

POLSKA AKADEMIA NAUK, INSTYTUT MATEMATYCZNY

5.07.83  
215

# DISSERTATIONES MATHEMATICAE (ROZPRAWY MATEMATYCZNE)

KOMITET REDAKCYJNY

**KAROL BORSUK** redaktor

ANDRZEJ BIAŁYNICKI-BIRUŁA, BOGDAN BOJARSKI,  
ZBIGNIEW CIESIELSKI, JERZY ŁOŚ, WIKTOR MAREK,  
ZBIGNIEW SEMADENI

## CCXV

MIREILLE CAR  
Sommes de carrés dans  $F_q[X]$

WARSZAWA 1983

P A Ń S T W O W E W Y D A W N I C T W O N A U K O W E

5.7133



PRINTED IN POLAND

Copyright © by PWN – Polish Scientific Publishers, Warszawa 1983

ISBN 83-01-03505-6

ISSN 0012-3862

## TABLE DES MATIÈRES

I. Introduction . . . . .	5
II. Notations . . . . .	6
III. La méthode du cercle . . . . .	8
IV. Evaluation de $R_k(M)$ . . . . .	9
V. Sommes de $k$ carrés dans un corps fini . . . . .	13
VI. Les séries singulières $\mathfrak{S}_k(M)$ . . . . .	14
VII. Estimation de $\mathcal{L}_3(M)$ lorsque $-M$ est carré . . . . .	28
VIII. Estimation des nombres $R_k(M)$ . (Fin) . . . . .	33
Bibliographie . . . . .	36

---



## I. Introduction

Soit  $F_q$  le corps fini à  $q$  éléments,  $q$  étant un entier impair, et  $F_q[X]$  l'anneau des polynômes à une indéterminée sur le corps  $F_q$ .

On a des formules donnant le nombre de représentations d'un polynôme de  $F_q[X]$  comme somme de  $1, 2, \dots, k, \dots$  carrés. Ces formules sont établies dans [4], [5], [6], [7], [9], [10] et [11]. Il n'est pas facile de déduire de ces formules que ce nombre de représentations est ou n'est pas strictement positif. De plus, les conditions de degré qui sont exigées dans ces représentations ne sont pas les plus restrictives possibles.

Dans ce qui suit nous nous intéressons aux représentations d'un polynôme de  $F_q[X]$  comme somme de  $k$  carrés, en exigeant les conditions de degré les plus restrictives possibles.

Si  $M$  est un polynôme de  $F_q[X]$  de degré  $2n$  ou  $2n-1$ , toute solution  $(M_1, \dots, M_k)$  de l'équation

$$M = M_1^2 + \dots + M_k^2$$

en polynômes  $M_1, \dots, M_k$  de  $F_q[X]$  de degré au plus égal à  $n$  sera dite *représentation restreinte de  $M$*  comme somme de  $k$  carrés, le nombre de ces représentations restreintes sera noté  $R_k(M)$ .

Deux problèmes peuvent se poser :

(1) Existe-t-il des entiers  $k$  pour lesquels tout polynôme de  $F_q[X]$  admette une représentation restreinte en sommes de  $k$  carrés, et, si oui, quel est le plus petit de ces entiers  $k$  que l'on désignera par  $g(2)$ ?

(2) Si  $k$  est un entier au moins égal à  $g(2)$ , si  $M$  est un polynôme de  $F_q[X]$ , déterminer le nombre  $R_k(M)$ .

Ces problèmes sont des cas particuliers du problème de Waring pour  $F_q[X]$  déjà traité dans [19] pour des exposants  $k \geq 2$  mais seulement pour polynômes de degré multiple de  $k$ , dans [15] pour des exposants  $k \geq 3$ , et dans [3] pour des exposant  $k \geq 2$ . Les résultats obtenus dans les articles cités sont intéressants par leur généralité, mais des calculs plus adaptés à l'exposant 2 donneront de meilleurs résultats. De plus, une difficulté qui n'existe pas pour le problème de Waring classique, apparait dans l'étude du problème de Waring pour  $F_q[X]$ , elle provient de la majoration de sommes de caractères analogue à la majoration de Weyl, qui, introduisant le facteur  $k!$ ,

exige que la caractéristique du corps  $F_q$  soit strictement supérieure à  $k$ . On voudrait pouvoir remplacer cette condition par la condition plus naturelle " $k$  différent de la caractéristique du corps  $F_q$ ". Lorsque  $k = 2$  ces deux conditions sont identiques, et, de plus, le problème de la majoration des sommes de Weyl ne se pose pas.

Il est bien connu que les polynômes de  $F_q[X]$  ne sont pas tous carrés. Si  $-1$  est carré dans  $F_q$ , aucun polynôme irréductible de  $F_q[X]$  n'est somme de 2 carrés. Si  $-1$  n'est pas carré dans  $F_q$ , les polynômes de degré impair ne sont pas sommes de 2 carrés. Notons que les polynômes de degré pair ne sont pas tous sommes de 2 carrés, le nombre de polynômes de  $F_q[X]$  de degré  $2n$  sommes de 2 carrés étant asymptotiquement équivalent à

$$a(q)q^{2n}n^{-1/2},$$

$a(q)$  étant une constante strictement positive qui ne dépend que de  $q$ , ceci d'après [4].

Dans [9] il est démontré que tout polynôme de  $F_q[X]$  est égal à une somme de 3 carrés, aucune condition de degré n'étant exigée. On peut démontrer que tout polynôme de  $F_q[X]$  admet une représentation restreinte en somme de 3 carrés, d'où la relation  $g(2) = 3$ . La démonstration de ce résultat due à Monsieur J. P. Serre n'a pas été publiée. Elle ne donne pas d'évaluation asymptotique du nombre de représentations restreintes.

L'objet principal de ce travail est de donner une évaluation asymptotique des nombres  $R_k(M)$ . Nous obtiendrons des résultats analogues à ceux connus sur les représentations d'entiers naturels comme sommes de  $k$  carrés,  $k$  étant un entier au moins égal à 3 (c.f. [2]).

## II. Notations

Nous reprenons les notations introduites dans [14] et nous en introduisons de nouvelles.

