r^* \mathcal{G}_{m_1}$ est géométriquement irréductible, on a l'égalité

$$H_c^2(U \otimes \overline{\mathbb{F}}_q, \mathrm{End}(r^* \mathcal{G}_{m_1})) = \mathbb{Q}_\ell(-1).$$

D'autre part, $H_c^0(\cdots)$ est nul, $H_c^1(\cdots)$ est mixte de poids ≤ 1 et sa dimension est contrôlée comme précédemment, on obtient donc l'égalité

$$\sum_{\substack{x \in \mathbf{F}_q \\ r(x) \neq 0, \infty}} \frac{|S_k(r(x), m_1; q)|^2}{q} = q + O(q^{1/2})$$

ce qui donne l'égalité (3.2).

Pour (3.3), on passe par les sommes de Gauss. En supposant $k > 1$ par exemple et en mettant à part les cas où $y_1 = 0$ et $y_2 = 0$, on a les égalités

$$\sum_{\substack{x\in\mathbb{F}_q\\ r(x)\neq 0,\infty}} |S_k(r(x),0;q)|^2 = \sum_{\substack{x\in\mathbb{F}_q\\ r(x)\neq 0,\infty}} \sum_{y_1}\sum_{y_2} \psi_q\big((y_1^k - y_2^k)r(x)\big) =$$

$$\sum_{\substack{\chi^k=\chi_0\\ \chi'^k=\chi_0}} \sum_{t,t'\in\mathbb{F}_q} \chi(t)\chi(t') \sum_{\substack{x\in\mathbb{F}_q\\ r(x)\neq 0,\infty}} \psi_q\big((t-t')r(x)\big) + \sum_{\substack{x\in\mathbb{F}_q\\ r(x)\neq 0,\infty}} \Big\{S_k(r(x),0;q)+S_k(-r(x),0;q)-1\Big\}$$

$$= \sum_{\chi^k=\chi_0}\sum_{\chi'^k=\chi_0} G_{\chi,\psi_q} G_{\chi',\overline{\psi_q}} \sum_{\substack{x\in\mathbb{F}_q\\ r(x)\neq 0,\infty}} \overline{\chi\chi'}(r(x)) + O(q^{\frac{3}{2}}).$$

Dans la somme précédente, le caractère $\overline{\chi\chi'}$ a pour ordre un diviseur d de k et $q-1$.

–Si $d = 1$, on somme trivialement. Puisqu'il y a exactement $(k, q-1) - 1$ couples de caractères (χ, χ'), tels que $\chi^k = \chi'^k = \chi_0$, $\overline{\chi\chi'}$ d'ordre 1, $\chi \neq \chi_0$, on voit que la contribution des (χ, χ') tels que $d = 1$ est

$$\big((k, q-1) - 1\big)q^2 + O(q);$$

d'où le terme principal de (3.3).

–Si $d > 1$, grâce à l'hypothèse $(3.*)$, on peut appliquer ([Schm] Theorem 2C', page 43), sur les sommes de caractères :

LEMME 3.5. – *Soit χ un caractère multiplicatif sur $\mathbb{F}_q$, d'ordre $d > 1$, et soit $r(X)$ une fraction rationnelle de $\mathbb{F}_q(X)$ qui n'est pas de la forme $r(X) = c\big(s(X)\big)^d$ avec $c \in \mathbb{F}_q$ et $s(X) \in \mathbb{F}_q(X)$. Il existe alors une constante C dépendant au plus des degrés du numérateur et du dénominateur de $r(X)$, tel qu'on ait la majoration*

$$\Big|\sum_{\substack{x\in\mathbb{F}_q\\ r(x)\neq 0,\infty}} \chi\big(r(x)\big)\Big| \leq Cq^{\frac{1}{2}}.$$

En fait, Schmidt n'énonce ce résultat que pour $r(X)$ polynôme, la généralisation à une fraction rationnelle est aisée. Dans notre situation, on a donc la relation

$$\sum_{\substack{x\in\mathbb{F}_q\\ r(x)\neq 0,\infty}} \overline{\chi\chi'}(r(x)) = O(q^{\frac{1}{2}}),$$

ce qui termine la preuve de (3.3). ■

IV. Démonstration de la proposition 1.2.

Dans cette partie f désigne une fraction rationnelle vérifiant (†). Nous avons calqué notre démarche sur celle de Friedlander et Iwaniec ([Fr–I1]Theorem 3), nous nous intéressons donc à la somme

$$S_I(f,q;M,N)=\sum_{m\le M}\alpha_m\sum_{n\in\mathcal{I}}\psi(f(mn)),$$

où $\mathcal{I}$ est un intervalle contenant N entiers exactement.

Pour éviter un raisonnement par récurrence, nous incorporons un artifice de présentation apparu dans ([Fr–I2]), basé sur des techniques de Fourier. Si $\mathcal{I}=[u,u']$ (u et u' entiers), on note g la fonction trapèze qui vaut 1 sur $[u,u']$, 0 sur $]-\infty,u-1]$ et $[u'+1,\infty[$ et est continue et linéaire sur $[u-1,u]$ et $[u',u'+1]$. Sa transformée de Fourier $\hat{g}(y)=\int_{-\infty}^{\infty}g(t)e(-yt)\,dt$ vérifie

$$\hat{g}(y)=O\big(\min(N,|y|^{-1},|y|^{-2})\big). \tag{4.1}$$

Soit v un entier positif quelconque. Par translation par v, on a, pour tout entier m, l'égalité

$$\sum_{n\in\mathcal{I}}\psi(f(mn))=\sum_{n}\psi(f(mn))g(n)=\sum_{n}\psi\big(f(m(n+v))\big)g(n+v), \tag{4.2}$$

puis, on choisit v de la forme particulière $v=ab$ avec

$$A/2\le a\le A,\quad B/2\le b\le B,$$

où A et B sont des paramètres vérifiant les contraintes

$$AB\le N\quad\text{et}\quad AM<q.$$

Comme il est signalé dans [Fr–I1], cette idée de translation par un nombre de la forme ab, se trouve déjà chez Vinogradov, Karatsuba ou Burgess.

Sommant maintenant (4.2) sur tous les v vérifiant les conditions précédentes et en notant V le cardinal de l'ensemble de tels v, on parvient aux inégalités

$$\begin{aligned}(4.3)\quad V|S_{\mathrm{I}}(f,q;M,N)| &\le \sum_{A/2\le a\le A}\sum_{m\le M}\sum_{n}\Big|\sum_{B/2\le b\le B}\psi\big(f(am(\bar{a}n+b))\big)g(n+ab)\Big|\\ &\le \sum_{A/2\le a\le A}\frac{1}{a}\sum_{m\le M}\sum_{n\in\mathcal{I}'}\Big|\sum_{B/2\le b\le B}\psi\big(f(am(\bar{a}n+b))\big)\\ &\quad\times\int_{-\infty}^{\infty}\hat{g}\Big(\frac{t}{a}\Big)e\Big(-\frac{nt}{a}\Big)e\Big(-bt\Big)\,dt\Big|\\ &\le \sum_{A/2\le a\le A}\frac{1}{a}\sum_{m\le M}\sum_{n\in\mathcal{I}'}\int_{-\infty}^{\infty}\Big|\hat{g}\Big(\frac{t}{a}\Big)\Big|\Big|\sum_{B/2\le b\le B}\psi\big(f(am(\bar{a}n+b))\big)e(-bt)\Big|\,dt,\end{aligned}$$

avec $\mathcal{I}'$ un nouvel intervalle ayant $2N$ éléments et $\bar{a}$ inverse de a modulo q. Mais (4.1) implique la relation

$$\frac{1}{a}\int_{-\infty}^{\infty} |\hat{g}(\frac{t}{a})|\, dt = \int_{-\infty}^{\infty} |\hat{g}(t)|\, dt = O(\log q),$$

ainsi, grâce à (4.3), on voit qu'on a, pour un certain t réel, la relation

(4.4)
$$\begin{aligned} VS_{\mathrm{I}}(f,q;M,N) &\ll \log q\Big(\sum_{A/2\le a\le A}\sum_{m\le M}\sum_{n\in\mathcal{I}'}\Big|\sum_{B/2\le b\le B}\psi\big(f(am(\bar{a}n+b))\big)e(-bt)\Big|\Big) \\ &\ll (\log q)\Sigma_t(A,B;M,N), \end{aligned}$$

par définition.

a. Transformation de $\Sigma_t(A,B;M,N)$.

