ACTA ARITHMETICA
LXII.4 (1992)

Sommes d'exponentielles dans $\mathbb{F}_{2^h}((X^{-1}))$

par

Mireille Car (Marseille)

Introduction. Soit $\mathbb{F}_q$ le corps fini à q éléments. Il est intéressant de poser le problème de Waring dans l'anneau $\mathbb{F}_q[X]$ avec les conditions de degré les plus restrictives possibles. On a alors un problème analogue au problème de Waring "difficile" de l'arithmétique classique. Pour le résoudre, on adapte à $\mathbb{F}_q[X]$ la méthode de Hardy et Littlewood, dite méthode du cercle. C'est ce qui a été fait par R. M. Kubota (cf. [4]), pour des exposants $k < p$, où p est la caractéristique du corps $\mathbb{F}_q$. Cette restriction sur les exposants provient du fait suivant. On majore des sommes de caractères par la méthode de Weyl. Celle-ci, basée sur des différentiations successives, introduit un facteur $k!$ qui est nul et conduit donc à la majoration triviale pour $k \geq p$.

Partant d'une remarque de R. C. Vaughan (cf. [6]), J. Cherly a, dans sa thèse, supprimé cette restriction pour le problème de Waring pour les cubes dans l'anneau $\mathbb{F}_2[X]$ (cf. [2]). Il était facile de généraliser ses résultats à un anneau $\mathbb{F}_q[X]$ où q est une puissance de 2. En modifiant la méthode utilisée dans [2], on améliore les résultats qui y sont obtenus. C'est ce que nous avons fait. Les calculs étant très longs, nous présentons ce travail en deux parties. La partie consacrée à l'étude du problème de Waring pour les cubes donnera lieu à un article ultérieur. Nous donnons ici une majoration de sommes de caractères qui sera cruciale dans l'étude du problème de Waring. Pour énoncer le théorème principal, nous devons préciser quelques notations.

Soit q une puissance de 2. On note $\mathbb{A}$ l'anneau $\mathbb{F}_q[X]$, $\mathbb{K}$ le corps $\mathbb{F}_q(X)$. Sur le corps $\mathbb{K}$ est définie la valuation à l'infini $\nu = \nu_\infty$ par

$$\nu(A/B) = \deg B - \deg A$$

pour tout couple (A, B) de polynômes non nuls. Le complété $\mathbb{K}_\infty$ de $\mathbb{K}$ pour cette valuation s'identifie au corps $\mathbb{F}_q((X^{-1}))$ des séries de Laurent

formelles, la valuation ν se prolongeant à $\mathbb{K}_\infty$ par

$$\nu\Big(\sum_{s=-\infty}^{+\infty} a_s X^s\Big) = -\sup\{r \in \mathbb{Z} \mid a_r \neq 0\}\,.$$

Soit ψ le caractère du groupe additif de $\mathbb{F}_q$ défini par

$$\psi(x) = (-1)^{\mathrm{tr}(x)}$$

où tr est la trace de l'extension $\mathbb{F}_q|\mathbb{F}_2$. On associe au caractère non trivial ψ, le caractère E du groupe additif de $\mathbb{K}_\infty$ défini par la relation

$$E\Big(\sum_{s=-\infty}^{+\infty} a_s X^s\Big) = \psi(a_{-1})\,.$$

Soit un entier $n > 0$. On définit une application f de $\mathbb{F}_q((X^{-1}))$ dans $\mathbb{Z}$ par

$$f(t) = \sum_{\substack{A\in\mathbb{A}\\ \deg A\leq n}} E(tA^3)\,.$$

Dans ce qui suit, nous établissons une majoration non triviale des sommes $f(t)$ pour des séries formelles t "mal approchées" par des fractions rationnelles. Ces séries correspondent aux arcs mineurs de la méthode du cercle. Plus précisément, nous démontrons le théorème suivant.

THÉORÈME. *Soit un nombre réel $\varepsilon > 0$. Soit un entier $n > 0$. Soient H et G des polynômes premiers entre eux et $u \in \mathbb{K}_\infty$ tels que*

$$\deg H \leq n\,, \tag{i}$$

$$n + \deg H < \nu(u) \leq 2n + \deg H\,. \tag{ii}$$

Alors, on a

$$\Big|\sum_{\substack{A\in\mathbb{A}\\ \deg A\leq n}} E\Big(\Big(\frac{G}{H} + u\Big)A^3\Big)\Big| \ll q^{n(5/6+\varepsilon)}\,,$$

la constante impliquée par le symbole $\ll$ ne dépendant que de q et de ε.

Notons que la majoration triviale est $|f(t)| \leq q^{n+1}$et que dans [2], la majoration obtenue sous les mêmes hypothèses était $|f(G/H + u)| \ll q^{19n/20}$. C'est l'étude minutieuse des sommes $S(H, G, K)$ qui sera faite au paragraphe II qui permet d'améliorer les résultats établis en [2]. Il est à noter que les résultats relatifs aux sommes $S(H, G, K)$ sont en eux mêmes très intéressants.

I. Résultats auxiliaires

I.1. *Notations et conventions.* Dans ce qui suit, le mot polynôme désignera un élément de $\mathbb{A} = \mathbb{F}_q[X]$. L'ensemble des polynômes irréductibles unitaires sera noté $\mathcal{I}$. L'idéal principal de $\mathbb{A}$ engendré par le polynôme H sera noté (H).

On notera $\mathbb{A}_n$ l'ensemble des polynômes de $\mathbb{A}$ de degré au plus n et $\mathbb{B}_{n,m}$ l'ensemble des polynômes de $\mathbb{A}_n$ divisibles par X^m.

Soit H un polynôme non nul. L'ensemble des polynômes de degré strictement inférieur à $\deg H$ identifié à l'ensemble des classes de congruence modulo H sera noté $\boldsymbol{C}_H$, l'ensemble des polynômes de $\boldsymbol{C}_H$ inversibles modulo H sera noté $\boldsymbol{C}_H^*$.

A la valuation à l'infini $\nu = \nu_\infty$ est associée la valeur absolue $|\ |_\infty$ définie par

$$|a|_\infty = q^{-\nu(a)} \quad \text{si } a \neq 0, \qquad |0|_\infty = 0\,.$$

Nous noterons $|\ |$ cette valeur absolue car le contexte permet de la distinguer aisément de la valeur absolue de $\mathbb{R}$ qui sera aussi utilisée.

Si $u \in \mathbb{K}_\infty$, et si

$$u = \sum_{s=-\infty}^{+\infty} u_s X^s$$

on pose

$$\mathrm{Res}(u) = u_{-1}\,.$$

Si, de plus, $u \neq 0$, on pose

$$\mathrm{sgn}(u) = u_{-\nu(u)}\,.$$

De façon générale, on note B^* l'ensemble des éléments non nuls d'un ensemble B contenant 0 et si B est un ensemble fini, on note $\#B$ le nombre d'éléments de B.

I.2. *Le caractère E et la mesure de Haar dt.* On définit un caractère E de $\mathbb{K}_\infty$ en posant

$$E(y) = \psi(\mathrm{Res}(y))\,. \tag{I.1}$$

Le caractère ψ de $\mathbb{F}_q$ étant non trivial, il existe $\alpha \in \mathbb{F}_q$ tel que

$$\psi(\alpha) = -1\,, \tag{I.2}$$

et le caractère E est non trivial.

On désigne par $\mathcal{P}$ l'idéal de valuation de $\mathbb{K}_\infty$, et, pour tout entier rationnel j, par $\mathcal{P}_j$ l'idéal $\{t \in \mathbb{K}_\infty \mid \nu(t) > j\}$. i

Les ensembles $\mathcal{P}_j$ sont des sous-groupes compacts du groupe additif localement compact $\mathbb{K}_\infty$. Tout élément u de K_∞ s'écrit de façon unique

comme somme

$$u = [u] + \{u\}, \qquad [u] \in \mathbb{A}, \qquad \{u\} \in \mathcal{P}\,. \tag{I.3}$$

On utilisera aussi la notation $[y]$ pour désigner la partie entière d'un nombre réel y, mais il y a peu de risque de confusion.

On désigne par dt la mesure de Haar sur $\mathbb{K}_\infty$ normalisée à 1 sur l'idéal de valuation $\mathcal{P}$.

Les quatre propositions suivantes ont été établies dans [3] ou se démontrent de façon identique. Nous n'en donnons pas la démonstration.

PROPOSITION I.1. *Pour tout entier rationnel j, $\mathcal{P}_j$ a pour mesure q^{-j}.*

PROPOSITION I.2. (i) *On a $E(H) = 1$ pour tout $H \in \mathbb{A}$.*

(ii) *Pour tout polynôme H non nul, si A et B sont des polynômes congrus modulo H, on a*

$$E\left(\frac{A}{H}\right) = E\left(\frac{B}{H}\right).$$

(iii) *Pour $u \in \mathbb{K}_\infty$, on a l'implication*

$$\nu(u) \geq 2 \;\Rightarrow\; E(u) = 1\,. \tag{I.4}$$

PROPOSITION I.3. *Soient j un entier rationnel et $u \in \mathbb{K}_\infty$. Alors, on a*

$$\int_{\mathcal{P}_j} E(ut)\,dt = \begin{cases} q^{-j} & \text{si } \nu(u) > -j, \\ 0 & \text{sinon.} \end{cases} \tag{I.5}$$

PROPOSITION I.4. *Soit un entier $j > 0$ et soit $u \in \mathbb{K}_\infty$. Alors, on a*

$$\sum_{B \in \mathbb{A}_j} E(uB) = \begin{cases} q^{j+1} & \text{si } \nu(\{u\}) > j+1, \\ 0 & \text{sinon.} \end{cases} \tag{I.6}$$

Cette proposition admet le corollaire suivant que nous utiliserons fréquemment.

COROLLAIRE I.5. *Soient H un polynôme non nul et G un polynôme. Alors, on a*

$$\sum_{R \in \mathsf{C}_H} E\left(\frac{G}{H}R\right) = \begin{cases} |H| & \text{si } H \text{ divise } G, \\ 0 & \text{sinon.} \end{cases} \tag{I.7}$$

La proposition suivante donne une formule de "changement de variable" dans les intégrales.