Soit  $H$  un polynôme non nul de  $F_q[X]$ , son degré sera noté  $d^0H$ , le coefficient de son terme de plus haut degré  $\text{sgn}(H)$ ; l'ensemble des polynômes de degré strictement inférieur au degré de  $H$ , identifié à l'ensemble des classes de congruence modulo  $H$ , sera noté  $\mathcal{C}_H$  et le groupe multiplicatif des classes inversibles modulo  $H$  sera noté  $\mathcal{C}_H^*$ , l'ordre de ce groupe sera noté  $\Phi(H)$ . Comme la fonction d'Euler classique, la fonction  $\Phi$  est multiplicative, et, si  $P$  est un polynôme irréductible de degré  $n$ , si  $j$  est un entier strictement positif,

$$\Phi(P^j) = (q^n - 1)q^{j-1}n.$$

On désigne par  $\mathcal{U}$  l'ensemble des polynômes unitaires. Sur  $\mathcal{U}$  on définit la fonction de Möbius  $\mu$  par

$$\mu(H) = \begin{cases} 1 & \text{si } H = 1, \\ 0 & \text{si } H \text{ a un diviseur carré non constant,} \\ (-1)^r & \text{si } H \text{ est produit de } r \text{ polynômes} \\ & \text{irréductibles distincts.} \end{cases}$$

L'ensemble des polynômes irréductibles unitaires sera noté  $\mathcal{I}$ , l'ensemble des polynômes de degré  $m$  sera noté  $D_m$ , l'ensemble des polynômes de degré au plus égal à  $m$  sera noté  $F_m$ , le mot polynôme désignant en fait un polynôme de  $F_q[X]$ .

Si  $H$  est un polynôme non nul, si  $A$  et  $B$  sont des polynômes, la relation  $A$  est congru à  $B$  modulo  $H$  sera notée  $A \equiv B \pmod{H}$ , si  $A$  et  $B$  sont des polynômes non nuls, la relation  $A$  divise  $B$  sera notée  $A|B$ , le plus grand commun diviseur unitaire des polynômes  $A$  et  $B$  sera noté  $(A, B)$ , si  $P$  est un polynôme irréductible, on notera  $v_P(A)$  la valuation  $P$ -adique de  $A$ , c'est à dire le plus grand entier  $h$  tel que  $P^h$  divise  $A$ .

Sur le corps  $F_q(X)$  des fractions rationnelles on définit une valuation  $v$  par

$$v(A/B) = d^0 B - d^0 A,$$

si  $A$  et  $B$  sont des polynômes non nuls. Le complété de  $F_q(X)$  pour cette valuation s'identifie au corps  $K$  des séries de Laurent formelles en  $1/X$  à coefficients dans le corps  $F_q$ , la valuation  $v$  se prolongeant à  $K$  par

$$v\left(\sum_{s \in \mathbf{Z}} a_s X^s\right) = -\text{Sup}\{r \in \mathbf{Z} \mid a_r \neq 0\}.$$

A cette valuation  $v$  est associée la valeur absolue  $|\cdot|_v$ , définie par

$$\begin{aligned} |a|_v &= q^{-v(a)} & \text{si } a \neq 0, \\ |0|_v &= 0. \end{aligned}$$

Nous noterons simplement  $|\cdot|$  cette valeur absolue, tout en utilisant aussi ce symbole pour désigner la valeur absolue classique sur  $C$ .

On désigne par  $\mathcal{P}$  l'idéal de valuation de  $K$ , et, pour tout entier relatif  $j$ , par  $\mathcal{P}_j$  l'idéal

$$\{t \in K \mid v(t) > j\}.$$

Les ensembles  $\mathcal{P}_j$  sont des sous-groupes compacts du groupe additif localement compact  $K$ . Désignons par  $dt$  la mesure de Haar sur  $K$  normalisée à 1 sur  $\mathcal{P}$ . Tout élément  $u \in K$  s'écrit de façon unique comme somme

$$u = P(u) + \{u\},$$

$P(u)$  étant un polynôme et  $\{u\}$  un élément de  $\mathcal{P}$ ;  $\{u\}$  est appelé *partie fractionnaire de  $u$* .

Soit  $e$  un caractère non principal du groupe additif de  $F_q$ . On définit un caractère non principal  $E$  du groupe additif de  $K$  en posant

$$E\left(\sum_{s \in \mathbb{Z}} a_s X^s\right) = e(a_{-1}).$$

Si  $a$  est un élément de  $F_q$ , on désigne, pour tout entier  $k \geq 1$ , par  $r_k(a)$  le nombre de solutions  $(a_1, \dots, a_k) \in F_q^k$  de l'équation

$$a = a_1^2 + \dots + a_k^2.$$

Si  $\mathcal{A}$  est une partie de  $K$  contenant 0, l'ensemble des éléments non nuls de  $\mathcal{A}$  sera noté  $\mathcal{A}^*$ .

### III. La méthode du cercle

Les quatre propositions suivantes ont été établies dans [14] ou se démontrent par des méthodes analogues.

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

PROPOSITION III.2. (i) *Pour tout polynôme  $A$ ,  $E(A) = 1$ .*

(ii) *Pour tout polynôme  $H$  non nul, si  $A$  et  $B$  sont des polynômes congrus modulo  $H$ ,  $E(A/H) = E(B/H)$ .*

(iii) *Si  $u \in \mathcal{P}^2$ ,  $E(u) = 1$ .*

PROPOSITION III.3. *Soient un entier  $j \geq 0$ ,  $u \in K$  et  $b \in \mathcal{P}$ . Alors,*

$$(III.1) \quad \int_{b + \mathcal{P}_j} E(ut) dt = \begin{cases} q^{-j} E(ub) & \text{si } v(u) > -j, \\ 0 & \text{si } v(u) \leq -j. \end{cases}$$

PROPOSITION III.4 *Soient  $j$  un entier naturel et  $u \in K$ . Alors,*

$$(III.2) \quad \sum_{B \in \mathcal{F}_j} E(uB) = \begin{cases} q^{j+1} & \text{si } v(\{u\}) > j+1, \\ 0 & \text{si } v(\{u\}) \leq j+1. \end{cases}$$

De cette proposition on déduit un corollaire que l'on utilisera fréquemment par la suite.