Dans la définition de Σ_t, posons $r=\bar{a}n$, $s=am$ et désignons par $\nu(r,s)$ le nombre de solutions au système $r=\bar{a}n(\mathrm{mod}\ q)$ et $s=\ am$, où les inconnues vérifient $A/2\le a\le A$, $1\le m\le M$ et $n\in\mathcal{I}'$. Remarquons que la variable s vérifie maintenant l'inégalité $1\le s\le AM$ et qu'on a la majoration

$$\sum_r\sum_s \nu^2(r,s) \ll_\varepsilon AMNq^\varepsilon. \tag{4.5}$$

Par application de l'inégalité de Hölder avec l'exposant 2ℓ avec ℓ entier au moins égal à 2, on a

$$\begin{aligned} \Sigma_t &= \sum_r\sum_s \nu(r,s)\Big|\sum_b \psi\big(f(s(r+b))\big)e(-bt)\Big| \\ &\le \Big\{\sum_r\sum_s \nu^2(r,s)\Big\}^{1-\frac{1}{2\ell}}\Big\{\sum_r\sum_s\Big|\sum_b\Big|^{2\ell}\Big\}^{\frac{1}{2\ell}}, \end{aligned}$$

soit encore, en utilisant (4.5),

(4.6)
$$\Sigma_t \ll_\varepsilon q^\varepsilon (AMN)^{1-\frac{1}{2\ell}}\Big\{\sum_{\mathbf{b}\in\mathcal{B}}\Big|\sum_{r(\mathrm{mod}\ q)}\sum_{s\le AM}\psi\big((\Delta_{\mathbf{b}}f)(r,s)\big)\Big|\Big\}^{\frac{1}{2\ell}} := q^\varepsilon (AMN)^{1-\frac{1}{2\ell}}\Xi^{\frac{1}{2\ell}}$$

où $\mathcal{B}$ est l'ensemble des 2ℓ –uplets d'entiers $\mathbf{b}=(b_1,\cdots,b_\ell,b'_1,\cdots,b'_\ell)=(b_1,\cdots,b_{2\ell})$ compris entre 0 et B et $\Delta_{\mathbf{b}}$ est l'opérateur de décalage défini au paragraphe II.

L'ensemble $\mathcal{B}$ possède deux sous–ensembles intéressants :

• $\mathcal{A}(B,q,f)$ qui contient la plupart des $\mathbf{b}$ tels que pour tout $m\in\mathbb{Z}$, la variété définie par $\big(\Delta_{\mathbf{b},m}f\big)(X,Y)-T=0$ soit irréductible sur $\overline{\mathbb{F}_q(T)}$. La définition de $\mathcal{A}(B,q,f)$ dépendra de la nature de f.

• $\mathcal{D}(B)$ qui est l'ensemble des éléments *diagonaux* c'est–à–dire les $\mathbf{b}$ tels qu'il existe une permutation σ de $\{1,\cdots,\ell\}$ avec $b'_i=b_{\sigma(i)}$, l'opérateur $\Delta_{\mathbf{b}}$ est alors nul.

Le traitement de Ξ diffère quelque peu suivant la nature de f.

b. Cas où f est une fraction rationnelle non polynôme

b.1. Contribution des b de $\mathcal{A}(B,q,f)$

Ici, $\mathcal{A}(B,q,f)$ est l'ensemble es $\mathbf{b}$ vérifiant les conditions (2.1) et (2.2) de la Proposition 2.3. On développe en série de Fourier la fonction caractéristique de l'intervalle $[1,AM]$. Par des techniques classiques, on a donc l'inégalité

$$\sum_{r(\mathrm{mod}\ q)} \sum_{s\le AM} \psi\big((\Delta_{\mathbf{b}} f)(r,s)\big) \ll \frac{1}{q} \sum_{m=0}^{m=q-1} \min(AM, \|m/q\|^{-1}) \Big| \sum_{r(\mathrm{mod}\ q)} \sum_{s(\mathrm{mod}\ q)} \psi\Big((\Delta_{\mathbf{b},m} f)(r,s)\Big)\Big|$$

avec $\|\alpha\|$ désigne la distance de α à l'entier le plus proche.

Puisque $\mathbf{b}$ appartient à $\mathcal{A}(B,q,f)$, nous pouvons faire appel au résultat suivant de Hooley, conséquence de la résolution par Deligne de la conjecture de Weil([Ho] Theorem 5) :

LEMME 4.1. – *Soit q un nombre premier, $f(X_1,X_2,X_3)$ et $g(X_1,X_2,X_3)$ deux fractions rationnelles à trois variables sur $\mathbb{F}_q$, tels que*

i) *La variété $W(t)$ définie par les équations $f(\mathbf{X})-t=0$ et $g(\mathbf{X})=0$ est génériquement une courbe absolument irréductible;*

ii) *Pour toute spécialisation de t dans $\overline{\mathbb{F}}_q$, $W(t)$ est une courbe (éventuellement réductible) ou la variété vide. Alors, on a la majoration*

$$\sum_{\substack{g(X_1,X_2,X_3)=0 \ (\mathrm{mod}\ q)\\ 0\le X_1,X_2,X_3<q}} \psi\big(f(X_1,X_2,X_3)\big) = O(q),$$

où la constante impliquée dans le symbole O ne dépend que des degrés de f et g.

Si $\mathbf{b}\in\mathcal{A}(B,q,f)$ la condition *i)* est donc satisfaite. La condition *ii)* est satisfaite elle-aussi, puisque $\big(\Delta_{\mathbf{b},m} f\big)$ est non constant (voir la discussion aux paragraphes II.c.1 et II.c.2, concernant $\mathrm{NUM}(X,0)$ qui comporte un terme de degré $(2\ell-1)q(0)$). La contribution à Ξ, des $\mathbf{b}\in\mathcal{A}(B,q,f)$ en question est ainsi en $O(AB^{2\ell}M+qB^{2\ell}\log q)$ soit encore

$$O(qB^{2\ell}\log q). \tag{4.7}$$

b.2. Cas où $\mathbf{b}$ n'appartient pas à $\mathcal{A}(B,q,f)$

Nous montrons d'abord le

LEMME 4.2. – *Soit $f(X)=P(X)/Q(X)$ une fraction rationnelle de $\mathbb{Z}(X)$, quotient de deux polynômes unitaires de $\mathbb{Z}[X]$, premiers entre eux avec $\deg Q\ge 1$. Soit $\mathbf{b}=(b_1,\cdots,b_\ell,b'_1,\cdots,b'_\ell)$, un élément non diagonal de $(\mathbb{Z}/q\mathbb{Z})^{2\ell}$. Il existe alors une constante absolue $C=C(\deg P,\deg Q)$ telle que le cardinal de l'ensemble des Y_0 modulo q pour lesquels la fonction rationnelle en X définie par $(\Delta_{\mathbf{b}} f)(X,Y_0)$ soit constante sur $\mathbb{Z}/q\mathbb{Z}$ est inférieur à C.*