PROPOSITION I.6 *Soient $a_0, a_1, \ldots, a_d$ des éléments de $\mathbb{K}_\infty$ et F l'application de $\mathbb{K}_\infty$ dans $\mathbb{K}_\infty$ définie par*

$$F(t) = a_0 + a_1 t + \ldots + a_d t^d\,.$$

Alors, pour tout entier rationnel j, pour tout $y \in \mathbb{K}_\infty^*$, on a

$$|y| \int_{\mathcal{P}_j} E(F(ty))\,dt = \int_{\mathcal{P}_{j+\nu(y)}} E(F(t))\,dt\,. \tag{I.8}$$

Démonstration. L'application $t \mapsto ty$ est un automorphisme du groupe additif $\mathbb{K}_\infty$. L'unicité de la mesure de Haar à constante multiplicative près donne l'existence d'une constante $c(y) > 0$ telle que pour toute fonction $g : \mathbb{K}_\infty \to \mathbb{C}$, localement sommable, pour toute partie compacte W de $\mathbb{K}_\infty$, on ait

$$\int_W g(ty)\,dt = c(y) \int_{yW} g(t)\,dt\,.$$

On prend pour g la fonction constante égale à 1 et pour W l'idéal de valuation $\mathcal{P}$. On obtient

$$c(y) = |y|^{-1}\,.$$

Pour avoir (I.8) il suffit de montrer que F est localement sommable. On montre qu'elle est localement constante. Soit

$$k = \max\left(2 - \nu(a_1), \left[\frac{4-\nu(a_2)}{2}\right], \ldots, \left[\frac{2+d-\nu(a_d)}{d}\right]\right).$$

Si $t \in \mathcal{P}_{k-1}$, $\nu(a_1 t + \ldots + a_d t^d) \geq 2$, et (I.4) nous donne $E(F(t)) = E(F(0))$.

Tous ces résultats sont vrais en caractéristique quelconque, la relation (I.2) s'écrivant alors $\psi(\alpha) \neq 1$. Ce qui va suivre est propre à la caractéristique 2.

Proposition I.7. *Soient $\mathbb{G}$ un sous-groupe additif de $\mathbb{K}_\infty$, $a \in \mathbb{K}_\infty$ et $b \in \mathbb{K}_\infty$. Alors, on a*

$$\sum_{G \in \mathbb{G}} E(aG^2 + bG) \in \{0, \#\mathbb{G}\}\,. \tag{I.9}$$

Démonstration. Désignons par $S = S(\mathbb{G}, a, b)$ la somme ci-dessus. On a

$$S^2 = \sum_{G \in \mathbb{G}} \sum_{H \in \mathbb{G}} E(a(G^2 + H^2) + b(G + H))\,.$$

Comme on est en caractéristique 2,

$$S^2 = \sum_{G \in \mathbb{G}} \sum_{H \in \mathbb{G}} E(a(G + H)^2 + b(G + H))\,.$$

Comme G est un sous-groupe de $\mathbb{K}_\infty$, on a $S^2 = \#\mathbb{G}S$, d'où le résultat annoncé.

Proposition I.8. *Soient k un entier rationnel, a et b des éléments de $\mathbb{K}_\infty$. Alors, on a*

$$\int_{\mathcal{P}_k} E(at^2+bt)\,dt \in \{0, q^{-k}\}\,. \tag{I.10}$$

Démonstration. Comme on est en caractéristique 2, l'application $t \mapsto E(at^2+bt)$ est un caractère du groupe additif de $\mathbb{K}_\infty$ et (I.10) est alors due à l'invariance de la mesure de Haar par translation.

La démonstration de la proposition suivante demande un lemme préliminaire. En vue d'une utilisation ultérieure, nous démontrons ce lemme sous une forme plus générale que celle nécessitée par son utilisation immédiate.

Lemme I.9. *Soit Q une puissance de 2 et ψ_Q le caractère additif de $\mathbb{F}_Q$ défini par*

$$\psi_Q(y) = (-1)^{\mathrm{tr}_{\mathbb{F}_Q|\mathbb{F}_2}(y)}\,.$$

Pour a et b dans $\mathbb{F}_Q$, soit

$$\sigma_Q(a,b) = \sum_{a\in\mathbb{F}_Q} \psi_Q(ay^2+by)\,.$$

Alors, $\sigma_Q(a,b) \in \{0, Q\}$ et $\sigma_Q(a,b) = Q$ si et seulement si $a = b^2$.

Démonstration. La première assertion se démontre comme la relation (I.9). Soit $b \in \mathbb{F}_Q$. Alors, on a

$$\sum_{a\in\mathbb{F}_Q} \sigma_Q(a,b) = \sum_{y\in\mathbb{F}_Q} \psi_Q(by) \sum_{a\in\mathbb{F}_Q} \psi_Q(ay^2) = \psi_Q(0)Q = Q\,.$$

Il existe un seul élément $a \in \mathbb{F}_Q$ tel que $\sigma_Q(a,b) = Q$. Montrons que b^2 est cet élément. C'est évident si $b = 0$. On suppose $b \neq 0$. Pour tout $z \in \mathbb{F}_Q$, on a $\mathrm{tr}_{\mathbb{F}_Q|\mathbb{F}_2}(z) = \mathrm{tr}_{\mathbb{F}_Q|\mathbb{F}_2}(z^2)$, d'où $\psi_Q(b^2z^2+bz) = 1$, ce qui donne $\sigma_Q(b^2,b) = Q$.

Proposition I.10. *Soient a et b des éléments de $\mathbb{K}_\infty$ et*

$$I(a,b) = \int_{\mathcal{P}} E(at^2+bt)\,dt\,. \tag{I.11}$$

Alors, $I(a,b) = 1$ si et seulement si $[a] - X[b]^2$ est carré dans $\mathbb{A}$.

Démonstration. Soient $A = [a]$ et $B = [b]$. Pour $t \in \mathcal{P}$, on a $\nu(\{a\}t^2) \geq 3$ et $\nu(\{b\}t) \geq 2$, d'où avec (I.4), $E(\{a\}t^2 + \{b\}t) = 1$, et

$$I(a,b) = I(A,B)\,. \tag{i}$$

Le polynôme A s'écrit de façon unique comme somme

$$A = U^2 + XV^2\,, \tag{ii}$$

U et V étant des polynômes.

Pour tout $t \in \mathcal{P}$, $\mathrm{Res}(U^2t^2) = 0$, et, d'après (I.1), $E(U^2t^2) = 1$, d'où

$$E(At^2 + Bt) = E(XV^2t^2 + Bt)\,,$$

et

$$I(a,b) = I(XV^2, B)\,. \tag{iii}$$

On a trivialement $I(0,0) = 1$. D'autre part, soit V un polynôme non nul de degré d. Il existe $\beta \in \mathbb{F}_q$ tel que $\beta^2 = \alpha$, α vérifiant (I.2). Soit $y = \beta\,\mathrm{sgn}(V)^{-1}X^{-d-1}$. Alors $y \in \mathcal{P}$, $\mathrm{Res}(XV^2y^2) = \beta^2 = \alpha$ et $E(XV^2y^2) = \psi(\alpha) = -1$. Le changement de variable $u = t + y$ dans l'intégrale $I(XV^2, 0)$ donne

$$I(XV^2, 0) = E(XV^2y^2)I(XV^2, 0) = -I(XV^2, 0)\,,$$

d'où $I(XV^2, 0) = 0$. On a donc $I(XV^2, 0) = 1$ si et seulement si $V = 0$. De même, avec (I.5), on a $I(0, B) = 1$ si et seulement si $B = 0$. Dans ce qui suit on suppose $B \neq 0$ et $V \neq 0$. Soit

$$N = \max(1 + \deg V, 1 + \deg B)\,.$$

Si $\nu(t) > N$, $\nu(tB) \geq 1 + N - \deg B \geq 2$, $\nu(t^2XV^2) \geq 1 + 2N - \deg V \geq 3$, et $E(XV^2t^2 + Bt) = 1$. Tout élément $t \in \mathcal{P}$ s'écrit de façon unique comme somme

$$t = t_{-1}X^{-1} + \ldots + t_{-N}X^{-N} + z, \quad t_{-1} \in \mathbb{F}_q, \ldots, t_{-N} \in \mathbb{F}_q, \quad z \in \mathcal{P}_N\,.$$

Avec (I.4) et la proposition I.1, on a

$$I(XV^2, B) = q^{-N} \sum_{t_{-1} \in \mathbb{F}_q} \ldots \sum_{t_{-N} \in \mathbb{F}_q} E\Big(XV^2\Big(\sum_{i=1}^{N} t_{-i}X^{-i}\Big)^2 + B\Big(\sum_{i=1}^{N} t_{-i}X^{-i}\Big)\Big)\,.$$

Quitte à introduire des coefficients b_j et v_j nuls, on peut poser

$$V = v_0 + v_1X + \ldots + v_{N-1}X^{N-1}, \qquad B = b_0 + b_1X + \ldots + b_{N-1}X^{N-1}\,.$$

On a alors

$$\mathrm{Res}\,\Big(XV^2\Big(\sum_{i=1}^{N} t_{-i}X^{-i}\Big)^2\Big) = \sum_{i=1}^{N} t_{-i}^2 v_{i-1}^2\,,$$

$$\mathrm{Res}\,\Big(B\sum_{i=1}^{N} t_{-i}X^{-i}\Big) = \sum_{i=1}^{N} t_{-i}b_{i-1}\,,$$

d'où

$$I(XV^2, B) = q^{-N} \sum_{t_{-1} \in \mathbb{F}_q} \ldots \sum_{t_{-N} \in \mathbb{F}_q} \psi\Big(\sum_{i=1}^{N} v_{i-1}^2 t_{-i}^2 + b_{i-1}t_{-i}\Big)$$

$$= q^{-N} \prod_{i=1}^{N} \Big(\sum_{t_{-i} \in \mathbb{F}_q} \psi\Big(\sum_{i=1}^{N} v_{i-1}^2 t_{-i}^2 + b_{i-1} t_{-i} \Big) \Big)$$

$$= q^{-N} \prod_{i=1}^{N} \sigma_q(v_{i-1}^2, b_{i-1}) \,.$$

D'après le lemme précédent, $I(XV^2, B) = 1$ si et seulement si $\sigma_q(v_{i-1}^2, b_{i-1}) = q$ pour tout $i = 1, \dots, N$, c'est-à-dire si $v_{i-1} = b_{i-1}$ pour tout $i = 1, \dots, N$. On a donc $I(XV^2, B) = 1$ si et seulement si $V = B$. Avec (ii) et (iii) on a alors $I(A, B) = 1$ si et seulement si $A + XB^2$ est un carré dans $\mathbb{A}$. On conclut avec (i).