COROLLAIRE. *Soient  $G$  et  $H$  des polynômes,  $H$  n'étant pas nul. Alors,*

$$(III.3) \quad \sum_{R \in \mathcal{C}_H} E((G/H)R) = \begin{cases} |H| & \text{si } H \text{ divise } G, \\ 0 & \text{si } H \text{ ne divise pas } G. \end{cases}$$



Démonstration. On applique (III.2) avec  $j = d^0 H - 1$  et  $u = G/H$ .

La proposition III.3 donne l'égalité fondamentale de la "méthode du cercle". En effet, soit  $n$  un entier strictement positif, et soit  $f$  l'application de  $\mathcal{P}$  dans  $\mathcal{C}$  définie par

$$(III.4) \quad f(t) = \sum_{A \in F_n} E(tA^2).$$

Pour tout entier  $k \geq 1$ , pour tout polynôme  $M \in F_q[X]$  soit

$$(III.5) \quad R_k(M) = \int_{\mathcal{P}} f^k(t) E(-Mt) dt.$$

Alors  $R_k(M)$  est égal au nombre de solutions  $(A_1, \dots, A_k)$  de l'équation

$$M = A_1^2 + \dots + A_k^2$$

en polynômes  $A_1, \dots, A_k$  de degré au plus  $n$ . Si  $M$  est de degré  $2n$  ou  $2n-1$ , l'intégrale  $R_k(M)$  donne le nombre de représentations restreintes de  $M$  comme sommes de  $k$  carrés.

DÉFINITIONS. On appelle *fraction de Farey à l'ordre  $n$*  toute fraction rationnelle  $G/H$  telle que

- (i)  $H$  est un polynôme unitaire de degré au plus  $n$ ,
- (ii)  $G \in \mathcal{C}_H^*$ .

Si  $G/H$  est une fraction de Farey à l'ordre  $n$ , on appelle *arc de Farey la boule*

$$\mathcal{U}_{G/H} = \{t \in \mathcal{P} \mid v(t - (G/H)) > d^0 H + n\}.$$

PROPOSITION III.5. *Pour tout entier  $n$ , lorsque  $G/H$  décrit l'ensemble des fractions de Farey à l'ordre  $n$ , les arcs de Farey  $\mathcal{U}_{G/H}$  forment une partition de  $\mathcal{P}$ .*

Démonstration. C'est le théorème 4.3 de [14].

#### IV. Evaluation de $R_k(M)$

Dans ce paragraphe  $k$  est un entier fixé strictement positif,  $M$  est un polynôme de degré  $2n$  ou  $2n-1$ ; la fonction  $f$  est la fonction définie au paragraphe précédent par la relation (III.4). Les fractions de Farey considérées ici seront toutes des fractions de Farey à l'ordre  $n$ . Si  $G/H$  est une telle fraction de Farey, soit

$$(IV.1) \quad I_{k,G/H}(M) = \int_{\mathcal{U}_{G/H}} f(t)^k E(-Mt) dt.$$

La proposition III.5 nous donne l'égalité

$$(IV.2) \quad R_k(M) = \sum_{\substack{H \in \mathcal{H} \\ d^0 H \leq n}} \sum_{G \in \mathcal{G}_H} I_{k, G/H}(M).$$

PROPOSITION IV.1 Soit  $u \in \mathcal{P}$  de valuation  $v(u) > n$ . Alors,

- (i) si  $v(u) > 2n+1$ ,  $f(u) = q^{n+1}$ ,
- (ii) si  $v(u) = 2k$ , avec  $k \leq n$ ,  $f(u) = q^k$ ,
- (iii) si  $v(u) = 2k+1$ , avec  $k \leq n$ , et si  $a$  est l'élément de  $F_q^*$  tel que  $v(u - aX^{-2k-1}) > 2k+1$ ,

$$f(u) = q^k \sum_{b \in F_q} e(ab^2).$$

Démonstration. Compte tenu de la définition du caractère  $E$ , (i) est immédiat. Pour avoir (ii) et (iii) on écrit

$$(IV.3) \quad f(u) = 1 + \sum_{m=0}^n \sum_{B \in D_m} E(uB^2).$$

Soit  $m \in \{0, \dots, n\}$ . Si  $B \in D_m$ , il existe  $b \in F_q^*$ ,  $V \in F_{2m-1}$ , tels que

$$B^2 = b^2 X^{2m} + V,$$

donc tels que

$$E(uB^2) = E(ub^2 X^{2m})E(uV).$$

Il existe exactement  $q^m$  polynômes  $W \in F_{2m-1}$  tels que

$$d^0(B^2 - b^2 X^{2m} - W) < m,$$

et, pour de tels polynômes

$$E(uV) = E(uW).$$

D'autre part, si  $b \in F_q^*$  et si  $V \in F_{2m-1}$ , il existe un et un seul polynôme  $B$  tel que

$$d^0(B^2 - b^2 X^{2m} - V) < m.$$

En effet, une telle relation détermine le degré de  $B$  qui doit être égal à  $m$ ,  $\text{sgn}(B)$  qui doit être égal à  $b$ , elle exige de plus que les coefficients  $b_0, \dots, b_{m-1}$ ,  $b$  du polynôme  $B$  et les coefficients  $v_0, \dots, v_{2m-1}$  du polynôme  $V$  soient liés par les relations

$$v_{2m-1} = 2bb_{m-1},$$

et, pour  $j \in \{m-2, \dots, 1, 0\}$ ,

$$v_{m+j} = 2bb_j + \sum_{\substack{r+s=m+j \\ j < r < m \\ j < s < m}} b_r b_s,$$

ce qui détermine  $b_{m-1}, \dots, b_1, b_0$  de façon unique. On a donc pour  $m \in \{0, \dots, n\}$ ,

$$\sum_{B \in D_m} E(uB^2) = q^{-m} \sum_{b \in F_q^*} E(ub^2 X^{2m}) \sum_{V \in F_{2m-1}} E(uV),$$

d'où, avec (III.2)

$$(IV.4) \quad \sum_{B \in D_m} E(uB^2) = \begin{cases} q^m \sum_{b \in F_q^*} E(ub^2 X^{2m}) & \text{si } v(u) > 2m, \\ 0 & \text{si } v(u) \leq 2m. \end{cases}$$