Preuve. – Quitte à diminuer la valeur de ℓ, on peut supposer qu'on a toujours $b_i \neq b'_j$, puisque l'opérateur $\Delta_{\mathbf{b}}$ est inchangé par suppression des b_i et b'_j tels que $b_i = b'_j$. Puisque le $\mathbf{b}$ initial est non diagonal, on parvient à un nouveau $\mathbf{b}$ de longueur $2\ell \geq 2$. Écrivons la décomposition en éléments simples de f sur $\overline{\mathbb{F}_q}$:

$$f(X) = \sum_{\nu=0}^{\infty} a_\nu X^\nu + \sum_{\alpha \in \overline{\mathbb{F}_q}} \sum_{\beta=1}^{\infty} \frac{C_{\alpha,\beta}}{(X-\alpha)^\beta};$$

où les a_ν et les $C_{\alpha,\beta}$ sont presque tous nuls.

Soit Y_0 non nul. Si q est assez grand, pour montrer que la fonction rationnelle $\big(\Delta_{\mathbf{b}} f\big)(X, Y_0)$ est constante, il faut et il suffit de montrer que le développement en éléments simples de la fraction rationnelle $\big(\Delta_{\mathbf{b}} f\big)(X, Y_0)$ est constant. Soit $\beta_0 (\geq 1)$ l'ordre maximal des zéros de $Q(X)$ et α^* les zéros correspondants. L'unicité du développement en éléments simples entraîne que si $\big(\Delta_{\mathbf{b}} f\big)(X, Y_0)$ est constant, il en est de même de

$$\sum_{\alpha^*} C_{\alpha^*,\beta_0} \Big\{ \sum_{i=1}^{\ell} \frac{1}{(Y_0(X+b_i) - \alpha^*)^{\beta_0}} - \sum_{j=1}^{\ell} \frac{1}{(Y_0(X+b'_j) - \alpha^*)^{\beta_0}} \Big\},$$

avec $C_{\alpha^*,\beta_0} \neq 0$. L'expression précédente est somme de fractions élémentaires dont les pôles sont les $-b_i + \alpha^* Y_0^{-1}$ et les $-b'_j + \alpha^* Y_0^{-1}$. La liste précédente comporte au moins deux termes. Donc les pôles doivent se détruire entre eux, ainsi dans la liste précédente, il y a au moins deux termes qui coïncident. L'éventualité $-b_i + \alpha_1^* Y_0^{-1} = -b'_j + \alpha_2^* Y_0^{-1}$ ne fournit qu'un nombre fini de possibilités pour Y_0. Il en est de même pour l'éventualité $-b_i + \alpha_1^* Y_0^{-1} = -b_j + \alpha_2^* Y_0^{-1}$ si $b_i \neq b_j$. Enfin, lorsque $b_i = b_j$ avec $i \neq j$, le pôle $-b_i + \alpha^* Y_0^{-1}$, au cas où il ne serait pas déjà de la forme $-b_k + \alpha_1^* Y_0^{-1}$ (b_k différent de b_i) ou $-b'_k + \alpha_1^* Y_0^{-1}$, ne peut disparaître puisque, après regroupement, l'élément simple qui lui serait associé serait

$$\frac{C_{\alpha^*,\beta_0}}{(Y_0(X+b_i) - \alpha^*)^{\beta_0}} . |\{j;\ b_j = b_i\}|,$$

qui est non nul, pour q assez grand. ■

Pour traiter ce cas nous utilisons le resultat de Weil, dont nous utilisons une des formes dues à Bombieri (voir aussi [De2]) :

LEMME 4.3 ([Bo] Theorem 6). – *Soit X une courbe projective de $\mathbb{P}^n(\mathbb{F}_p)$ de degré d_1. Soit $R(X_1, \cdots, X_{n+1})$ une fonction homogène rationnelle sur $\mathbb{P}^n(\mathbb{F}_p)$, et soit d_2 le degré de son numérateur. Soit ψ un caractère additif non trivial sur $\mathbb{F}_p$.*

On suppose qu'on a l'inégalité $d_1 d_2 < p$ et que R n'est constant sur aucune des composantes absolument irréductibles de la variété X. On a alors l'inégalité

$$\Big| \sum_{\mathbf{x} \in X} \psi\big(R(\mathbf{x})\big) \Big| \leq (d_1^2 + 2d_1 d_2 - 3d_1)\sqrt{p} + d_1^2.$$

La contribution à Ξ des $\mathbf{b}$ de $\mathcal{B}$ n'appartenant pas $\mathcal{A}(B, q, f)$ est en

$$O(B^{2\ell-1}.AM.q^{\frac{1}{2}} + B^{2\ell-1}.q + B^{\ell}.AM.q),$$

où le premier terme correspond aux $\mathbf{b}$ non diagonaux tels que $r \to (\Delta_{\mathbf{b}} f)(r,s)$ est non constante (on a fait appel au Lemme 4.3 et à la définition de $\mathcal{A}(B,q,f)$), le second terme aux $\mathbf{b}$ non diagonaux tels que $r \to (\Delta_{\mathbf{b}} f)(r,s)$ soit constante (on a fait appel au Lemme 4.2) et le troisième aux $\mathbf{b}$ diagonaux.

Ainsi, grâce à (4.7), on a la majoration

$$\Xi = O(qB^{2\ell}\log q + q^{\frac{1}{2}}AB^{2\ell-1}M + qAB^{\ell}M).$$

On fixe alors

$$A = M^{-\frac{1}{\ell+1}}N^{\frac{\ell}{\ell+1}} \text{ et } B = (MN)^{\frac{1}{\ell+1}}, \tag{4.8}$$

on a alors $AB = N$, les conditions $A \geq 1$ et $AM \leq q$ sont alors satisfaites si on a

$$(MN)^{\ell} < q^{\ell+1} \text{ et } M < N^{\ell}.$$

Ceci étant fixé, on a l'inégalité

$$\Xi = O\Big(q(MN)^{\frac{2\ell}{\ell+1}}\log q + q^{\frac{1}{2}}(MN)^{\frac{3\ell}{\ell+1}}\Big),$$

puis en reportant dans (4.6) et (4.4), on a finalement

$$S_{\mathrm{I}}(f,q;M,N) = O\Big(q^{\frac{1}{2\ell}+\varepsilon}M^{\frac{2\ell+1}{2\ell+2}}N^{\frac{2\ell^2-1}{2\ell^2+2\ell}} + q^{\frac{1}{4\ell}+\varepsilon}M^{\frac{2\ell^2+2\ell-1}{2\ell(\ell+1)}}N^{\frac{2\ell^2+\ell-2}{2\ell(\ell+1)}}\Big).$$

On reconnaît alors (1.2.1).