II. Les sommes $S(H, G, K)$. Soient $H \in \mathbb{A}$ unitaire, $G \in \mathbb{A}$ premier à H. Pour $K \in \mathbb{A}$, on pose

$$S(H, G, K) = \sum_{R \in \mathsf{C}_H} E\Big(\frac{GR^3 + KR}{H} \Big) \,. \tag{II.1}$$

L'étude des sommes $S(H, G, K)$ conduit à l'étude des sommes doubles

$$W(H, G) = \sum_{R \in \mathsf{C}_H} \sum_{Q \in \mathsf{C}_H} E\Big(\frac{G}{H} (R^2 Q + R Q^2) \Big) \,. \tag{II.2}$$

On montre dans ce paragraphe que $S(H, G, K)^2$ ne peut prendre que les valeurs 0 ou $W(H, G)$, on calcule $W(H, G)$ et on précise la répartition modulo H des polynômes K tels que $S(H, G, K) \neq 0$.

Dans $W(H, G)$ la somme intérieure apparaît comme le cas particulier $T(H, G, G, R)$ de la somme

$$T(H, A, B, R) = \sum_{Q \in \mathsf{C}_H} E\Big(\frac{AR^2 Q + BRQ^2}{H} \Big) \tag{II.3}$$

définie pour tout couple (A, B) de polynômes premiers à H.

La proposition I.7 s'applique à la somme $T(H, A, B, R)$ qui ne peut donc prendre que les valeurs 0 ou $|H|$. On désigne par $\mathcal{R}(H, A, B)$ l'ensemble des $R \in \boldsymbol{C}_H$ tels que $T(H, A, B, R) = |H|$. On notera $\mathcal{R}(H, G)$ l'ensemble $\mathcal{R}(H, G, G)$. On aura donc

$$W(H, G) = |H| \# \mathcal{R}(H, G) \,. \tag{II.4}$$

Proposition II.1. *Pour tout couple (A, B) de polynômes premiers à H, l'ensemble $\mathcal{R}(H, A, B)$ est un sous-groupe du groupe additif $\boldsymbol{C}_H$.*

Démonstration. Immédiate.

Proposition II.2. *Soient $P_1, \dots, P_r$ des polynômes irréductibles unitaires deux à deux distincts, $m_1, \dots, m_r$ des entiers strictement positifs et*

G un polynôme premier au produit $P_1 \times \ldots \times P_r$. Soit K un polynôme. Alors, on a

$$W\Big(\prod_{i=1}^{r} P_i^{m_i}, G\Big) = \prod_{i=1}^{r} W\Big(P_i^{m_i}, G \prod_{\substack{j=1\\ j\neq i}}^{r} P_j^{2m_j}\Big)\,, \tag{II.5}$$

$$S\Big(\prod_{i=1}^{r} P_i^{m_i}, G, K\Big) = \prod_{i=1}^{r} S\Big(P_i^{m_i}, G \prod_{\substack{j=1\\ j\neq i}}^{r} P_j^{2m_j}, K\Big)\,, \tag{II.6}$$

$$T\Big(\prod_{i=1}^{r} P_i^{m_i}, G, G, K\Big) = \prod_{i=1}^{r} T\Big(P_i^{m_i}, G, G \prod_{\substack{j=1\\ j\neq i}}^{r} P_j^{m_j}, K\Big)\,. \tag{II.7}$$

Démonstration. Si $r = 2$, on utilise l'isomorphisme canonique $(Q_1, Q_2) \mapsto H_2Q_1 + H_1Q_2$ de $\boldsymbol{C}_{H_1} \times \boldsymbol{C}_{H_2}$ sur $\boldsymbol{C}_{H_1H_2}$ lorsque H_1 et H_2 sont des polynômes premiers entre eux. Ensuite, on procède par récurrence sur l'entier r.

Lemme II.3. *Soient H un polynôme unitaire et G un polynôme premier à H. Alors, pour tout $K \in \mathbb{A}$, on a*

$$S^2(H, G, K) = |H| \sum_{R \in \mathcal{R}(H,G)} E\Big(\frac{GR^3 + KR}{H}\Big)\,. \tag{II.8}$$

Démonstration. En utilisant la structure de groupe de $\boldsymbol{C}_H$ on obtient aisément l'égalité

$$S^2(H, G, K) = |H| \sum_{R \in \mathsf{C}_H} \sum_{Q \in \mathsf{C}_H} E\Big(\frac{GR^3 + KR}{H}\Big) E\Big(\frac{G}{H}(R^2Q + RQ^2)\Big)\,,$$

$$S^2(H, G, K) = \sum_{R \in \mathsf{C}_H} E\Big(\frac{GR^3 + KR}{H}\Big) T(H, G, G, R)\,,$$

et (II.8) se déduit de la définition de $\mathcal{R}(H, G)$.

Proposition II.4. *Soient H un polynôme unitaire, G un polynôme premier à H et $K \in \mathbb{A}$. Alors, on a*

$$S^2(H, G, K) \in \{0, W(H, G)\}\,. \tag{II.9}$$

De plus, $S(H, G, K) \neq 0$ si et seulement si pour tout $R \in \mathcal{R}(H, G)$, $E\Big(\frac{GR^3+KR}{H}\Big) = 1$.

Démonstration. On pose $\mathcal{R} = \mathcal{R}(H, G)$. En utilisant le fait que $\mathcal{R}$ est un sous-groupe de $\boldsymbol{C}_H$, on obtient à l'aide du lemme précédent

que

$$S^4(H,G,K) = |H|^2 \sum_{R\in\mathcal{R}} \sum_{Q\in\mathcal{R}} E\Big(\frac{GR^3+KR+G(R^2Q+RQ^2)}{H}\Big).$$

Pour $R \in \mathcal{R}$ et $Q \in \boldsymbol{C}_H$, on a $E\Big(\frac{G}{H}(R^2Q+RQ^2)\Big) = 1$. On a aussi l'inclusion $\mathcal{R} \subset \boldsymbol{C}_H$, d'où

$$S^4(H,G,K) = |H|^2 \sum_{R\in\mathcal{R}} E\Big(\frac{GR^3+KR}{H}\Big)\#\mathcal{R}.$$

Avec (II.8), on a$S^4(H,G,K) = |H|\#\mathcal{R}S^2(H,G,K)$, d'où,$S^2(H,G,K) \in \{0,|H|\#\mathcal{R}\}$. Compte tenu de la définition de $\mathcal{R} = \mathcal{R}(H,G)$ et de $W(H,G)$, on a là la relation (II.9). De plus, si $S(H,G,K) \neq 0$, $S^2(H,G,K) = |H|\#\mathcal{R}$, et, d'après (II.8),

$$\#\mathcal{R} = \sum_{R\in\mathcal{R}} E\Big(\frac{GR^3+KR}{H}\Big),$$

ce qui implique que chaque terme de la somme ci-dessus est égal à 1.

Proposition II.5. *Soient P un polynôme irréductible unitaire et G un polynôme premier à P. Alors, on a*

$$W(P,G) = \begin{cases} 2|P| & \textit{si } 3 \textit{ ne divise pas } |P|-1\,, \\ |P| \textit{ ou } 4|P| & \textit{si } 3 \textit{ divise } |P|-1. \end{cases} \tag{II.10}$$

Démonstration. Les caractères du groupe additif du corps $\mathbb{F}_{|P|} = \mathbb{A}/(P)$ sont les applications $Q \mapsto \psi_{|P|}(AQ)$, A décrivant $\mathbb{F}_{|P|}$, le caractère $\psi_{|P|}$ étant celui défini au lemme I.9 (cf. [5]). Par abus de notation, on identifie $\boldsymbol{C}_P$ au corps $\mathbb{F}_{|P|}$. L'application $Q \mapsto E(Q/P)$ est un caractère non trivial du groupe additif $\boldsymbol{C}_P$. Il existe $A \in \boldsymbol{C}_P^*$ tel que pour tout $Q \in \boldsymbol{C}_P$, on ait $E(Q/P) = \psi_{|P|}(AQ)$. On peut donc écrire

$$W(P,G) = \sum_{R\in\mathbb{F}_{|P|}} \sum_{Q\in\mathbb{F}_{|P|}} \psi_{|P|}(AG(R^2Q+RQ^2)) = \sum_{R\in\mathbb{F}_{|P|}} \sigma_{|P|}(AGR, AGR^2),$$

$\sigma_{|P|}$ étant la somme définie au lemme I.9. D'après ce lemme,

$$W(P,G) = |P|\#\{R \in \mathbb{F}_{|P|} \mid AGR = (AGR^2)^2\}\,,$$

d'où,

$$W(P,G) = |P|\#\{R \in \boldsymbol{C}_P \mid R \equiv AGR^4 \bmod P\}\,.$$

La congruence

$$R \equiv AGR^4 \bmod P \tag{i}$$

admet la solution triviale $R \equiv 0$. Elle admet une solution $R \not\equiv 0 \bmod P$ si et seulement si $1 \equiv AGR^3 \bmod P$. Si 3 et $|P|-1$ sont premiers entre eux, tout élément de $\mathbb{F}_{|P|}$ est un cube, la congruence (i) admet une et une seule

solution non nulle et $W(P,G) = 2|P|$. Si 3 divise $|P|-1$, la congruence (i) admet soit 3 soit 0 solutions non nulles suivant que AG est ou n'est pas cube modulo P. Dans ce cas $W(P,G)$ vaut $4|P|$ ou $|P|$.