D'autre part, d'après la définition du caractère  $E$ , pour tout élément  $b$  de  $F_q^*$ , si  $v(u) > 2m+1$ ,

$$E(ub^2 X^{2m}) = 1,$$

et, si  $v(u) = 2m+1$ , si  $a$  est l'élément de  $F_q^*$  tel que  $v(u - aX^{-2m-1}) > 2m+1$ ,

$$E(ub^2 X^{2m}) = e(ab^2).$$

Les égalités (IV.3) et (IV.4) donnent alors, pour  $v(u) = 2k$

$$f(u) = 1 + \sum_{m=0}^{k-1} q^m (q-1) = q^k,$$

et, pour  $v(u) = 2k+1$ ,  $a$  désignant l'élément de  $F_q^*$  tel que  $v(u - aX^{-2k-1}) > 2k+1$ ,

$$f(u) = 1 + \sum_{m=0}^{k-1} q^m (q-1) + q^k \sum_{b \in F_q^*} e(ab^2) = q^k \sum_{b \in F_q^*} e(ab^2).$$

On remarque que si  $u \in \mathcal{P}$  est de valuation  $k > n$ , si  $a \in F_q^*$  est tel que  $v(u - aX^{-k}) > k$ ,  $f(u)$  ne dépend que de  $k$  et de  $a$ . Posons pour  $v \in \mathcal{P}_k$ , pour  $a \in F_q^*$ ,

$$(IV.5) \quad f(aX^{-k} + v) = g(k, a).$$

PROPOSITION IV.2. Soit  $t = G/\tilde{H} + u$  appartenant à l'arc de Farey  $\mathcal{U}_{G,H}$ . Alors,

$$(IV.6) \quad f(t) = |H|^{-1} S(G, H) f(u),$$

où

$$(IV.7) \quad S(G, H) = \sum_{R \in \mathcal{G}_{\tilde{H}}} E((G/H)R^2).$$

Démonstration. On a

$$\begin{aligned} f((G/H) + u) &= \sum_{R \in \mathcal{G}_H} \sum_{L \in F_{n-d^0_H}} E(((G/H) + u)(R + LH)^2) \\ &= \sum_{R \in \mathcal{G}_H} E((G/H)R^2) \sum_{L \in F_{n-d^0_H}} E(u(R + LH)^2). \end{aligned}$$

Comme  $v(u) > n + d^0H$ , pour  $R \in \mathcal{C}_H$ , pour  $L \in F_{n-d^0H}$

$$v(u(R^2 + 2RLH)) > 1$$

et

$$f((G/H) + u) = \sum_{R \in \mathcal{C}_H} E((G/H)R^2) \sum_{L \in F_{n-d^0H}} E(uL^2H^2).$$

D'autre part,

$$\begin{aligned} |H| \sum_{L \in F_{n-d^0H}} E(uL^2H^2) &= \sum_{R \in \mathcal{C}_H} \sum_{L \in F_{n-d^0H}} E(uL^2H^2) \\ &= \sum_{R \in \mathcal{C}_H} \sum_{L \in F_{n-d^0H}} E(u(L^2H^2 + 2RLH + R^2)) \\ &= \sum_{B \in F_n} E(uB^2) = f(u). \end{aligned}$$

PROPOSITION IV.3. Soit

$$(IV.8) \quad A_k(M) = \begin{cases} r_k(\text{sgn}(M)) & \text{si } M \text{ est de degré pair,} \\ r_k(0) - 1 & \text{si } M \text{ est de degré impair.} \end{cases}$$

Alors, pour toute fraction de Farey  $G/H$ ,

$$(IV.9) \quad I_{k,G/H}(M) = q^{n(k-2)} A_k(M) |H|^{-k} S^k(G, H) E(-M(G/H)).$$

Démonstration. Posons

$$J_{k,H}(M) = \int_{v(u) > n + d^0H} f^k(u) E(-Mu) du.$$

Alors, avec (IV.6)

$$I_{k,G/H}(M) = |H|^{-k} S^k(G, H) E(-M(G/H)) J_{k,H}(M).$$

La proposition IV.1 permet le calcul de  $J_{k,H}(M)$ . Compte tenu de (IV.5) on a

$$\begin{aligned} J_{k,H}(M) &= q^{(n+1)k} \int_{v(u) > 2n+1} E(-Mu) du + \\ &+ \sum_{j=n+d^0H+1}^{2n+1} \sum_{a \in F_q^*} g(a, j)^k E(-aM/X^j) \int_{v(v) > j} E(-Mv) dv; \end{aligned}$$

(III.1) donne alors

$$J_{k,H}(M) = q^{(n+1)k - 2n - 1} + \sum_{j=d^0M+1}^{2n+1} q^{-j} \sum_{a \in F_q^*} g(a, j)^k E(-aMX^{-j}).$$

Dans le cas où  $d^0 M = 2n$  on a

$$J_{k,H}(M) = q^{n(k-2)+k-1} + q^{n(k-2)-1} \sum_{a \in \mathbb{F}_q} \left( \sum_{b \in \mathbb{F}_q} e(ab^2) \right)^k e(-a \operatorname{sgn}(M)),$$

$$J_{k,H}(M) = q^{n(k-2)-1} \left( q^k + \sum_{b_1 \in \mathbb{F}_q} \dots \sum_{b_k \in \mathbb{F}_q} \sum_{a \in \mathbb{F}_q} e(a(b_1^2 + \dots + b_k^2 - \operatorname{sgn}(M))) \right),$$

$$J_{k,H}(M) = q^{n(k-2)-1} \left( q^k + r_k(\operatorname{sgn}(M))(q-1) - (q^k - r_k(\operatorname{sgn}(M))) \right),$$

$$J_{k,H}(M) = q^{n(k-2)} r_k(\operatorname{sgn}(M)).$$

Dans le cas où  $d^0 M = 2n-1$  on a

$$J_{k,H}(M) = q^{n(k-2)+k-1} + q^{n(k-2)} \sum_{a \in \mathbb{F}_q} e(-a \operatorname{sgn}(M)) + q^{n(k-2)-1} \sum_{a \in \mathbb{F}_q} \left( \sum_{b \in \mathbb{F}_q} e(ab^2) \right)^k,$$

d'où,

$$J_{k,H}(M) = q^{n(k-2)} (r_k(0) - 1).$$

**COROLLAIRE.** Le nombre  $R_k(M)$  de représentations restreintes de  $M$  comme sommes  $k$  carrés est donné par la relation

$$(IV.10) \quad R_k(M) = q^{n(k-2)} A_k(M) \mathcal{S}_k(M),$$

où

$$(IV.11) \quad \mathcal{S}_k(M) = \sum_{\substack{H \in \mathcal{H} \\ d^0 H \leq n}} \sum_{G \in \mathcal{G}_H} |H|^{-k} S^k(G, H) E(-M(G/H)).$$