c. Cas où f est un polynôme de degré au moins 3

c.1. Contribution des $\mathbf{b}$ de $\mathcal{A}(B,q,f)$

Nous définissons $\mathcal{A}(B,q,f)$ comme étant l'ensemble des $\mathbf{b}$ de $\mathcal{B}$, tels que, pour aucun m de $\mathbb{Z}$, $\big(\Delta_{\mathbf{b},m} f\big)(X,Y)$ ne soit composé et tels que $b_1 + \cdots + b_\ell - b'_1 - \cdots - b'_\ell \neq 0$ ou $b_1^2 + \cdots + b_\ell^2 - b_1'^2 - \cdots - b_\ell'^2 \neq 0$ modulo q. Autrement dit, le complémentaire dans $\mathcal{B}$, de $\mathcal{A}(B,q,f)$ est la réunion des ensembles $\mathcal{E}(B,q,f)$ et $\mathcal{F}(B,q,f)$ (définis au paragraphe II.d.1) qui sont tous deux de cardinal en $O(B^{2\ell-2})$, d'après la Proposition 2.4. Par une démarche semblable à celle du paragraphe IV.b.1, la condition *ii)* du Lemme 4.1 étant alors facilement satisfaite (voir (2.5) par exemple), on voit que la contribution de tels $\mathbf{b}$ vérifie aussi (4.7).

c.2. Cas où $\mathbf{b}$ n'appartient pas à $\mathcal{A}(B,q,f)$

Nous remplaçons le Lemme 4.2 par le

LEMME 4.4. – *Soit* $\mathbf{b}$ *un élément non diagonal de* $(\mathbb{Z}/q\mathbb{Z})^{2\ell}$, *et soit* f *un polynôme unitaire modulo* q, *de degré* $k > \ell$. *Il existe alors une constante* $C = C(\deg f)$ *tel que le nombre de* Y_0, *modulo* q, *pour lesquels le polynôme en* X, $(\Delta_{\mathbf{b}} f)(X,Y_0)$ *soit constant, est inférieur à* C.

Preuve. – Soit $f(X) = \sum_{i=0}^{k} f_i X^i$ avec $f_k = 1$ et

$$\sigma_i = b_1^i + \cdots + b_\ell^i - {b'_1}^i + \cdots + {b'_\ell}^i.$$

Puisque $\mathbf{b}$ est non diagonal et que q est assez grand, il existe ν avec $1 \leq \nu \leq \ell$ tel que σ_ν soit non nul (c'est une conséquence des formules de Newton). On fixe ν comme étant le plus petit possible. La relation

$$(\Delta_{\mathbf{b}} X^n)(X,Y) = Y^n \sum_{i=1}^{n} \binom{n}{i} \sigma_i X^{n-i},$$

entraîne, par linéarité, l'égalité

$$\begin{aligned}(\Delta_{\mathbf{b}} f)(X,Y_0) &= \sum_{n=1}^{k} f_n Y_0^n \sum_{i=1}^{n} \binom{n}{i} \sigma_i X^{n-i} = \sum_{n=\nu}^{k} f_n Y_0^n \sum_{i=\nu}^{n} \binom{n}{i} \sigma_i X^{n-i} \\ &= \sum_{j=0}^{k-\nu} X^j \Big(\sum_{n=j+\nu}^{k} f_n \binom{n}{j} \sigma_{n-j} Y_0^n \Big).\end{aligned}$$

Puisque, dans l'expression précédente, on a $k > \ell \geq \nu$, le coefficient du terme de plus haut degré en X est un polynôme en Y_0 de degré k et de terme dominant $f_k \binom{k}{k-\nu} \sigma_\nu Y_0^k$. Ce polynôme en Y_0 n'est pas formellement nul, il y a donc au plus que k valeurs de Y_0 telles que $(\Delta_{\mathbf{b}} f)(X,Y_0)$ soit constant par rapport à Y_0. ■

Le cardinal du complémentaire de $\mathcal{A}(B,q,f)$ est maintenant en $O(B^{2\ell-2})$. Par la démarche de IV.b.2 (qui consiste à envisager séparément $\mathcal{D}(B)$, et les $\mathbf{b}$ non diagonaux suivant que l'application $r \to (\Delta_{\mathbf{b}} f)(r,s)$ soit constante ou non) et par les Lemmes 4.3 et 4.4, on voit que la contribution à Ξ des $\mathbf{b}$ n'appartenant pas à $\mathcal{A}(B,q,f)$ est

$$O(B^{2\ell-2}.AM.q^{\frac{1}{2}} + B^{2\ell-2}.q + B^{\ell}.AM.q),$$

puis, grâce à (4.7), on a finalement

$$\Xi = O(qB^{2\ell} \log q + q^{\frac{1}{2}} AB^{2\ell-2} M + qAB^{\ell} M).$$

On donne à A et B les valeurs fixées par (4.8) on parvient à

$$\Xi = O\big(q(MN)^{\frac{2\ell}{\ell+1}} \log q + q^{\frac{1}{2}} (MN)^{\frac{3\ell-2}{\ell+1}}\big),$$

on reporte alors dans (4.6) et (4.4). La majoration (1.2.2) est ainsi obtenue. ■

d. Cas où f est un quasi–monôme

Nous sommes maintenant dans la situation où $f(X) = X^k + uX$ avec u entier et k entier relatif différent de 0 et 1. Notre intention est d'appliquer le Théorème 3.1 au lieu du Lemme 4.1 ; le contrôle de la condition $(3.*)$ est assuré par le

LEMME 4.5. – *Pour $k \in \mathbb{Z} - \{0,1\}$ et $\mathbf{b} = (b_1, \cdots, b_\ell, b'_1, \cdots b'_\ell) \in \mathbb{Z}^{2\ell}$, on pose*

$$R_{\mathbf{b}}(X) = \sum_{i=1}^{\ell} \big((X+b_i)^k - (X+b'_i)^k\big), \tag{4.9}$$

et $\mathcal{D}(B;q,k)$ désigne l'ensemble des $\mathbf{b}$ avec b_i, b'_i compris entre 0 et B, tels qu'il existe un entier λ tel que la fraction rationnelle $R_{\mathbf{b}}(X) + \lambda$ ne vérifie pas la condition $(3.*)$.

Si $k < 0$ ou si $1 \leq \ell < \min\{p; p|(k, q-1)\}$, l'ensemble $\mathcal{D}(B;q,k)$ est la diagonale $\mathcal{D}(B)$.

Pour $k < 0$, on utilise l'existence et l'unicité de la décomposition d'une fraction rationnelle en éléments simples. Soit $\mathbf{b}$ non diagonal et q assez grand, on écrit

$$R_{\mathbf{b}}(X) = \sum_{i=1}^{n} c_i (X + \tilde{b}_i)^k,$$

avec $n \geq 2$, les c_i tous non nuls modulo q et les $\tilde{b}_i$ tous distincts. Soit $d|(k, q-1)$, $d > 1$, tel qu'on ait l'écriture

$$R_{\mathbf{b}}(X) + \lambda = c\big(s(X)\big)^d. \tag{4.10}$$

Nécessairement $s(X)$ admet $-\tilde{b}_1$ comme pôle d'ordre k/d, ce qui donne

$$s(X) = \alpha(X + \tilde{b}_1)^{k/d} + s_1(X),$$

avec $c_1 = c\alpha^d$, $s_1(X)$ non nul admettant $-\tilde{b}_1$, pour pôle d'ordre δ avec $0 \leq \delta < k/d$. Mais en développant la fonction

$$S(X) = c(s(X))^d - c_1(X + \tilde{b}_1)^k,$$

on voit que celle–ci admet $-\tilde{b}_1$ pour pôle d'ordre $(d-1)k/d + \delta$ (donc d'ordre au moins égal à 1 puisque $d > 1$), ce qui est impossible puisque $S(X)$ est aussi égale à $\sum_{i=2}^{n} c_i (X + \tilde{b}_i)^k$.