PROPOSITION II.6. *Soient P un polynôme irréductible unitaire, G un polynôme premier à P et un entier $k \geq 0$. Alors, on a*

$$W(P^{k+3},G) = |P|^4 W(P^k,G)\,, \tag{II.11}$$

$$W(P^{3k},G) = |P|^{4k}\,, \tag{II.12}$$

$$W(P^{3k+1},G) = |P|^{4k} W(P,G)\,, \tag{II.13}$$

$$W(P^{3k+2},G) = |P|^{4k+2}\,. \tag{II.14}$$

Démonstration. Soit un entier $k \geq -1$. Alors,

$$W(P^{k+3},G) = \sum_{R \in \mathsf{C}_{P^{k+3}}} \sum_{Q \in \mathsf{C}_{P^{k+3}}} E\Big(\frac{G(R^2Q+RQ^2)}{P^{k+3}}\Big)\,.$$

On divise R et Q par P^{k+2}. Il vient

$$W(P^{k+3},G) =$$

$$\sum_{\substack{U \in \mathsf{C}_{P^{k+2}} \\ V \in \mathsf{C}_P}} \sum_{\substack{Y \in \mathsf{C}_{P^{k+2}} \\ Z \in \mathsf{C}_P}} E\Big(\frac{G(U^2Y+U^2P^{k+2}Z+UY^2+P^{k+2}VY^2)}{P^{k+3}}\Big) =$$

$$\sum_{U \in \mathsf{C}_{P^{k+2}}} \sum_{Y \in \mathsf{C}_{P^{k+2}}} E\Big(\frac{G(U^2Y+UY^2)}{P^{k+3}}\Big) \sum_{V \in \mathsf{C}_P} E\Big(\frac{GY^2V}{P}\Big) \sum_{Z \in \mathsf{C}_P} E\Big(\frac{GU^2Z}{P}\Big),$$

d'où avec (I.7),

$$W(P^{k+3},G) = \sum_{\substack{U \in \mathsf{C}_{P^{k+2}} \\ P|U}} \sum_{\substack{Y \in \mathsf{C}_{P^{k+2}} \\ P|Y}} E\Big(\frac{G(U^2Y+UY^2)}{P^{k+3}}\Big)|P|^2\,.$$

Pour $k=-1$, cette relation s'écrit

$$W(P^2,G) = |P|^2\,. \tag{i}$$

Pour $k \geq 0$, on a

$$W(P^{k+3},G) = |P|^2 \sum_{S \in \mathsf{C}_{P^{k+1}}} \sum_{T \in \mathsf{C}_{P^{k+1}}} E\Big(\frac{G(S^2T+ST^2)}{P^k}\Big)\,.$$

On divise les S et T de la somme ci-dessus par P^k. Il vient

$$W(P^{k+3},G) = |P|^4 \sum_{R \in \mathsf{C}_{P^k}} \sum_{Q \in \mathsf{C}_{P^k}} E\Big(\frac{G(R^2Q+RQ^2)}{P^k}\Big)\,,$$

d'où, pour $k=0$,

$$W(P^{k+3},G) = |P|^4\,, \tag{ii}$$

et, pour $k > 0$,

(iii) $$W(P^{k+3}, G) = |P|^4 W(P^k, G)\,.$$

C'est là la relation (II.11) annoncée. Les relations (II.12)–(II.14) se déduisent des égalités (i)–(iii) par récurrence sur k.

Nous allons préciser maintenant la structure des groupes $\mathcal{R}(H, G, A)$.

Proposition II.7. *Soient P un polynôme irréductible unitaire, G et A des polynômes premiers à P et un entier $m \geq 1$. Alors, on a*

(II.15) $$\mathcal{R}(P^{3m}, G, A) \subset (P^m)\,,$$

(II.16) $$\mathcal{R}(P^{3m-1}, G, A) \subset (P^{m+1})\,,$$

(II.17) $$\mathcal{R}(P^{3m-2}, G, A) \subset (P^{m-1})\,,$$

(II.18) $$\#\{\mathcal{R}(P^{3m-2}, G, A) \cap (P^m)\} = |P|^{m-1}\,.$$

Démonstration. Les relations (II.17) et (II.18) sont triviales pour $m = 1$. Soit un entier $k \geq 2$. Soit $R \in \mathcal{R}(P^k, G, A)$. Alors,

(i) $$E\left(\frac{GRQ^2 + AR^2Q}{P^k}\right) = 1 \quad \text{pour tout } Q \in \boldsymbol{C}_{P^k}\,.$$

En particulier, si $Z \in \boldsymbol{C}_P$,

$$E\left(\frac{GR(P^{k-1}Z)^2 + AR^2P^{k-1}Z}{P^k}\right) = 1 \quad \text{et} \quad E\left(\frac{AR^2Z}{P}\right) = 1\,,$$

d'où

$$|P| = \sum_{Z \in \mathsf{C}_P} E\left(\frac{AR^2Z}{P}\right).$$

D'après (I.7), P divise R. Posons $R = PB$. Si $k = 2$, l'égalité (i) nous donne pour tout $Q \in \boldsymbol{C}_P$

$$1 = E\left(\frac{GPBQ^2 + A(PB)^2Q}{P^2}\right) = E\left(\frac{GBQ^2}{P}\right).$$

Dans le corps $\mathbb{F}_{|P|}$ tout élément est un carré. L'application $Q \mapsto Q^2$ est une bijection de $\boldsymbol{C}_P$ sur lui même. On a donc $E\left(\frac{GBZ}{P}\right) = 1$ pour tout $Z \in \boldsymbol{C}_P$. Comme ci-dessus, celà entraîne que P divise B et que P^2 divise R, ce qui démontre (II.16) pour $m = 1$. Supposons maintenant $k \geq 3$. La relation (i) nous donne pour tout $H \in \boldsymbol{C}_{P^{k-3}}$,

$$1 = E\left(\frac{GPB(PH)^2 + A(PB)^2(PH)}{P^k}\right) = E\left(\frac{GBH^2 + AB^2H}{P^{k-3}}\right),$$

par suite, $T(P^{k-3}, G, A, B) = |P|^{k-3}$ et le reste de B modulo P^{k-3} appartient à $\mathcal{R}(P^{k-3}, G, A)$. On a donc l'inclusion

(ii) $$\mathcal{R}(P^k, G, A) \subset \mathcal{R}(P^{k-3}, G, A)P + (P^{k-2})\,.$$

Avec $k = 3$, la relation (ii) nous donne (II.15) pour $m = 1$. Ensuite, la relation (ii) permet d'établir les relations (II.15)–(II.17) par récurrence sur l'entier m. Désignons, pour tout entier $m \geq 0$, par $\mathcal{B}_m$ l'ensemble des polynômes $B \in \boldsymbol{C}_{P^{2m}}$ tels que $BP^{m+1} \in \mathcal{R}(P^{3m+1}, G, A)$ et par β_m le nombre d'éléments de cet ensemble. La définition des ensembles $\mathcal{R}(H, G, A)$ nous donne l'équivalence

$$\text{(iii)} \qquad B \in \mathcal{B}_m \;\Leftrightarrow\; |P|^{3m+1} = \sum_{Q \in \mathsf{C}_{P^{3m+1}}} E\Big(\frac{GBQ^2}{P^{2m}} + \frac{AB^2Q}{P^{m-1}}\Big)\,.$$

Soit un entier $m \geq 1$. On a

$$\begin{aligned}
&\beta_m |P|^{3m+1} \\
&\quad = \sum_{B \in \mathsf{C}_{P^{2m}}} \sum_{Q \in \mathsf{C}_{P^{3m+1}}} E\Big(\frac{GBQ^2}{P^{2m}} + \frac{AB^2Q}{P^{m-1}}\Big) \\
&\quad = \sum_{B \in \mathsf{C}_{P^{2m}}} \sum_{Y \in \mathsf{C}_P} \sum_{Z \in \mathsf{C}_{P^{3m}}} E\Big(\frac{GB(Y+PZ)^2}{P^{2m}} + \frac{AB^2(Y+PZ)}{P^{m-1}}\Big) \\
&\quad = \sum_{B \in \mathsf{C}_{P^{2m}}} \sum_{Y \in \mathsf{C}_P} E\Big(\frac{GBY^2}{P^{2m}} + \frac{AB^2Y}{P^{m-1}}\Big) \sum_{Z \in \mathsf{C}_{P^{3m}}} E\Big(\frac{GBZ^2}{P^{2m-2}} + \frac{AB^2Z}{P^{m-2}}\Big)\,.
\end{aligned}$$

La somme intérieure vaut 0 ou $|P|^{3m}$. D'après (iii), elle vaut $|P|^{3m}$ si et seulement si le reste de B modulo P^{2m-2} appartient à $\mathcal{B}_{m-1}$, d'où

$$\begin{aligned}
&\beta_m |P|^{3m+1} = \\
&|P|^{3m} \sum_{B \in \mathcal{B}_{m-1}} \sum_{L \in \mathsf{C}_{P^2}} \sum_{Y \in \mathsf{C}_P} E\Big(\frac{G(B+LP^{2m-2})Y^2}{P^{2m}} + \frac{A(B+LP^{2m-2})^2Y}{P^{m-1}}\Big), \\
&\beta_m |P| = \sum_{B \in \mathcal{B}_{m-1}} \sum_{Y \in \mathsf{C}_P} E\Big(\frac{GBY^2}{P^{2m}} + \frac{ABY}{P^{m-1}}\Big) \sum_{L \in \mathsf{C}_{P^2}} E\Big(\frac{GLY^2}{P^2}\Big)\,.
\end{aligned}$$

Avec (I.7) on a $\beta_m |P| = |P|^2 \# \mathcal{B}_{m-1} = |P|^2 \beta_{m-1}$, d'où la relation de récurrence$\beta_m = |P| \beta_{m-1}$ qui établit (II.18).