## V. Sommes de $k$ carrés dans un corps fini

Dans ce paragraphe  $F_s$  est un corps fini à  $s$  éléments,  $s$  étant un entier impair. Les résultats établis ici seront utilisés pour des corps  $F_s$  extensions finies du corps  $F_q$ .

Si  $a \in F_s$ , on désigne encore, pour tout entier  $j \geq 1$ , par  $r_j(a)$  le nombre de solutions  $(a_1, \dots, a_j) \in F_s^j$  de l'équation

$$a = a_1^2 + \dots + a_j^2.$$

On désigne aussi par  $\lambda$  le caractère quadratique du groupe multiplicatif  $F_s^*$ . On a immédiatement

$$(V.1) \quad \sum_{u \in F_s^*} \lambda(u) = 0.$$

On a aussi le

**THÉORÈME.** (1)  $r_1(0) = 1$ ;

(2) si  $a$  est un élément non nul de  $F_s$ ,  $r_1(a) = 1 + \lambda(a)$ ;

(3) pour tout entier  $k \geq 1$ , pour tout élément  $a \in F_s$ , non nul,

$$(V.2) \quad r_{2k}(0) = s^{2k-1} - s^{k-1} \lambda(-1)^k + s^k \lambda(-1)^k,$$

$$(V.3) \quad r_{2k+1}(0) = s^{2k},$$

$$(V.4) \quad r_{2k}(a) = s^{2k-1} - s^{k-1} \lambda(-1)^k,$$

$$(V.5) \quad r_{2k+1}(a) = s^{2k} + s^k \lambda(-1)^k \lambda(a).$$

Démonstration. Les (1) et (2) sont immédiats. On démontre (V.2) et (V.4) par récurrence sur l'entier  $k$ . Posons

$$\lambda(-1) = \varepsilon.$$

Si  $-1$  n'est pas carré dans  $F_s$ ,  $r_2(0) = 1$ ,  $\varepsilon = -1$ , et  $r_2(0) = s - \varepsilon + s\varepsilon$ . Si  $-1$  est carré dans  $F_s$ ,  $r_2(0) = 2(s-1) + 1$ ,  $\varepsilon = 1$  et  $r_2(0) = s - \varepsilon + s\varepsilon$ . Si  $a$  est un élément non nul de  $F_s$ ,

$$r_2(a) = \sum_{b \in F_s} r_1(a-b^2) = \sum_{b \in F_s} r_1(a-b)r_1(b),$$

d'où, en utilisant les (1) et (2),

$$r_2(a) = \sum_{\substack{b \in F_s \\ b \neq a}} (1 + \lambda(a-b))(1 + \lambda(b)) + 2 + 2\lambda(a),$$

$$r_2(a) = s + \sum_{\substack{b \in F_s \\ b \neq a}} \lambda(a-b) + \sum_{\substack{b \in F_s \\ b \neq a}} \lambda(b) + 2\lambda(a) + \sum_{\substack{b \in F_s \\ b \neq a}} \lambda(a-b)\lambda(b),$$

d'où, avec (V.1),

$$r_2(a) = s + \sum_{\substack{b \in F_s \\ b \neq a}} \lambda(ab^{-1} - 1) = s - \lambda(-1).$$

Les relations (V.2) et (V.4) sont établies pour  $k = 1$ . On a, pour tout élément  $a \in F_s$ , pour tout entier  $k \geq 1$ ,

$$r_{2k+2}(a) = \sum_{b \in F_s} r_{2k}(a-b)r_2(b);$$

cette formule de récurrence permet d'établir (V.2) et (V.4) pour tout entier  $k \geq 1$ . On obtient alors les égalités (V.3) et (V.5) à partir de la relation.

$$r_{2k+1}(a) = \sum_{b \in F_s} r_{2k}(a-b)r_1(b).$$

## VI. Les séries singulières $\mathfrak{S}_k(M)$

Posons, pour tout entier  $k \geq 1$ , pour tout polynôme  $A$ , pour tout polynôme  $H$  non nul

$$(VI.1) \quad C_k(A, H) = |H|^{-k} \sum_{G \in \mathfrak{C}_H} S^k(G, H)E(-A(G/H)).$$

Les 3 propositions suivantes se démontrent comme les théorèmes 8.4, 8.5, 8.7 et 8.8, chapitre IV de [1] avec quelques simplifications pour la dernière proposition, ce qui permet d'avoir une égalité au lieu d'une majoration.

PROPOSITION VI.1. Pour tout entier  $k \geq 1$ , pour tout polynôme  $A$ , la fonction

$$Q \mapsto C_k(A, Q)$$

est multiplicative.

PROPOSITION VI.2. Si  $P$  est un polynôme irréductible, si  $G$  est un polynôme premier à  $P$ ,

$$|S(G, P)| = |P|^{1/2},$$

et pour tout entier  $m > 0$ ,

$$(VI.2) \quad |S(G, P^{2m})| = |P|^m,$$

$$(VI.3) \quad |S(G, P^{2m+1})| = |P|^m S(G, P).$$

PROPOSITION VI.3. Si  $G$  et  $H$  sont des polynômes premiers entre eux,

$$(VI.4) \quad |S(G, H)| = |H|^{1/2}.$$

COROLLAIRE. Soient un entier  $k \geq 1$ ,  $A$  un polynôme et  $H$  un polynôme non nul. Alors,

$$(VI.5) \quad |C_k(A, H)| \leq |H|^{1-k/2}.$$

Démonstration. Immédiate.