Dans le cas où k est au moins égal à 1, on raisonne différemment. On part de la relation (4.10) mais avec maintenant $s(X) \in \mathbb{Z}[X]$. Puisque le membre de gauche est de degré au plus $k-1$ et qu'il est un multiple de d, il ne peut être qu'inférieur à $k-d$. En écrivant que les coefficients des monômes de degré compris entre $k-d+1$ et $k-1$ sont nuls, on obtient les relations

$$\sum_{i=1}^{\ell} b_i^j = \sum_{i=1}^{\ell} b_i'^j \quad (1 \leq j \leq d-1),$$

et ceci entraîne que $(b_1, \cdots, b_\ell)$ coïncide avec $b'_1, \cdots, b'_\ell$ à l'ordre près, pourvu que $d - 1 \geq \ell$. ■

Partant de (4.6), on décompose la contribution à Ξ des $\mathbf{b}$ en deux parties :

• La contribution des $\mathbf{b}$ de $\mathcal{D}(B;q,k)=\mathcal{D}(B)$ est, d'après le Lemme 4.5, trivialement en $O(qAMB^{\ell})$.

• Pour les autres $\mathbf{b}$, on développe, comme en IV.b.1, en série de Fourier la fonction caractéristique de l'intervalle $[1,AM]$. On obtient alors, en suivant les notations du paragraphe III, la relation

$$\sum_{r(\mathrm{mod}\ q)}\sum_{s\leq AM}\psi\big((\Delta_{\mathbf{b}}f)(r,s)\big)\ll\frac{1}{q}\sum_{m=0}^{m=q-1}\min\big(AM,\|(m/q)\|^{-1}\big)\Big|\sum_{x}S_k(R_{\mathbf{b}}(x),u\beta+m)\Big|,$$

avec

$$\beta=\sum_{i=1}^{\ell}(b_i-b_i'). \tag{4.11}$$

La fonction $R_{\mathbf{b}}(X)$ est une fraction rationnelle qui vérifie l'hypothèse $(3.*)$. On fait donc appel à la majoration (3.1) du Théorème 3.1. On obtient finalement

$$\Xi=O\big(qB^{2\ell}\log q+qAB^{\ell}M\log q\big).$$

On donne aux paramètres A et B les valeurs (4.8). Par (4.4) et (4.6) on est parvenu à (1.2.3). ■

V. Démonstration de la proposition 1.3

La démonstration est une conséquence du Lemme 4.3. Par Cauchy–Schwarz, on a l'inégalité

$$|S_{\mathrm{II}}(f,q;M,N)|\leq M^{\frac{1}{2}}\Big\{\sum_{n_1}\sum_{n_2}\Big|\sum_{m}\psi(f(mn_1)-f(mn_2))\Big|\Big\}^{\frac{1}{2}}, \tag{5.1}$$

Pour étudier la fonction $f(mn_1)-f(mn_2)$, nous montrerons d'abord le

LEMME 5.1. – *Soit $R(X)$ une fraction rationnelle de $\mathbb{Z}(X)$, qui n'est ni un polynôme de degré 1, ni un polynôme constant. Alors, pour q assez grand, le cardinal des (n_1,n_2) avec $1\leq n_1,n_2\leq N<q$, tels que $R(n_1X)-R(n_2X)(\mathrm{mod}\ q)$ soit un polynôme de degré 1 ou un polynôme constant est $O(N)$. Le O dépend au plus des degrés du numérateur et du dénominateur de R.*

Signalons d'abord que l'ensemble étudié contient trivialement (n_1,n_2) avec $n_1=n_2$. Par changement de variable, le cardinal cherché est inférieur à

$$N.\sharp\{t(\mathrm{mod}\ q);R(X)-R(tX)=aX+b(\mathrm{mod}\ q)\}.$$

Faisons la décomposition en éléments de $R(X)$ sur $\overline{\mathbb{F}}_q(X)$; ainsi, a–t–on

$$R(X)=\sum_{\nu=0}^{\infty}a_\nu X^\nu+\sum_{\beta=1}^{\infty}\sum_{\alpha\in\overline{\mathbb{F}}_q}\frac{C_{\alpha,\beta}}{(X-\alpha)^\beta},$$

où les a_ν et les $C_{\alpha,\beta}$ sont presque tous nuls. Par hypothèse, l'une au moins des trois éventualités suivantes a lieu :

– il existe $\nu \geq 2$ avec $a_\nu \neq 0$. On a alors $t^\nu = 1$, d'où un nombre fini de valeurs possibles pour t.

– il existe $\beta \geq 1$ avec $C_{0,\beta} \neq 0$. On a de même $t^\beta = 1$, d'où un nombre fini de valeurs possibles pour t.

– la fraction rationnelle R a un pôle $\alpha \neq 0$, donc R a aussi pour pôles α/t, α/t^2,...or R n'a qu'un nombre fini de pôles, d'où, là aussi un nombre fini de valeurs de t. ■

Par le Lemme 5.1, la contribution à $\{\cdots\}$ de (5.1), des (n_1, n_2) tels que $f(mn_1) - f(mn_2)$ soit un polynôme de degré au plus 1 est trivialement en $O(MN)$.

Pour les (n_1, n_2) restants, on fait un développement en série de Fourier de l'intervalle de sommation sur m, qui nous amène à considérer, comme dans IV.b.1, pour tout h entier compris entre 0 et $q-1$, la somme complète

$$\sum_{m(\mathrm{mod}\ q)} \psi\big(f(mn_1) - f(mn_2) - hm\big).$$

Puisque la fonction de m en cause dans l'expression précédente n'est pas constante, d'après le Lemme 4.3, on voit que cette somme est en $O(q^{1/2})$. Reportant dans (5.1) ces deux types de contribution, on obtient la majoration

$$S_{\mathrm{II}}(f, q; M, N) \ll M^{\frac{1}{2}}\big\{MN + q^{\frac{1}{2}}N^2 \log q\big\}^{\frac{1}{2}}. \quad ■$$

VI. Démonstration du théorème 1.1

a. Cas où f n'est pas un polynôme de degré 2 ou 3

Il est classique de démontrer la même relation que (1.1) pour la somme

$$\tilde{S}(f; q, x) := \sum_{n \leq x} \Lambda(n)\psi(f(n))$$

et de se ramener à $S(f; q, x)$ par une sommation d'Abel. On part de l'identité de Vaughan (voir par exemple [Da] p.139), pour écrire

$$\tilde{S}(f; q, x) = \sum_{m \leq UV} \alpha_m^{(1)} \sum_{n < x/m} \psi(f(mn)) + \sum_{m \leq V} \alpha_m^{(2)} \sum_{n < x/m} \log n\ \psi(f(mn)) +$$

$$+ \sum_{m > U} \alpha_m^{(3)} \sum_{\substack{n > V \\ n < x/m}} \beta_n^{(3)} \psi(f(mn)) + O(U), \tag{6.1}$$

où U et V sont deux paramètres supérieurs à 1, à notre disposition. Les quatre coefficients $\alpha^{(1)}$, $\alpha^{(2)}$, $\alpha^{(3)}$ et $\beta^{(3)}$, dont il est inutile de rappeler la définition, ont la propriété d'être en $O(q^\varepsilon)$ pour tout $\varepsilon > 0$.

Nous fixons

$$U = q^{-\frac{3}{8}} x^{\frac{7}{16}}, \quad V = q^{\frac{1}{8}} x^{\frac{7}{16}}.$$

On décompose la première somme à droite de (6.1) en $\sum_{m \leq V} \sum_{n < x/m}$ et $\sum_{V < m \leq UV} \sum_{U < n < x/m}$, les termes oubliés contribuant en $O(q^{\varepsilon} U^2 V)$.