On introduit les fonctions multiplicatives ϕ et λ définies sur l'ensemble des polynômes unitaires par

$$\text{(II.19)} \qquad \phi(P^{3m+r}) = P^{m+r} \quad \text{si } r = 0, 1, 2\,,$$

$$\text{(II.20)} \qquad \lambda(P^{3m}) = \lambda(P^{3m+2}) = 1\,,$$

$$\text{(II.21)} \qquad \lambda(P^{3m+1}) = W(P, G)|P|^{-1}\,,$$

valables pour tout polynôme irréductible unitaire P et tout entier $m \geq 0$. La proposition II.7 admet alors le corollaire suivant:

Corollaire II.8. *Soient H un polynôme unitaire et G un polynôme premier à H. Alors, on a*

$$\#\mathcal{R}(H,G) = \lambda(H)\#(\mathcal{R}(H,G)\cap(\phi(H)))\,. \tag{II.22}$$

Démonstration. Immédiate avec (II.4), (II.5), (II.13), (II.15), (II.16) et (II.18)–(II.21).

Proposition II.9. *Soient H un polynôme unitaire et G un polynôme premier à H. Soit $\mathcal{R}(H,G)^\perp$ l'ensemble des polynômes $L\in\boldsymbol{C}_H$ tels que*

$$E\Big(\frac{RL}{H}\Big) = 1 \quad \text{pour tout } R\in\mathcal{R}(H,G)\,.$$

Alors, $\mathcal{R}(H,G)^\perp$ est un sous-groupe additif de $\boldsymbol{C}_H$ et on a la relation

$$|H| = \#\mathcal{R}(H,G)\#\mathcal{R}(H,G)^\perp\,. \tag{II.23}$$

Pour tout $R\in\boldsymbol{C}_H$, on a l'équivalence

$$R\in\mathcal{R}(H,G) \;\Leftrightarrow\; E\Big(\frac{LR}{H}\Big)=1 \text{ pour tout } L\in\mathcal{R}(H,G)^\perp\,. \tag{II.24}$$

Pour tout $K\in\boldsymbol{C}_H$ tel que $S(H,G,K)\neq 0$, tout $L\in\boldsymbol{C}_H$, on a l'équivalence

$$|S(H,G,K+L)| = |S(H,G,K)| \;\Leftrightarrow\; L\in\mathcal{R}(H,G)^\perp\,, \tag{II.25}$$

et, modulo $\mathcal{R}(H,G)^\perp$ il n'y a qu'un seul $K\in\boldsymbol{C}_H$ tel que $S(H,G,K)\neq 0$.

Démonstration. On a immédiatement que $\mathcal{R}(H,G)^\perp$ est un sous-groupe de $\boldsymbol{C}_H$ ainsi que (II.23) et (II.24). Soit $K\in\boldsymbol{C}_H$. D'après (II.8), $S(H,G,K)\neq 0$ si et seulement si $E\Big(\frac{GR^3+KR}{H}\Big)=1$ pour tout $R\in\mathcal{R}(H,G)$, d'où (II.25). Soit $Y(H)$, resp. $y(H)$, le nombre d'éléments $K\in\boldsymbol{C}_H$, resp. le nombre d'éléments $K\in\boldsymbol{C}_H$ distincts modulo $\mathcal{R}(H,G)^\perp$, tels que $S(H,G,K)\neq 0$. On a

$$Y(H) = y(H)\#\mathcal{R}(H,G)^\perp\,. \tag{i}$$

D'autre part, d'après (II.9), on a

$$Y(H)W(H,G) = \sum_{R\in\mathsf{C}_H} S(H,G,K)^2\,,$$

d'où, avec (II.4) et (II.8),

$$Y(H)|H|\#\mathcal{R}(H,G) = \sum_{K\in\mathsf{C}_H}|H|\sum_{R\in\mathcal{R}(H,G)}E\Big(\frac{GR^3+KR}{H}\Big)\,,$$

$$Y(H)\#\mathcal{R}(H,G) = \sum_{R\in\mathcal{R}(H,G)}E\Big(\frac{GR^3}{H}\Big)\sum_{K\in\mathsf{C}_H}E\Big(\frac{KR}{H}\Big)\,,$$

puis, avec (I.7),

$$Y(H)\#\mathcal{R}(H,G) = |H|\,. \tag{ii}$$

Les relations (i) et (II.23) nous donnent alors $y(H) = 1$.

PROPOSITION II.10. *Soit un nombre réel $\varrho > 0$. Soient H un polynôme unitaire, G un polynôme premier à H. Alors, on a*

$$W(H,G)^{1/2} \le a_1(q)|H|^{2/3}\,, \tag{II.26}$$

$$|H|^{1/6}|\phi(H)|^{-1/2}\lambda(H)^{1/2} \le a_2(q)\,, \tag{II.27}$$

$$\lambda(H)|H|^{5/6}W(H,G)^{-1/2}|\phi(H)|^{-1/2} \le a_1(q)\,, \tag{II.28}$$

$$\lambda(H)W(H,G)^{-1/2}|H|^{1/2} \le a_3(q,\varrho)|H|^{\varrho}\,, \tag{II.29}$$

$a_1(q)$, $a_2(q)$, $a_3(q,\varrho)$ étant les constantes définies par les relations

$$a_1(q)^2 = \Big(\prod_{\substack{P\in\mathcal{I}\\ |P|\not\equiv 1 \bmod 3\\ |P|\le 8}} 2|P|^{-1/3}\Big)\Big(\prod_{\substack{P\in\mathcal{I}\\ |P|\equiv 1 \bmod 3\\ |P|\le 64}} 4|P|^{-1/3}\Big)\,, \tag{II.30}$$

$$a_2(q)^2 = \Big(\prod_{\substack{P\in\mathcal{I}\\ |P|\not\equiv 1 \bmod 3\\ |P|^2\le 8}} 2|P|^{-2/3}\Big)\Big(\prod_{\substack{P\in\mathcal{I}\\ |P|\equiv 1 \bmod 3\\ |P|\le 8}} 4|P|^{-2/3}\Big)\,, \tag{II.31}$$

$$a_3(q,\varrho)^2 = \Big(\prod_{\substack{P\in\mathcal{I}\\ |P|\not\equiv 1 \bmod 3\\ |P|^{2\varrho}\le 2}} 2|P|^{-2\varrho}\Big)\Big(\prod_{\substack{P\in\mathcal{I}\\ |P|\equiv 1 \bmod 3\\ |P|^{2\varrho}\le 4}} 4|P|^{-2\varrho}\Big)\,. \tag{II.32}$$

Démonstration. Toutes ces relations se démontrent de façon similaire en utilisant la multiplicativité des fonctions considérées. Nous ne démontrerons ici que la dernière de ces relations. Posons

$$\alpha(H) = \lambda(H)W(H,G)^{-1/2}|H|^{1/2-\varrho}\,.$$

Avec (II.10), (II.12), (II.13), (II.14), (II.20) et (II.21), on a

$$\alpha(P^{3m}) = |P|^{-m(1/2+3\varrho)}\,, \quad \alpha(P^{3m+2}) = |P|^{-m(1/2+3\varrho)-2\varrho}\,,$$
$$\alpha(P^{3m+1}) = \lambda(P)^{1/2}|P|^{-m(1/2+3\varrho)-\varrho}\,,$$

d'où,

$$\alpha(H) \le \prod_{\substack{P\in\mathcal{I}\\ P|H\\ v_P(H)=3m+1}} \lambda(P)^{1/2}|P|^{-\varrho}\,,$$

$v_P(H)$ désignant la valuation P-adique de H.

Avec (II.10) et (II.21), on a

$$\lambda(P) = \begin{cases} 2 & \text{si } |P| \not\equiv 1 \bmod 3,\\ 1 \text{ ou } 4 & \text{si } |P| \equiv 1 \bmod 3, \end{cases}$$

d'où,

$$\alpha(H)^2 \le \Big(\prod_{\substack{P\in\mathcal{I}\\ |P|\not\equiv 1 \bmod 3\\ |P|^{2\varrho}\le 2}} 2|P|^{-2\varrho}\Big)\Big(\prod_{\substack{P\in\mathcal{I}\\ |P|\equiv 1 \bmod 3\\ |P|^{2\varrho}\le 4}} 4|P|^{-2\varrho}\Big),$$

ce qui est le résultat annoncé.

III. Les sommes $Y(u,\alpha)$ et les ensembles $\mathcal{A}(u)$. Soient $u \in \mathcal{P}$ et un entier n tels que

$$\nu(u) > n > 0\,. \tag{III.1}$$

Pour $\alpha \in \mathcal{P}$, on pose

$$Y(u,\alpha) = Y_n(u,\alpha) = \sum_{M\in\mathbb{A}_n} E(uM^3 + \alpha M)\,. \tag{III.2}$$

Comme au paragraphe précédent, on peut démontrer que $|Y(u,\alpha)|$ ne prend que les valeurs 0 ou $g(u)^{1/2}$, $g(u)$ étant la somme double

$$\sum_{A\in\mathbb{A}_n}\sum_{B\in\mathbb{A}_n} E(u(A^2B + AB^2))\,,$$

et étudier l'ensemble $\mathcal{B}(u)$ des polynômes $A \in \mathbb{A}_n$ tels que $E(u(A^2B + AB^2)) = 1$ pour tout $B \in \mathbb{A}_n$. L'étude de cet ensemble est aisée lorsque $\nu(u) > 2n+1$, plus délicate lorsque $\nu(u) \le 2n+1$ car la somme intérieure dans $g(u)$ ne peut plus être écrite sous forme d'une intégrale. Il est plus facile d'étudier un sous-ensemble $\mathcal{A}(u)$ de $\mathcal{B}(u)$. Il s'avère que cette étude sera suffisante pour nos calculs ultérieurs. On pose

$$\nu(u) = k = 3m + \varrho, \qquad \varrho \in \{-1,0,1\}\,. \tag{III.3}$$

On définit l'ensemble $\mathcal{A}(u)$ par la condition

$$\begin{aligned} &A \in \mathcal{A}(u)\\ &\quad\Leftrightarrow\ A \in \mathbb{A}_{m-1} \text{ et } E(u(A^2B + AB^2)) = 1 \text{ pour tout } B \in \mathbb{A}_n\,. \end{aligned} \tag{III.4}$$