PROPOSITION VI.4. Soit un entier  $k \geq 5$ . Alors il existe une constante  $a_1 = a_1(q, k) \leq \sqrt{q}(\sqrt{q}-1)^{-1}$ , ne dépendant que de  $q$  et de  $k$ , telle que, pour tout entier  $t \geq 0$ ,

$$(VI.6) \quad \sum_{\substack{Q \in \mathcal{A} \\ d^0 Q \geq t}} |C_k(A, Q)| \leq a_1 q^{-t(k-4)/2}.$$

Démonstration. Avec (VI.5) il vient

$$\sum_{\substack{Q \in \mathcal{A} \\ d^0 Q \geq t}} |C_k(A, Q)| \leq q^{-t(k-4)/2} \sum_{h=0}^{\infty} q^{-h(k-4)/2} \leq q^{-t(k-4)/2} \sum_{h=0}^{\infty} q^{-h/2}.$$

La majoration (VI.5) montre aussi que, pour tout polynôme  $A$ , la série

$$(VI.7) \quad \mathfrak{S}_k(A) = \sum_{Q \in \mathcal{A}} C_k(A, Q)$$

est absolument convergente lorsque  $k$  est supérieur ou égal à 5. De plus, on a la

PROPOSITION VI.5. Il existe des constantes  $a_2 = a_2(q)$ ,  $a_3 = a_3(q)$ , stricte-

ment positives, ne dépendant que de  $q$ , telles que, pour tout polynôme  $M$ , pour tout entier  $k \geq 5$ ,

$$(VI.8) \quad a_2 \leq \mathfrak{S}_k(M) \leq a_3.$$

Démonstration. Soit un entier  $k \geq 5$  et  $M$  un polynôme. La somme  $\mathfrak{S}_k(M)$  s'écrit comme produit eulérien absolument convergent

$$(i) \quad \mathfrak{S}_k(M) = \prod_{P \in \mathcal{P}} \Psi_k(M, P),$$

où, pour tout polynôme irréductible  $P$ ,

$$\Psi_k(M, P) = \sum_{j=0}^{\infty} C_k(M, P^j).$$

Une étude précise montrerait que les sommes  $\Psi_k(M, P)$  sont finies, mais nous n'utiliserons pas ce résultat ici. Avec la majoration (VI.5) on a, pour tout polynôme irréductible  $P$ ,

$$|\Psi_k(M, P) - 1| \leq \sum_{j=1}^{\infty} |P|^{j(1-k/2)} = (|P|^{k/2-1} - 1)^{-1},$$

or,

$$|P|^{k/2-1} \geq |P|^{3/2} - 1 \geq |P|^{5/4},$$

d'où,

$$(ii) \quad 1 - |P|^{-5/4} \leq \Psi_k(M, P) \leq 1 + |P|^{-5/4}.$$

Désignons par  $a_2(q)$  et  $a_3(q)$  les produits absolument convergents

$$\prod_{P \in \mathcal{P}} (1 - |P|^{-5/4}) \quad \text{et} \quad \prod_{P \in \mathcal{P}} (1 + |P|^{-5/4});$$

(VI.8) se déduit alors de (i) et de (ii).

Pour  $k \leq 4$ , la relation (VI.7) ne définit pas une série absolument convergente; les sommes  $\mathfrak{S}_4(M)$  et  $\mathfrak{S}_3(M)$  seront définies d'une autre façon qui demande une étude plus précise des nombres  $C_4(M, Q)$  et  $C_3(M, Q)$ .

**PROPOSITION VI.6.** Soient  $P$  un polynôme irréductible et  $A$  un polynôme non divisible par  $P$ . Alors, pour tout entier  $m > 0$ ,

$$(VI.9) \quad \sum_{G \in \mathcal{G}_{P^m}} E(AG/P^m) = \begin{cases} -1 & \text{si } m = 1, \\ 0 & \text{si } m > 1. \end{cases}$$

Démonstration. Si  $m = 1$ , on applique le corollaire de la proposition III.4

$$0 = \sum_{G \in \mathcal{G}_P} E(AG/P) = 1 + \sum_{G \in \mathcal{G}_P} E(AG/P);$$



si  $m > 1$ ,

$$\sum_{G \in \mathfrak{G}_{P^m}^*} E(AG/P^m) = \sum_{R \in \mathfrak{G}_{P^{m-1}}^*} E(AR/P^m) \sum_{Q \in \mathfrak{G}_P} E(AQ/P),$$

et le corollaire de la proposition III.4 donne encore le résultat annoncé.

PROPOSITION VI.7. Soient  $P$  un polynôme irréductible et  $A$  un polynôme de valuation  $P$ -adique  $v$ . Alors, pour tout entier  $m > 0$ ,

$$(VI.10) \quad C_4(A, P^m) = \begin{cases} (|P|-1)|P|^{-m-1} & \text{si } m \leq v, \\ -|P|^{-m-1} & \text{si } m = v+1, \\ 0 & \text{si } m > v+1. \end{cases}$$

Démonstration. Supposons d'abord  $m$  pair; alors, d'après (VI.2),

$$C_4(A, P^m) = |P|^{-4m} |P|^{2m} \sum_{G \in \mathfrak{G}_{P^m}^*} E(-AG/P^m),$$

si  $v \geq m$ ,

$$C_4(A, P^m) = (|P|-1)|P|^{-m-1},$$

si  $v < m$ , posons  $A = P^v A'$ , alors,

$$C_4(A, P^m) = |P|^{-2m} \sum_{Q \in \mathfrak{G}_{P^v}^*} \sum_{R \in \mathfrak{G}_{P^{m-v}}^*} E(-A'R/P^{m-v}),$$

et la proposition précédente donne

$$C_4(A, P^m) = \begin{cases} -|P|^{-2m+v} & \text{si } m-v = 1, \\ 0 & \text{si } m-v > 1. \end{cases}$$

Les égalités (VI.10) sont établies lorsque  $m$  est pair. Examinons le cas où  $m$  est impair. Posons  $m = 2j+1$ . D'après (VI.3),

$$C_4(A, P^m) = |P|^{-4m+4j} \sum_{G \in \mathfrak{G}_{P^m}^*} S^4(G, P) E(-AG/P^m).$$