On découpe alors les intervalles de variation de m et n en $O(q^{\varepsilon})$ intervalles de la forme $]M, 4M/3]$ et $]N, 4N/3]$. Après division par q^{ε}, l'étude de la partie droite de (6.1) se réduit à majorer deux types de sommes :

$$\Sigma^{(\mathrm{I})}(M,N) = \sum_{\substack{M < m \leq 4M/3 \\ mn < x}} \sum_{N < n \leq 4N/3} \alpha_m \psi(f(mn)),$$

pour $M < V$ et $MN < x$, et

$$\Sigma^{(\mathrm{II})}(M,N) = \sum_{\substack{M < m \leq 4M/3 \\ mn < x}} \sum_{N < n \leq 4N/3} \alpha_m \beta_n \psi(f(mn)),$$

pour $M > V$, $N > U$ et $MN < x$. Dans ces expressions, α_m et β_n sont des coefficients inférieurs à 1 en valeur absolue et la deuxième somme à droite de (6.1) nécessite, en plus, une sommation d'Abel (que nous omettons) pour tenir compte des lentes variations du logarithme.

En conclusion, nous avons l'inégalité

$$\tilde{S}(f;q,x) \ll q^{\varepsilon} \Big(\sup_{M < V, MN < x} \Big| \Sigma^{(\mathrm{I})}(M,N) \Big| + \sup_{\substack{M > V, N > U \\ MN < x}} \Big| \Sigma^{(\mathrm{II})}(M,N) \Big| + U^2 V \Big). \tag{6.2}$$

Dans les sommes $\Sigma^{(\mathrm{I})}(M,N)$ et $\Sigma^{(\mathrm{II})}(M,N)$, la condition de sommation $mn < x$ est superflue lorsque M et N vérifient $16MN/9 < x$. Pour les autres (M,N), c'est-à-dire ceux tels que $MN < x < 16MN/9$, on voit que le produit mn se déplace sur un intervalle de longueur $7MN/9 < q$. La fonction caractéristique de cet intervalle s'exprime alors, de façon classique, par les caractères additifs ψ^h avec $0 \leq h \leq q-1$, d'où, en reprenant les notations de l'introduction, on a l'inégalité

$$\Sigma^{(\mathrm{I})}(M,N) \ll \frac{1}{q} \sum_{h=0}^{q-1} \min \left(q, \left\| \frac{h}{q} \right\|^{-1} \right) |S_{\mathrm{I}}(f(X) - hX, q; M, N)| \tag{6.3}$$

et une relation absolument identique en remplaçant les indices I par II.

Il est important de noter que l'adjonction à $f(X)$ de la fonction $-hX$ n'affecte en rien sa nature de fraction rationnelle avec pôle, de polynôme de degré ≥ 4 ou de quasi-monôme. Ainsi, suivant les cas, les relations (1.2.1) ou (1.2.2), donnent, pour M et N comme ci-dessus, et le choix $\ell = 3$, l'inégalité

$$\Sigma^{(\mathrm{I})}(M,N) \ll q^{\frac{1}{6}+\varepsilon} M^{\frac{7}{8}} (x/M)^{\frac{17}{24}} \ll q^{\frac{1}{6}+\varepsilon} x^{\frac{17}{24}} V^{\frac{1}{6}} \ll q^{\frac{3}{16}+\varepsilon} x^{\frac{25}{32}}. \tag{6.4}$$

Maintenant, l'analogue, pour $\Sigma^{(\mathrm{II})}(M,N)$, de la relation (6.3) donne, grâce à la Proposition 1.3, la majoration suivante

$$\Sigma^{(\mathrm{II})}(M,N) \ll q^{\varepsilon} x N^{-\frac{1}{2}} + q^{\frac{1}{4}+\varepsilon} x M^{-\frac{1}{2}}.$$

Les minorations $M > V$ et $N > U$, et les valeurs de U et V prouvent que $\Sigma^{(\mathrm{II})}(M,N)$ et $U^2 V$ vérifient aussi l'inégalité (6.4), ce qui, par (6.2), termine la preuve du Théorème 1.1, dans ce cas.

b. Cas où f est un polynôme de degré 2 ou 3

Les conditions relatives à (1.2.2) nous obligeraient à choisir $\ell = 2$ si $\deg f = 3$, ce qui donnerait un résultat moins bon, ou $\ell = 1$ si $\deg f = 2$, ce qui serait totalement inefficace. Heureusement le résultat suivant ([Harm] Theorem 1) permet de conclure :

LEMME 6.1. – *Soit $f(X)$ un polynôme de $\mathbb{R}[X]$ de degré $k \geq 2$. On suppose que le coefficient dominant α de f vérifie $|\alpha - \frac{a}{q}| \leq \frac{1}{q^2}$ avec a et q entiers premiers entre eux. On a alors, pour tout $\varepsilon > 0$ la majoration*

$$\sum_{p \leq x} e(f(p)) = O_\varepsilon\left(x^{1+\varepsilon}\left(\frac{1}{q} + \frac{1}{\sqrt{x}} + \frac{q}{x^k}\right)^{4^{1-k}}\right).$$

Ainsi pour $\deg f = 2$, on a

$$S(f;q,x) \ll q^\varepsilon(x^{\frac{7}{8}} + q^{\frac{1}{4}}x^{\frac{1}{2}}) \ll q^{\frac{3}{16}+\varepsilon}x^{\frac{25}{32}},$$

et, pour $\deg f = 3$, on a

$$S(f;q,x) \ll q^\varepsilon(x^{\frac{31}{32}} + q^{\frac{1}{16}}x^{\frac{13}{16}}) \ll q^{\frac{3}{16}+\varepsilon}x^{\frac{25}{32}},$$

pour $x \leq q$. ■

Remarques. – Il est clair que les mêmes Proposition 1.2 et 1.3 conduisent à une majoration de $|S(f;q,x)|$ pour $x > q$ par des découpages de la forme $]M,(1+\delta)M]$ et $]N,(1+\delta)N]$,avec $\delta = q/(3x)$ par exemple. Mais les majorations obtenues deviennent rapidement, lorsque $\log x/\log q$ s'éloigne de 1, de moins bonne qualité que ce qu'on obtiendrait en appliquant directement la majoration de Weil lors de l'étude de Σ^{I}. Enfin, il est peut–être possible d'améliorer le Théorème 1.1 par un jeu combinatoire plus sophistiqué sur les sommes de type I et II: ceci serait intéressant, non seulement par la qualité des résultats obtenus, mais aussi par les moyens de géométrie algébrique qu'il faudrait certainement mettre en œuvre.

VII. Démonstration du théorème 1.4

Dans ce paragraphe, f est le quasi–monôme $f(X) = X^k + uX$. L'inégalité de Cauchy–Schwarz rend la variable n lisse :

$$S := \sum_m \sum_n \alpha_m \beta_n \psi\big(f(mn)\big) \leq N^{\frac{1}{2}}\Big\{\sum_{m_1}\sum_{m_2}\Big|\sum_n \psi\big(f(m_1n) - f(m_2n)\big)\Big|\Big\}^{\frac{1}{2}}.$$

Puisque le nombre de solutions à $m_1^k = m_2^k \pmod q$ est $O_k(M)$, on voit que S vérifie

$$S \ll N^{\frac{1}{2}}\{MN + S^{\neq}\}^{\frac{1}{2}}, \tag{7.1}$$

avec

$$S^{\neq} = \sum_{\substack{m_1 \\ m_1^k \neq m_2^k}} \sum_{m_2} \sum_n \psi\big(f(m_1n) - f(m_2n)\big)\Big|.$$