Si $\nu(u) > 3n+1$, pour tout $M \in \mathbb{A}_n$, on a $\nu(uM^3) > 1$. D'après (I.4), $E(uM^3) = 1$. Dans ce cas les valeurs de $Y(u,\alpha)$ sont données par la proposition I.4. Dans ce qui suit, nous supposerons donc que

$$\nu(u) \le 3n+1\,, \tag{III.5}$$

ce qui implique

$$m \le n\,. \tag{III.6}$$

Proposition III.1. *Si $\nu(u) > 2n$, on a*

$$q^{n+1}\#\mathcal{A}(u) = \begin{cases} q^{2m+1} & \text{si } \nu(u) = 3m+1,\\ q^{2m} & \text{si } \nu(u) \ne 3m+1, \end{cases} \tag{III.7}$$

et, pour tout entier naturel $j < m$, on a l'implication

$$\nu(u) > 2n + 1 + j \;\Rightarrow \mathbb{A}_j \subset \mathcal{A}(u)\,. \tag{III.8}$$

D é m o n s t r a t i o n. Soit $j < m$ tel que $\nu(u) > 2n+1+j$. Si $A \in \mathbb{A}_j$ et $B \in \mathbb{A}_n$, $\nu(uAB^2) \geq 2$, $\nu(uA^2B) \geq 2$, et $E(u(A^2B+AB^2)) = 1$, d'où (III.8). On a

$$\begin{aligned} q^{n+1}\#\mathcal{A}(u) &= \sum_{A\in\mathbb{A}_{m-1}} \sum_{B\in\mathbb{A}_n} E(u(A^2B + AB^2)) \\ &= \sum_{B\in\mathbb{A}_n} \sum_{A\in\mathbb{A}_{m-1}} E(u(A^2B + AB^2)). \end{aligned}$$

Soient $B \in \mathbb{A}_n$ et $A \in \mathbb{A}_{m-1}$. Si $y \in \mathcal{P}$, $\nu(uBy^2) \geq 3$, $\nu(uB^2y) \geq 2$, et $E(u(A^2B + AB^2)) = E(u((A+y)^2B + (A+y)B^2))$. On a donc, pour tout $B \in \mathbb{A}_n$,

$$\sum_{A\in\mathbb{A}_{m-1}} E(u(A^2B + AB^2)) = \int\limits_{\nu(y)>-m} E(u(By^2 + B^2y))\,dy\,.$$

Avec (I.9), il vient

$$q^{n+1}\#\mathcal{A}(u) = q^m \sum_{B\in\mathbb{A}_n} J(u,B)\,,$$

où

$$J(u,B) = \int\limits_{\mathcal{P}} E(u(BX^{2m}t^2 + B^2X^m t))\,dt\,.$$

D'après la proposition I.10, $J(u,B) \neq 0$ si et seulement si $[uBX^{2m}] + X[uB^2X^m]^2$ est carré dans $\mathbb{A}$. Supposons $J(u,B) \neq 0$ et $[uBX^{2m}] \neq 0$, $[uB^2X^m] \neq 0$. On a

$$1 + 2\deg([uB^2X^m]) \leq \deg([uBX^{2m}])\,,$$

soit

$$1 + 3\deg B \leq \nu(u)\,.$$

Posons

$$\mu = m-1 \quad \text{si } k < 3m+1, \quad \mu = m \quad \text{si } k = 3m+1\,.$$

Alors, $B \in \mathbb{A}_\mu$. On vérifie aisément que si $J(u,B) \neq 0$ avec $[uBX^{2m}] = 0$ ou $[uB^2X^m] = 0$, $B \in \mathbb{A}_\mu$. Par suite,

$$q^{n+1}\#\mathcal{A}(u) = \sum_{B\in\mathbb{A}_\mu} \sum_{A\in\mathbb{A}_{m-1}} E(u(A^2B + AB^2))\,.$$

Si $B \in \mathbb{A}_\mu$, $A \in \mathbb{A}_{m-1}$, $\nu(u(A^2B + AB^2)) \geq k - 2\mu - m + 1 \geq 2$ et $E(u(A^2B + AB^2)) = 1$. On a donc

$$q^{n+1}\#\mathcal{A}(u) = q^{\mu+m+1}\,.$$

Proposition III.2. *Si* $\nu(u) \le 3n+1$, *pour tout* $\alpha \in \mathcal{P}$, *on a la majoration*

$$q^m|Y(u,\alpha)| \le q^{n+1} \sum_{B\in\mathcal{A}(u)} E(\alpha A)\,. \tag{III.9}$$

Si $\nu(u) > 2n+1$, *on a l'implication*

$$\nu(\alpha) < \nu(u) - 2n \;\Rightarrow\; Y(u,\alpha) = 0\,. \tag{III.10}$$

Démonstration. Avec (III.6) on peut écrire

$$Y(u,\alpha) = \sum_{B\in\mathbb{B}_{n,m}} \sum_{A\in\mathbb{A}_{m-1}} E(u(B+A)^3 + \alpha(B+A))\,,$$

d'où, avec (III.3),

$$Y(u,\alpha) = \sum_{B\in\mathbb{B}_{n,m}} E(uB^3+\alpha B) \sum_{A\in\mathbb{A}_{m-1}} E(u(B^2A+AB^2+\alpha A))\,.$$

La somme intérieure étant ≥ 0,

$$|Y(u,\alpha)| \le \sum_{B\in\mathbb{B}_{n,m}} \sum_{A\in\mathbb{A}_{m-1}} E(u(B^2A+BA^2)+\alpha A)\,. \tag{i}$$

Si $Y \in \mathbb{A}_{m-1}$, $A \in \mathbb{A}_{m-1}$, $E(u(Y^2A+YA^2)) = 1$, d'où

$$\begin{aligned} q^m|Y(u,\alpha)| &\le \sum_{B\in\mathbb{A}_n} \sum_{A\in\mathbb{A}_{m-1}} E(u(B^2A+BA^2)+\alpha A) \\ &\le \sum_{A\in\mathbb{A}_{m-1}} E(\alpha A) \sum_{B\in\mathbb{A}_n} E(u(B^2A+BA^2)), \end{aligned}$$

d'où (III.9). On suppose $\nu(u) > 2n+1$. Comme pour la proposition précédente, la somme intérieure dans (i) peut s'écrire sous forme d'intégrale, et

$$|Y(u,\alpha)| \le \sum_{B\in\mathbb{B}_{n,m}} \int_{\nu(y)>-m} E(u(B^2y+y^2B)+\alpha y)\,dy\,,$$

d'où, avec (I.8),

$$|Y(u,\alpha)| \le q^m \sum_{B\in\mathbb{B}_{n,m}} \int_{\mathcal{P}} E((uB^2+\alpha)X^m t + uBX^{2m}t^2)\,dt\,. \tag{ii}$$

Si $\nu(\alpha) < \nu(u)-2n$, pour tout $B \in \mathbb{B}_{n,m}$ on a $\nu(uB^2) > \nu(\alpha)$ et $\nu(uB^2+\alpha) = \nu(\alpha) < \nu(uB^2)$, si de plus B est non nul, $\deg B \ge m$ et, avec (III.3), on a $1+\nu(uB) \ge 2\nu(uB^2)$, d'où $1+2\deg([(uB^2+\alpha)X^m]) > \deg([uBX^{2m}])$ et, d'après la proposition I.10,

$$\int_{\mathcal{P}} E((uB^2+\alpha)X^m t + uBX^{2m}t^2)\,dt = 0\,.$$

Si $\nu(\alpha) < \nu(u) - 2n$, on ne retient dans la relation (ii) que l'intégrale correspondant à $B = 0$, d'où

$$|Y(u,\alpha)| \le q^m \int_{\mathcal{P}} E(\alpha X^m t)\, dt\,. \tag{iii}$$

Avec (III.6), on a $\nu(\alpha) \le m$, et d'après (I.5), l'intégrale ci-dessus est nulle.

PROPOSITION III.3. *Soit un polynôme Q tel que $\deg Q \le n$. Pour $R \in \boldsymbol{C}_Q$, soit $\mathcal{A}(u;Q,R)$ l'ensemble des polynômes $A \in \mathcal{A}(u)$ congrus à R modulo Q. Alors, on a*

$$\mathcal{A}(u;Q,R) \ne \emptyset \;\Rightarrow\; \#\mathcal{A}(u;Q,R) = \#\mathcal{A}(u;Q,0)\,, \tag{III.11}$$

$$\#\mathcal{A}(u;Q,0)\#(\mathcal{A}(u)\cap \boldsymbol{C}_Q) \le \#\mathcal{A}(u)\,. \tag{III.12}$$

Si, de plus, $2n + \deg Q < \nu(u)$, on a

$$\#\mathcal{A}(u;Q,0) = |Q|^{-1}\#\mathcal{A}(u)\,. \tag{III.13}$$

Démonstration. (III.11) est immédiat. Si $\deg Q \ge m$, $\mathcal{A}(u;Q,0) = \{0\}$, $\mathcal{A}(u)\cap \boldsymbol{C}_Q = \mathcal{A}(u)$, la relation (III.12) est triviale, et, compte tenu de (III.6), l'hypothèse $2n + \deg Q < \nu(u)$ est exclue. Il suffit de faire la démonstration dans le cas où $\deg Q < m$. On a alors

$$\#\mathcal{A}(u) = \sum_{R\in \mathsf{C}_Q} \#\mathcal{A}(u;Q,R)\,,$$

d'où, avec (III.11),

$$\#\mathcal{A}(u) = \#\mathcal{A}(u;Q,0)\#\{R \in \boldsymbol{C}_Q \mid \mathcal{A}(u;Q,R) \ne \emptyset\}\,.$$

Si $R \in \mathcal{A}(u)\cap \boldsymbol{C}_Q$, $R \in \mathcal{A}(u;Q,R)$ et $\mathcal{A}(u;Q,R) \ne 0$, d'où (III.12). Si $\nu(u) > 2n + \deg Q$, tout $R \in \boldsymbol{C}_Q$ appartient à $\mathcal{A}(u)$, et

$$\{R \in \boldsymbol{C}_Q \mid \mathcal{A}(u;Q,R) \ne \emptyset\} = \boldsymbol{C}_Q\,,$$

ce qui donne (III.13).