D'après la définition de  $S(G, P)$ , si les polynômes  $G$  et  $R$  sont congrus modulo  $P$ ,  $S(G, P) = S(R, P)$ , donc

$$C_4(A, P^m) = |P|^{-4m+4j} \sum_{R \in \mathfrak{G}_P^*} S^4(R, P) E(-RA/P^m) \sum_{Q \in \mathfrak{G}_{P^{m-1}}^*} E(-QA/P^{m-1}).$$

On utilise encore le corollaire de la proposition III.4. Si  $m-1 > v$ ,  $C_4(A, P^m) = 0$ , si  $m-1 \leq v$ ,

$$C_4(A, P^m) = |P|^{-3m+4j-1} \sum_{R \in \mathfrak{G}_P^*} S^4(R, P) E(-RA/P^m).$$



Posons  $A' = A/P^v$  si  $m = v+1$ ,  $A' = 0$  si  $m \leq v$ . Alors,

$$C_4(A, P^m) = |P|^{-3m+4j-1} \sum_{R \in \mathcal{C}_P} S^4(R, P) E(-RA'/P),$$

$$C_4(A, P^m) = |P|^{-3m+4j-1} \sum_{R \in \mathcal{C}_P} \sum_{A_1 \in \mathcal{C}_P} \dots \sum_{A_4 \in \mathcal{C}_P} E((R/P)(A_1^2 + \dots + A_4^2 - A')),$$

$$C_4(A, P^m) = |P|^{-3m+4j-1} ((|P|-1)\omega_P(A') - (|P|^4 - \omega_P(A'))),$$

$\omega_P(A')$  désignant le nombre de solutions  $(A_1, \dots, A_4) \in \mathcal{C}_P^4$  de la congruence

$$A' \equiv A_1^2 + \dots + A_4^2 \pmod{P}.$$

L'étude faite au chapitre précédent montre que

$$\omega_P(A') = \begin{cases} |P|^3 - |P| & \text{si } A' \not\equiv 0 \pmod{P}, \\ |P|^3 - |P| + |P|^2 & \text{si } A' \equiv 0 \pmod{P}. \end{cases}$$

Donc,

$$C_4(M, P^m) = \begin{cases} -|P|^{-3m+4j+1} & \text{si } m = v+1, \\ (|P|-1)|P|^{-3m+4j+1} & \text{si } m \leq v; \end{cases}$$

Les égalités (VI.10) sont ainsi démontrées pour  $m$  impair.

Si  $P$  est un polynôme irréductible ne divisant pas le polynôme  $A$ , on définit le symbole de Legendre  $\left(\frac{A}{P}\right)$  par

$$\left(\frac{A}{P}\right) = \begin{cases} 1 & \text{si } A \text{ est carré modulo } P, \\ -1 & \text{si } A \text{ n'est pas carré modulo } P. \end{cases}$$

**PROPOSITION VI.8.** Soient  $P$  un polynôme irréductible et  $A$  un polynôme de valuation  $P$ -adique  $v$ . Alors, pour tout entier  $m > 0$ ,

$$(VI.11) \quad C_3(A, P^{2m}) = \begin{cases} 0 & \text{si } 2m > v+1, \\ (|P|-1)|P|^{-m-1} & \text{si } 2m \leq v, \\ -|P|^{-m-1} & \text{si } 2m = v+1, \end{cases}$$

et, pour tout entier  $m \geq 0$ ,

$$(VI.12) \quad C_3(A, P^{2m+1}) = \begin{cases} 0 & \text{si } 2m > v, \\ 0 & \text{si } 2m+1 \leq v, \\ |P|^{-m-1} \left(\frac{-A'}{P}\right) & \text{si } 2m = v \text{ et si } A = P^v A'. \end{cases}$$

**Démonstration.** On procède comme pour la proposition précédente.

On utilise le fait que le nombre de solutions de la congruence

$$A \equiv A_1^2 + A_2^2 + A_3^2 \pmod{P}$$

est  $|P|^2 + |P| \left( \frac{-A}{P} \right)$  si  $P$  ne divise pas  $A$ , et qu'il est  $|P|^2$  si  $P$  divise  $A$ .

Ces deux propositions montrent que si  $Q$  est un polynôme premier à  $A$  ayant un facteur carré,  $C_4(A, Q) = C_3(A, Q) = 0$ , que, si  $K$  est un polynôme dont les facteurs irréductibles sont pris parmi les facteurs irréductibles de  $A$ , s'il existe un polynôme irréductible  $P$  divisant  $K$  avec une valuation  $v_P(K) > v_P(A) + 1$ , les sommes  $C_4(A, K)$  et  $C_3(A, K)$  sont nulles.

Dans les sommes  $\mathcal{S}_3(M)$  et  $\mathcal{S}_4(M)$  nous n'aurons à considérer que les termes  $C_k(M, H)$  où  $H$  s'écrit comme produit  $QK$ ,  $Q$  étant un polynôme sans facteur carré premier à  $M$ ,  $K$  décrivant un ensemble  $\mathcal{K}_M$  de polynômes unitaires que l'on va définir.

Si  $A$  est un polynôme unitaire de degré strictement positif, si

$$A = aP_1^{v_1} \dots P_r^{v_r},$$

$a$  étant un élément de  $F_q$ ,  $P_1, \dots, P_r$  étant des polynômes irréductibles distincts,  $v_1, \dots, v_r$  étant des entiers strictement positifs,  $\mathcal{K}_A$  désigne l'ensemble des polynômes unitaires

$$K = P_1^{k_1} \dots P_r^{k_r},$$

où pour  $i \in \{1, \dots, r\}$ ,  $k_i \in \{0, 1, \dots, v_i + 1\}$ .

Si  $A$  est une constante, l'ensemble  $\mathcal{K}_A$  sera réduit au polynôme 1.