Comme au paragraphe IV (voir la formule (4.3)), on opère une translation par l'entier ab avec $A/2 < a \leq A$ et $B/2 < b \leq B$ avec

$$AB < N \qquad AM < q$$

et on utilise l'artifice de la fonction trapèze g qui majore la fonction caractéristique de $[N, 2N]$, pour montrer que, pour un certain réel t, on a la relation suivante (où V désigne le nombre de ab utilisés pour les translations)

$$VS^{\neq} \ll \log q \Big(\sum_{a} \sum_{\substack{m_1 \\ m_1^k \neq m_2^k}} \sum_{m_2} \sum_{n} \Big| \sum_{b} \psi\big(f(am_1(\bar{a}n+b)) - f(am_2(\bar{a}n+b))\big) e(-bt) \Big| \Big)$$

$$\ll (\log q)\, \Sigma^{\neq}, \tag{7.2}$$

par définition. Le lemme suivant facilitera les changements de variables

LEMME 7.1. – *Soit $\nu(r, s_1, s_2)$ le nombre de solutions au système*

$$\begin{cases} r &= \bar{a}n \pmod q \\ s_1 &= am_1 \\ s_2 &= am_2 \end{cases}$$

avec $A/2 < a \leq A$, $N < n \leq 2N$ et $M < m_1,\ m_2 \leq 2M$. Alors pour $N < q$ et tout $\varepsilon > 0$, on a la relation

$$\sum_{r} \sum_{s_1} \sum_{s_2} \nu^2(r, s_1, s_2) \ll_{\varepsilon} AM^2 N q^{\varepsilon}.$$

Démonstration. – En effet, la quantité à majorer est égale au nombre de solutions au système de 3 équations à 8 inconnues

$$\begin{cases} \bar{a}n &= \bar{a}'n' \pmod q \\ am_1 &= a'm_1' \\ am_2 &= a'm_2' \end{cases}$$

Lorsque a, m_1 et m_2 sont fixés, les deux dernières équations ont $O(q^{\varepsilon})$ solutions en a', m_1' et m_2', enfin, quand ces six inconnues sont fixées, la première équation entraîne $n \equiv a\bar{a}'n' \pmod q$ et, puisque, $N < q$, cette équation a $O(N)$ solutions. ■

Ainsi, peut–on maintenant écrire

$$\Sigma^{\neq} = \sum_{r \pmod q} \sum_{s_1} \sum_{s_2} \nu(r, s_1, s_2) \Big| \sum_{b} \psi\big(f(s_1(r+b)) - f(s_2(r+b))\big) e(-bt) \Big|;$$

où les variables s_1 et s_2 décrivent l'intervalle $[AM/2, 2AM]$ avec la contrainte $s_1^k \neq s_2^k \pmod q$ et b parcourt l'intervalle $[B/2, B]$.

On applique l'inégalité de Hölder avec l'exposant 2ℓ, $\ell \geq 1$, on revient à l'écriture explicite de f et, soit $\mathbf{b} = (b_1, \cdots, b_\ell, b'_1, \cdots, b'_\ell)$ un vecteur de $\mathbb{Z}^{2\ell}$, avec b_i et $b'_i \leq B$. On parvient à

(7.3)

$$\Sigma^{\neq} \ll (AM^2N)^{1-\frac{1}{2\ell}} \Big\{ \sum_{\mathbf{b}} \Big| \sum_{r \pmod q} \sum_{\substack{s_1 \leq AM \\ s_1^k \neq s_2^k}} \sum_{s_2 \leq AM} \psi\big((s_1^k - s_2^k)R_{\mathbf{b}}(r) + u\beta(s_1 - s_2)\big) \Big| \Big\}^{\frac{1}{2\ell}},$$

avec $R_{\mathbf{b}}$ et β définis en (4.9) et (4.11).

On envisage maintenant les différentes types de contribution des $\mathbf{b}$ à l'accolade $\{\ldots\}$ de la partie droite de (7.3) :

• Les $\mathbf{b} \in \mathcal{D}(B, q, k)$ (défini au Lemme 4.5) ont une contribution trivialement en

$$O(qA^2B^\ell M^2), \tag{7.4}$$

puisque leur nombre est en $O(B^\ell)$.

• Si $\mathbf{b}$ est hors de $\mathcal{D}(B, q, k)$, la fonction $R_{\mathbf{b}}$, d'après le Lemme 4.5 n'est pas constante, on s'intéresse à la contribution des $r \pmod q$, tels que $R_{\mathbf{b}}(r) = 0 \pmod q$. Il est facile de voir qu'ils participent en

$$O(A^2B^{2\ell}M^2). \tag{7.5}$$

Signalons que pour $u = 0$, cette majoration est optimale, par contre si on suppose $u \neq 0$, on a une bien meilleure majoration en sommant une progression géométrique. Nous n'en aurons pas besoin ici.

• Pour les $\mathbf{b}$ et r restants, on se ramène à la situation du Théorème 3.1 par les deux artifices suivants :

– on détecte la condition $s_1^k \neq s_2^k$ modulo q, par la formule

$$1 - \frac{1}{q} \sum_{\lambda=1}^{q} \psi(\lambda(s_1^k - s_2^k))$$

– on développe en série de Fourier les intervalles de variation de s_1 et s_2.

Ainsi, par les notations du paragraphe III, la contribution recherchée est

$$\ll \frac{1}{q^2} \sum_{\mathbf{b}} \sum_{h_1=0}^{q-1} \sum_{h_2=0}^{q-1} \min(q, \|\frac{h_1}{q}\|^{-1}) \min(q, \|\frac{h_2}{q}\|^{-1}) \times$$

$$\Big| \sum_{\substack{r \pmod q \\ R_{\mathbf{b}}(r) \neq 0, \infty}} S_k(R_{\mathbf{b}}(r), u\beta + h_1) \overline{S_k(R_{\mathbf{b}}(r), u\beta + h_2)}$$

$$- \frac{1}{q} \sum_{\lambda=1}^{q} \sum_{\substack{r \pmod q \\ R_{\mathbf{b}}(r) \neq 0, \infty}} S_k(R_{\mathbf{b}}(r) + \lambda, u\beta + h_1) \overline{S_k(R_{\mathbf{b}}(r) + \lambda, u\beta + h_2)} \Big|. \tag{7.6}$$

On peut faire appel aux différentes estimations du Théorème 3.1, puisque, pour $\mathbf{b}$ non diagonal, l'hypothèse $(3.*)$ est satisfaite d'après le Lemme 4.5 :

– lorsque $(u\beta + h_1)^k \neq (u\beta + h_2)^k$, on utilise (3.4),

– lorsque $(u\beta + h_1)^k = (u\beta + h_2)^k \neq 0$ on utilise (3.2),

– $(u\beta + h_1)^k = (u\beta + h_2)^k = 0$, on se sert de (3.3).

Remarquons que dans ces deux derniers cas, les termes principaux disparaissent, ce qui explique pourquoi, dans (7.1), on a écarté tout de suite la contribution de $m_1^k = m_2^k$.