PROPOSITION III.4. *Soit Q un polynôme tel que $\nu(u) - 2n \le \deg Q < m$. Alors, on a*

$$\#(\mathcal{A}(u)\cap(Q)) \le q^{1/2} q^{m/2} |Q|^{-1/2}\,. \tag{III.14}$$

Démonstration. On a

$$\#(\mathcal{A}(u)\cap(Q))q^{n+1} = \sum_{L\in \mathbb{A}_{m-\deg Q-1}} \sum_{B\in\mathbb{A}_n} E(u(L^2Q^2B + LQB^2))\,.$$

Ici encore, la somme intérieure peut s'écrire sous forme d'intégrale, d'où

$$\#(\mathcal{A}(u)\cap(Q))q^{n+1} = \sum_{L\in \mathbb{A}_{m-\deg Q-1}} \int_{\nu(\beta)\ge -n} E(u(L^2Q^2\beta + LQ\beta^2))\, d\beta\,,$$

d'où, avec (I.8),

$$\text{(i)} \qquad \#(\mathcal{A}(u)\cap(Q)) = \sum_{L\in\mathbb{A}_{m-\deg Q-1}} J(u,L)\,,$$

où

$$\text{(ii)} \qquad J(u,L) = \int\limits_{\mathcal{P}} E(u(L^2Q^2X^{n+1}t + LQX^{2(n+1)}t^2))\,dt\,.$$

D'après la proposition I.10, l'intégrale $J(u,L)$ est égale à 1 si et seulement si

$$\text{(iii)} \qquad [uLQX^{2(n+1)}] + X[uL^2Q^2X^{n+1}]^2 \quad \text{est carré dans } \mathbb{A}\,.$$

De (i) on déduit que $\#(\mathcal{A}(u)\cap(Q))$ est égal au nombre de polynômes $L\in\mathbb{A}_{m-1-\deg Q}$ vérifiant (iii). On pose

$$\text{(iv)} \qquad uQ = \sum_{i\le -s} a_iX^i, \qquad s = k-\deg Q\,,$$

$$\text{(v)} \qquad uQ^2 = \sum_{i\le -t} b_iX^i, \qquad t = k-2\deg Q\,,$$

$$\text{(vi)} \qquad d = m-1-\deg Q\,.$$

Alors, $\#(\mathcal{A}(u)\cap(Q))$ est le nombre de solutions $(y_0,\dots,y_d)\in\mathbb{F}_q^{d+1}$ du système d'équations $(\mathcal{E})$ suivant:

$$(\mathcal{E}) \qquad \Big(\sum_{\substack{i+j=2p+1\\ i\le -s\\ 0\le j\le d}} a_iy_j + \sum_{\substack{i+2j=p\\ i\le -t\\ 0\le j\le d}} b_i^2y_j^4\Big)_{-n-1\le p\le M}$$

où

$$M = \max\left(2d-t, \left[\frac{d-s-1}{2}\right]\right).$$

On a $3m-1\le k\le 3m+1$. Il s'ensuit que

$$\text{(vii)} \qquad M = \left[\frac{d-s-1}{2}\right]$$

et que l'intervalle $[2d-t+1, [(d-s-1)/2]]$ contient au plus un entier et est vide si $k=3m-1$. L'équation (e_p) d'indice p s'écrit

$$(e_p) \qquad a_{-s}y_{2p+1+s} + \sum_{\substack{i+j=2p+1\\ i\le -s-1\\ 0\le j\le d}} a_iy_j + \sum_{\substack{i+2j=p\\ i\le -t\\ 0\le j\le d}} b_i^2y_j^4 = 0\,.$$

Pour les y_j intervenant dans la première somme, on a $j\ge 2p+2+s$. Pour les y_j intervenant dans la deuxième somme, on a $2j\ge p+t$. Si $p\le 2d-t$, on a $p+t\ge 2(2p+2+s)$ et on a aussi $j\ge 2p+2+s$ pour les y_j intervenant dans la deuxième somme. Si $p>2d-t$, $p=M$ et la deuxième

somme est vide. Les valeurs $y_d, y_{d-1}, \dots, y_{2p+2-s}$ étant fixées, l'équation (e_p) détermine un unique y_{2p+1+s}. Si $d-s-1$ est pair, l'équation (e_M) détermine y_d, ensuite, si s est pair, pour tout système $(y_{d-1}, y_{d-3}, \dots, y_0)$ d'éléments de $\mathbb{F}_q$, il existe au plus un système $(y_{d-1}, \dots, y_1)$ d'éléments de $\mathbb{F}_q$ tels que $(y_d, y_{d-1}, \dots, y_1, y_0)$ soit solution de $(\mathcal{E})$; si au contraire, s est impair, pour tout système $(y_{d-1}, y_{d-3}, \dots, y_1)$ d'éléments de $\mathbb{F}_q$ il existe au plus un système $(y_{d-2}, \dots, y_0)$ tel que $(y_d, \dots, y_0)$ soit solution de $(\mathcal{E})$. Suivant la parité de d, le nombre de solutions de $(\mathcal{E})$ est majoré par $q^{(d+1)/2}$ ou par $q^{d/2}$. Si $d-s$ est pair, l'équation (e_M) détermine y_{d-1}. Comme ci-dessus, on obtient que le nombre de solutions de $(\mathcal{E})$ est majoré par $q^{d/2+1}$ ou par $q^{(d+1)/2}$ suivant la parité de d. Dans tous les cas on a

$$\#(\mathcal{A}(u) \cap (Q)) \le q^{d/2+1}\,.$$

On conclut avec (vi).

IV. Majoration de $f(t)$. Soit un entier $n > 0$. On pose pour $t \in \mathbb{K}_\infty$,

$$f(t) = \sum_{A \in \mathbb{A}_n} E(tA^3)\,. \tag{IV.1}$$

La proposition I.2 montre que l'on peut limiter l'étude de $f(t)$ aux $t \in \mathcal{P}$. Suivant la méthode du cercle classique, on approche $t \in \mathcal{P}$ par des fractions rationnelles. On désigne par $\mathcal{F}_n$ l'ensemble des fractions de Farey à l'ordre n, c'est-à-dire, l'ensemble des fractions rationnelles G/H telles que $G \in \boldsymbol{C}_H$, $\operatorname{pgcd}(G,H) = 1$, et $\deg H \le n$. Si G/H est un élément de $\mathcal{F}_n$, on appelle *arc de Farey* de centre G/H l'ensemble $\mathcal{U}_{G/H}$ ainsi défini:

$$t \in \mathcal{U}_{G/H} \;\Leftrightarrow\; \nu(t - G/H) > n + \deg H\,. \tag{IV.2}$$

PROPOSITION IV.1. *Lorsque G/H décrit $\mathcal{F}_n$, les arcs de Farey $\mathcal{U}_{G/H}$ forment une partition de $\mathcal{P}$.*

Démonstration. C'est le théorème 4.3 de [3].

Pour les $t \in \mathcal{P}$ proches d'une fraction G/H de $\mathcal{F}_n$ on aura une bonne approximation de $f(t)$. Ces points sont ceux qui vérifient $\nu(t - G/H) > 2n + \deg H$. Ils correspondent aux arcs majeurs d'une dissection de Farey classique. Pour les autres t on aura seulement une majoration de $f(t)$. Dans ce qui suit G/H est une fraction de Farey à l'ordre n, t est un élément de l'arc de Farey $\mathcal{U}_{G/H}$ et on pose

$$t = G/H + u\,. \tag{IV.3}$$

On a donc

$$\deg H \le n\,, \tag{IV.4}$$

$$\nu(u) > n + \deg H \ge n\,. \tag{IV.5}$$

On pose aussi

$$\nu(u) = k = 3m + \varrho, \qquad \varrho \in \{-1, 0, +1\}\,. \tag{IV.6}$$

On notera ϕ le diviseur $\phi(H)$ défini au paragraphe II par la relation (II.19).

Proposition IV.2. *On a*

$$|H| f(t) = \sum_{K \in \mathsf{C}_H} S(H, G, K) Y(u, K/H)\,. \tag{IV.7}$$

Démonstration. On partage l'ensemble $\mathbb{A}_n$ suivant les différentes classes de congruence modulo H. Par une méthode classique (cf. [6]), à l'aide de la proposition I.2 et du corollaire I.5, on obtient la relation

$$|H| f(t) = \sum_{R \in \mathsf{C}_H} E\left(\frac{GR^3}{H}\right) \sum_{A \in \mathbb{A}_n} E(uA^3) \sum_{K \in \mathsf{C}_H} E\left(\frac{K(R+A)}{H}\right),$$

qui, après inversion de l'ordre des sommations donne la relation (IV.7), compte tenu des définitions (II.1) et (III.2).

Corollaire IV.3. *Si $\nu(t - G/H) > 2n + \deg H$, on a*

$$|H| f(t) = S(H, G, 0) f(u)\,, \tag{IV.8}$$

où

$$f(u) = \begin{cases} q^{n+1} & \text{si } \nu(u) > 3n+1, \\ q^m & \text{si } \nu(u) = 3m + \varrho, \varrho \neq 1, \nu(u) \leq 3n+1, \\ q^m \sum_{b \in \mathbb{F}_q} \psi(\operatorname{sgn}(u) b^3) & \text{si } \nu(u) = 3m+1 \leq 3n+1. \end{cases} \tag{IV.9}$$

Démonstration. Si $\nu(u) > 3n+1$, pour tout $K \in \boldsymbol{C}_H$, on a

$$Y\left(u, \frac{K}{H}\right) = \sum_{A \in \mathbb{A}_n} E\left(\frac{K}{H} A\right).$$

Si $K \neq 0$, $\nu(K/H) \leq \deg H \leq n$, et, d'après (I.6), $Y(u, K/H) = 0$. Supposons $\nu(u) \leq 3n+1$. On a $\nu(u) > 2n + \deg H$. Si $\deg H > 0$, on a $\nu(u) > 2n+1$, et, pour tout $K \in \boldsymbol{C}_H$ non nul, on a $\nu(K/H) \leq \deg H \leq \nu(u) - 2n$. D'après (III.10), $Y(u, K/H) = 0$. Enfin, si $\deg H = 0$, $\boldsymbol{C}_H = \{0\}$. Dans tous les cas (IV.7) se réduit à

$$|H| f(t) = S(H, G, 0) Y(u, 0) = S(H, G, 0) f(u)\,.$$

La démonstration de la proposition VIII.1 de [1] reste vraie en caractéristique 2, pour des exposants impairs et permet de calculer $f(u)$. Ce calcul donne (IV.9).