En conclusion, on peut majorer la quantité apparaissant dans (7.6) par

$$O(q^{\frac{3}{2}+\varepsilon} B^{2\ell}). \tag{7.7}$$

Il suffit alors de regrouper (7.3), (7.4), (7.5) et (7.7), pour obtenir la majoration

$$\Sigma^{\neq} \ll (AM^2N)^{1-\frac{1}{2\ell}} \left\{ qA^2B^\ell M^2 + A^2B^{2\ell}M^2 + q^{\frac{3}{2}+\varepsilon}B^{2\ell} \right\}^{\frac{1}{2\ell}}. \tag{7.8}$$

Il reste à choisir la valeur des paramètres A et B ; en égalisant les premier et troisième termes de (7.8) et en imposant $AB = N$, on parvient à

$$A = q^{\frac{1}{2(\ell+2)}} M^{-\frac{2}{\ell+2}} N^{\frac{\ell}{\ell+2}} \quad \text{et} \quad B = q^{-\frac{1}{2(\ell+2)}} M^{\frac{2}{\ell+2}} N^{\frac{2}{\ell+2}}.$$

Pour que les conditions initiales $AM \leq q$, A et $B \geq 1$ soient satisfaites, il suffit d'imposer

$$q^{\frac{1}{4}} \leq MN \leq q^{1+\frac{3}{2\ell}} \text{ et } q^{\frac{1}{2}} N^\ell \geq M^2.$$

Avec ce choix, on voit que le deuxième terme à droite de (7.8) est inférieur aux deux autres pour

$$MN \leq q^{\frac{3\ell+4}{4\ell}},$$

condition plus forte que $MN \leq q^{1+\frac{3}{2\ell}}$.

Il reste à regrouper (7.1), (7.2) et (7.8), pour écrire

$$S \ll M^{\frac{1}{2}} N + q^{\frac{3\ell+5}{8\ell(\ell+2)}+\varepsilon} M^{\frac{2\ell^2+3\ell-1}{2\ell(\ell+2)}} N^{\frac{2\ell^2+3\ell-1}{2\ell(\ell+2)}}.$$

■

Remarque finale. – On peut naturellement se demander ce que serait la majoration du Théorème 1.4, si on appliquait l'inégalité de Hölder au lieu de Cauchy–Schwarz au début de la preuve. Pour les applications que nous avions en vue, il semble que Cauchy–Schwarz soit optimal. Ceci déçoit un peu, puisque les résultats du Théorème 3.1 se généralisent agréablement à des sommes de produits de 2ℓ sommes S_k ; pour fixer les idées, on peut montrer l'égalité :

$$\sum_{\substack{x \in \mathbf{F}_q \\ r(x) \neq 0, \infty}} S_k(r(x), m_1; q) \dots S_k(r(x), m_\ell; q) \overline{S_k(r(x), m_1'; q)} \dots \overline{S_k(r(x), m_\ell'; q)} = O(q^{2\ell+1/2})$$

pour r fraction rationnelle non constante, et $m_i^k \neq m_j'^k$ modulo q, pour tous les indices i et j.

Remerciements

Les auteurs tiennent à remercier J.-L. Colliot-Thélène, J. Rivat et A. Schinzel de nous avoir généreusement fait partager leurs intuitions.

BIBLIOGRAPHIE

[Ba-H] R. C. Baker et G. Harman, *On the distribution of* $\{\alpha p^k\}$ *modulo* 1, (*Mathematika,* vol. 38, 1991, p. 170-184).

[Bo] E. Bombieri, *Exponential sums in finite fields,* (*Amer. J. Math.,* vol. 88, 1966, p. 71-105).

[B-S] E. Bombieri et S. Sperber, *On the estimation of certain exponential sums,* (*Acta Arith.*, vol. 69, 1995, p. 329-358).

[Da] H. Davenport, *Multiplicative Number Theory (Second Edition),* (*Graduate Texts in Mathematics*, vol. 74, Springer Verlag, Berlin-Heidelberg-New York, 1980).

[D-S] H. Davenport et A. Schinzel, *Two problems concerning polynomials,* (*J. reine angew. Math.*, vol. 214-215, 1964, p. 386-391).

[De1] P. Deligne, *La Conjecture de Weil I,* (*Publ. de l'I.H.E.S.*, vol. 43, 1974, p. 273-308).

[De2] P. Deligne, *Applications de la Formule des Traces aux Sommes Trigonométriques, Séminaire de Géométrie Algébrique du Bois-Marie SGA41/2, Cohomologie Étale,* (*Lecture Notes in Mathematics*, vol. 569, Springer Verlag, Berlin-Heidelberg-New York, 1977, p. 168-232).

[De3] P. Deligne, *La Conjecture de Weil II,* (*Publ. de l'I.H.E.S.*, vol. 52, 1981, p. 313-428).

[Fo-1] E. Fouvry et H. Iwaniec, *The divisor function over arithmetic progressions, (with appendix by N. Katz),* (*Acta Arith.,* vol 61, 1992, p. 271-287).

[Fri] M. Fried, *The field of definition of function fields and a problem in the reduibility of polynomials in 2 variables, Ill.* (*J. Math.*, vol. 17, 1973, p. 128-144).

[Fr-I1] J. Friedlander et H. Iwaniec, *Incomplete Kloosterman sums and a divisor problem,* (*Annals of Maths.*, vol. 121, 1985, p. 319-350).

[Fr-I2] J. Friedlander et H. Iwaniec, *Estimates for Character Sums,* (*Proc. Amer. Math. Soc.*, vol. 19, 1993, p. 365-372).

[Gh] A. Ghosh, *The Distribution of* αp^2 *modulo* 1, (*Proc. London Math. Soc.*, (3), vol. 42, 1981, p. 252-269).

[Harm] G. Harman, *Trigonometric Sums over Primes I,* (*Mathematika*, vol. 28, 1981, p. 249-254).

[Hart] R. Hartshorne, *Algebraic Geometry,* (*Graduate Texts in Mathematics*, vol. 52, Springer Verlag, Berlin-Heidelberg-New York, 1977).

[Ho] C. Hooley, *On exponential sums and certain of their applications,* (*Journées Arith. 1980*, J.V. Armitage (ed), p. 92-122, Cambridge, 1982).

[Hu] L. K. Hua, *Additive Theory of Prime Numbers,* (*Translations of Mathematical Monographs*, vol. 13, American Math. Soc., 1965).

[Ka1] N. M. Katz, *Gauss Sums, Kloosterman Sums and Monodromy Groups,* (*Annals of Maths. Studies*, vol. 116, PUP).

[Ka2] N. M. Katz, *Exponential sums and Differential Equations,* (*Annals of Maths. Studies*, vol. 124, PUP).

[Mi] P. Michel, *Autour des Conjectures de Sato-Tate,* (*Thèse de Doctorat d'État, Université de Paris-Sud,* Orsay, 1995).

[Mu] D. Mumford, *The Red Book of Varieties and Schemes,* (*Lectures Notes in mathematics*, vol. 1358, Springer Verlag, Berlin-Heidelberg-New York, 1988).

[Schi1] A. Schinzel, *Reducibility of polynomials in several variables,* (*Bull. Acad. Pol. Sci. Sér. Sci. Math. Astronom. Phys.*, vol. 11, 1963, p. 633-638).

[Schi2] A. Schinzel, *Reducibility of polynomials in several variables. II,* (*Pacific J. Math.*, vol. 118, 1985, p. 531-563).

[Schm] W. SCHMIDT, *Equations over finite fields : an elementary approach,* (*Lecture Notes in Mathematics*, vol. 536, Springer Verlag, Berlin-Heidelberg-New York, 1976).

[Va] R. C. VAUGHAN, *Mean Value Theorems in Prime Number Theory,* (*J. London Math. Soc., (2),* vol. 10, 1975, p. 153-162).

[Vi] M. VINOGRADOV, *The Method of Trigonometric Sum in the Theory of Numbers, Translated, revised and annotated by A. Davenport and K. F. Roth* (Interscience, New York, 1954).

(Manuscrit reçu le 5 novembre 1996.)

Étienne FOUVRY
et Philippe MICHEL
Mathématique, Bâtiment 425
Université de Paris-Sud
F-91405 Orsay Cedex
fouvry@math.u-psud.fr
michel@math.u-psud.fr