Proposition IV.4. *Soit un nombre réel $\varepsilon > 0$. Si $\nu(u) \leq 2n + \deg H$, on a*

$$|f(t)| \leq a_4(q, \varepsilon) q^{n(5/6+\varepsilon)}\,, \tag{IV.10}$$

où

$$a_4(q,\varepsilon) = \max(q^{3/2}a_1(q), qa_2(q), qa_3(q,\varepsilon))\,. \tag{IV.11}$$

Démonstration. On a vu au paragraphe II que les polynômes K pour lesquels $S(H,G,K) \neq 0$ sont tous dans la même classe modulo le sous-groupe $\mathcal{R}(H,G)^\perp$. Soit K l'un de ces polynômes. La relation (IV.7) peut s'écrire

$$|H|f(t) = \sum_{L\in\mathcal{R}(H,G)^\perp} S(H,G,K+L)Y\left(u, \frac{K+L}{H}\right).$$

Avec (II.9) et (III.9) il vient

$$\begin{aligned} q^m|H||f(t)| &\leq W(H,G)^{1/2}q^{n+1} \sum_{L\in\mathcal{R}(H,G)^\perp} \sum_{A\in\mathcal{A}(u)} E\left(\frac{K+L}{H}A\right) \\ &\leq W(H,G)^{1/2}q^{n+1} \sum_{A\in\mathcal{A}(u)} E\left(\frac{K}{H}A\right) \sum_{L\in\mathcal{R}(H,G)^\perp} E\left(\frac{L}{H}A\right). \end{aligned}$$

L'équivalence (II.24) nous donne

$$q^m|H||f(t)| \leq W(H,G)^{1/2}q^{n+1}\#(\mathcal{R}(H,G)^\perp) \sum_{R\in\mathcal{R}(H,G)} \sum_{\substack{A\in\mathcal{A}(u)\\ A\equiv R \bmod H}} E\left(\frac{K}{H}A\right),$$

d'où

$$q^m|H||f(t)| \leq W(H,G)^{1/2}q^{n+1}\#(\mathcal{R}(H,G)^\perp) \sum_{R\in\mathcal{R}(H,G)} \#\mathcal{A}(u;H,R)\,,$$

$\mathcal{A}(u;H,R)$ étant l'ensemble défini à la proposition III.3. Cette même proposition III.3 nous donne alors

$$\begin{aligned} \text{(i)}\quad q^m|H||f(t)| &\leq W(H,G)^{1/2}q^{n+1}\#(\mathcal{R}(H,G)^\perp) \\ &\quad \times \#(\mathcal{A}(u)\cap(H))\#\{R\in\mathcal{R}(H,G) \mid \mathcal{A}(u;H,R)\neq\emptyset\}\,. \end{aligned}$$

Supposons d'abord $\deg H < m$. Dans ce cas, on majore trivialement

$$\#\{R\in\mathcal{R}(H,G) \mid \mathcal{A}(u;H,R)\neq\emptyset\}$$

par $\#\mathcal{R}(H,G)$. Avec (II.23), on obtient

$$q^m|f(t)| \leq W(H,G)^{1/2}q^{n+1}\#(\mathcal{A}(u)\cap(H))$$

d'où, avec (III.14),

$$\begin{aligned} q^m|f(t)| &\leq q^{3/2}q^{n+m/2}|H|^{-1/2}W(H,G)^{1/2}\,, \\ |f(t)| &\leq q^{3/2}q^{n-m/2}|H|^{-1/2}W(H,G)^{1/2}\,. \end{aligned}$$

Avec (IV.5), (IV.6) et (II.26) on a alors,

$$\text{(ii)}\qquad |f(t)| \leq q^{3/2}a_1(q)q^{5n/6}\,.$$

Supposons maintenant que $\deg H \geq m$. Dans ce cas, $\mathcal{A}(u) \cap (H) = \{0\}$ et, pour tout $R \in \boldsymbol{C}_H$, $\mathcal{A}(u; Q, R)$ est soit vide, soit égal à $\{R\}$. La relation (i) s'écrit

$$q^m |H||f(t)| \leq W(H,G)^{1/2} q^{n+1} \#(\mathcal{R}(H,G)^{\perp}) \#(\mathcal{R}(H,G) \cap \mathcal{A}(u)) \,.$$

On majore $\#(\mathcal{R}(H,G) \cap \mathcal{A}(u))$ par $\#\mathcal{R}(H,G)$. Avec (II.4) on obtient la majoration

$$|f(t)| \leq q^{n+1-m} W(H,G)^{1/2} \,. \tag{iii}$$

Avec (II.23) et (II.4) on a

$$q^m |f(t)| \leq |H| W(H,G)^{-1/2} q^{n+1} \#(\mathcal{R}(H,G) \cap \mathcal{A}(u)) \,.$$

Par ailleurs, on a

$$\#\left(\frac{\mathcal{R}(H,G) \cap \mathcal{A}(u)}{\mathcal{R}(H,G) \cap \mathcal{A}(u) \cap (\phi)} \right) \leq \#\left(\frac{\mathcal{R}(H,G)}{\mathcal{R}(H,G) \cap (\phi)} \right) ,$$

d'où, avec (II.22),

$$q^m |f(t)| \leq \lambda(H) |H| W(H,G)^{-1/2} q^{n+1} \#(\mathcal{R}(H,G) \cap \mathcal{A}(u) \cap (\phi)) \,,$$

$$|f(t)| \leq q^{n+1-m} \lambda(H) |H| W(H,G)^{-1/2} \#(\mathcal{A}(u) \cap (\phi)) \,. \tag{iv}$$

Si $\deg \phi \geq m$, $\#(\mathcal{A}(u) \cap (\phi)) = 1$, d'où

$$|f(t)| \leq q^{n+1-m} \lambda(H) |H| W(H,G)^{-1/2} \,.$$

Avec (IV.5) et (IV.6), on a

$$|f(t)| \leq q^{1+2n/3} \lambda(H) |H|^{2/3} W(H,G)^{-1/2} \,,$$

d'où, avec (II.29),

$$|f(t)| \leq q^{1+2n/3} a_3(q,\varepsilon) |H|^{1/6+\varepsilon} \,,$$

puis, avec (IV.4)

$$|f(t)| \leq q a_3(q,\varepsilon) q^{n(5/6+\varepsilon)} \,. \tag{v}$$

Si $\deg \phi < m$ et si $\nu(u) > 2n + 1 + \deg \phi$, d'après (III.13), on a

$$\#(\mathcal{A}(u) \cap (\phi)) = |\phi|^{-1} \#\mathcal{A}(u) \,.$$

La relation (iv) nous donne alors

$$|f(t)| \leq q^{n+1-m} \lambda(H) |H| W(H,G)^{-1/2} |\phi|^{-1} \#\mathcal{A}(u) \,,$$

d'où, avec (III.7),

$$|f(t)| \leq q^{m+1} \lambda(H) |H| W(H,G)^{-1/2} |\phi|^{-1} \,. \tag{vi}$$

Des majorations (iii) et (vi) on déduit la majoration

$$|f(t)| \leq q^{1+n/2}|H|^{1/2}\lambda(H)^{1/2}|\phi|^{-1/2}\,,$$

puis avec (II.27) et (IV.4), on obtient

(vii) $$|f(t)| \leq qa_2(q)q^{5n/6}\,.$$

Si $\deg\phi < m$ et si $\nu(u) \leq 2n+1+\deg\phi$, la majoration (III.14) nous donne

$$\#(\mathcal{A}(u)\cap(\phi)) \leq q^{1/2}(q^m|\phi|^{-1})^{1/2}$$

et (iv) donne alors

$$|f(t)| \leq q^{3/2+n-m/2}\lambda(H)|H|W(H,G)^{-1/2}|\phi|^{-1/2}\,.$$

Enfin, avec (IV.5), (IV.6) et (II.28) il vient

(viii) $$|f(t)| \leq q^{3/2}a_1(q)q^{5n/6}\,.$$

On conclut avec (ii), (v), (vi) et (viii).

Cette dernière proposition donne le théorème annoncé.

Remarques. On peut penser généraliser cette étude en remplaçant l'exposant 3 par un exposant $k = 2^h+1$, et, de façon plus générale, étudier, en caractéristique p, le problème posé par les exposants p^h+1. S'il est vrai que la proposition I.10 et les résultats relatifs aux sommes $S(H,G,K)$ ou aux sommes $Y(u,\alpha)$ se généralisent très bien, la méthode utilisée au paragraphe IV s'avère insuffisante en caractéristique 2 pour des exposants autres que 3.

On peut donc poser la question suivante : Peut-on améliorer l'étude des sommes $Y(u,\alpha)$ afin d'obtenir des résultats pour des exposants autres que 3, ou bien 3 est-il le seul exposant pour lequel la méthode utilisée dans ce travail soit performante, ce qui est déjà le cas pour la méthode de R. C. Vaughan (cf. [6]), pour le problème de Waring classique?

Références

[1] M. Car, *Sommes de puissances et d'irréductibles dans* $\mathbb{F}_q[X]$, Acta Arith. 44 (1984), 7–34.

[2] J. Cherly, *Sommes d'exponentielles cubiques dans l'anneau des polynômes en une variable sur le corps à deux éléments, et application au problème de Waring*, Thèse soutenue le 27 octobre 1989 à l'Université de Bordeaux I.

[3] D. R. Hayes, *The expression of a polynomial as a sum of three irreducibles*, Acta Arith. 11 (1966), 461–488.

[4] R. M. Kubota, *Waring's problem for* $\mathbb{F}_q[X]$, Dissertationes Math. 117 (1974).

[5] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1986.
[6] R. C. Vaughan, *Some remarks on Weyl sums*, in: Topics in Classical Number Theory, Budapest 1981, Colloq. Math. Soc. János Bolyai 34, Vol. II, North-Holland, 1984, 1585–1602.

U. R. A. 225
FACULTÉ DE SAINT-JEROME
AVENUE ESCADRILLE NORMANDIE-NIEMEN
13397 MARSEILLE CEDEX 13
FRANCE

Reçu le 22.2.1991 (2040)