PROPOSITION VI.9. *Pour tout réel  $\varepsilon > 0$ , il existe une constante  $c(q, \varepsilon)$ , ne dépendant que de  $q$  et de  $\varepsilon$ , telle que, pour tout polynôme  $A$ ,*

$$(VI.13) \quad \text{Card}(\mathcal{K}_A) \leq c(q, \varepsilon) |A|^\varepsilon.$$

Démonstration. Si  $A$  est une constante,  $\text{Card}(\mathcal{K}_A) = 1 = |A|$ . Si  $A$  n'est pas une constante,

$$\text{Card}(\mathcal{K}_A) = \prod_{\substack{P \in \mathcal{P} \\ P|A}} (v_P(A) + 2).$$

On obtient (VI.13) par une majoration analogue à celle du nombre  $d(A)$  de diviseurs unitaires de  $A$  comme pour le lemme 5.1, chapitre IV de [1].

PROPOSITION VI.10. *Pour tout polynôme  $M$ , la série*

$$(VI.14) \quad S(M) = \sum_{\substack{Q \in \mathcal{Q} \\ (Q, M) = 1}} \mu(Q) |Q|^2$$

est absolument convergente. Soit

$$(VI.15) \quad \mathfrak{S}_4(M) = S(M) \sum_{K \in \mathcal{K}_M} C_4(M, K);$$

alors,

$$(VI.16) \quad \mathfrak{S}_4(M) = ((q-1)/q) \sum_{\substack{D \in \mathcal{D} \\ D|M}} |D|^{-1},$$

et

$$(VI.17) \quad ((q-1)/q) \leq \mathfrak{S}_4(M) \leq ((q-1)/q) |M|/\Phi(M).$$

**Démonstration.** La somme  $\mathcal{S}(M)$  s'écrit comme produit eulérien absolument convergent

$$\mathcal{S}(M) = \prod_{\substack{P \in \mathcal{P} \\ P \nmid M}} (1 - |P|^{-2}),$$

d'autre part, avec (VI.10) et la définition de l'ensemble  $\mathcal{K}_M$ ,

$$\sum_{K \in \mathcal{K}_M} C_4(M, K) = \prod_{\substack{P \in \mathcal{P} \\ P|M}} \left( 1 + \sum_{j=1}^{v_P(M)} (|P|-1) |P|^{-j-1} - |P|^{-v_P(M)-2} \right),$$

d'où,

$$\mathfrak{S}_4(M) = \left\{ \prod_{P \in \mathcal{P}} (1 - |P|^{-2}) \right\} \left\{ \prod_{\substack{P \in \mathcal{P} \\ P|M}} \left( \frac{1 + |P|^{-1} - |P|^{-v_P(M)-1} - |P|^{-v_P(M)-2}}{1 - |P|^{-2}} \right) \right\},$$

$$(i) \quad \mathfrak{S}_4(M) = ((q-1)/q) \prod_{\substack{P \in \mathcal{P} \\ P|M}} \left( \frac{1 - |P|^{-v_P(M)-1}}{1 - |P|^{-1}} \right),$$

$$\mathfrak{S}_4(M) = \sum_{\substack{P \in \mathcal{P} \\ P|M}} (1 + |P|^{-1} + \dots + |P|^{-v_P(M)}),$$

d'où la relation (VI.16). On a immédiatement

$$(q-1)/q \leq \mathfrak{S}_4(M)$$

et, de (i) on déduit

$$\mathfrak{S}_4(M) \leq ((q-1)/q) \prod_{\substack{P \in \mathcal{P} \\ P|M}} (|P|/(|P|-1)) = ((q-1)/q) |M|/\Phi(M).$$

**PROPOSITION VI.11.** Il existe une constante  $a_4 = a_4(q)$ , ne dépendant que de  $q$ , telle que, pour tout polynôme  $A$  de degré au moins égal à 2,

$$(VI.18) \quad |A|/\Phi(A) \leq a_4 \log(d^0 A).$$

Démonstration. Comme pour le théorème 5.1, chapitre I de [16].

PROPOSITION VI.12. *Pour tout réel  $\varepsilon > 0$ , il existe une constante  $\alpha(q, \varepsilon)$ , ne dépendant que de  $q$  et de  $\varepsilon$ , telle que, pour tout polynôme  $M$  de degré strictement positif, pour tout entier  $t \geq 0$ ,*

$$(VI.19) \quad |\mathfrak{S}_4(M) - \sum_{\substack{H \in \mathcal{H} \\ d^0 H \leq t}} C_4(M, H)| \leq \alpha(q, \varepsilon) q^{-t} |M|^\varepsilon.$$

Démonstration. Posons

$$U_t = \mathfrak{S}_4(M) - \sum_{\substack{H \in \mathcal{H} \\ d^0 H \leq t}} C_4(M, H).$$

Les sommes  $C_4(M, H)$  sont nulles sauf pour les polynômes  $H$  s'écrivant comme produit  $QK$  où  $Q$  est un polynôme sans facteur carré premier à  $M$ , où  $K$  appartient à l'ensemble  $\mathcal{X}_M$ , et dans ce cas, d'après les égalités (VI.10)

$$C_4(M, H) = \frac{\mu(Q)}{|Q|^2} C_4(M, K).$$

Donc,

$$U_t = \sum_{K \in \mathcal{X}_M} C_4(M, K) \sum_{\substack{Q \in \mathcal{H} \\ (Q, M) = 1}} \mu(Q)/|Q|^2 - \sum_{\substack{K \in \mathcal{X}_M \\ d^0 K \leq t}} C_4(M, K) \sum_{\substack{Q \in \mathcal{H} \\ (Q, M) = 1 \\ d^0(QK) \leq t}} \mu(Q)/|Q|^2,$$

$$U_t = V_t + V'_t,$$

avec

$$V_t = \sum_{\substack{K \in \mathcal{X}_M \\ d^0 K > t}} C_4(M, K) \sum_{\substack{Q \in \mathcal{H} \\ (Q, M) = 1}} \mu(Q)/|Q|^2 \quad \text{et} \quad V'_t = \sum_{\substack{K \in \mathcal{X}_M \\ d^0 K \leq t}} \sum_{\substack{Q \in \mathcal{H} \\ (Q, M) = 1 \\ d^0(QK) > t}} \mu(Q)/|Q|^2.$$

On a

$$\begin{aligned} \sum_{\substack{Q \in \mathcal{H} \\ (Q, M) = 1}} |\mu(Q)/|Q|^2| &\leq \sum_{Q \in U} |\mu(Q)/|Q|^2| = \prod_{P \in \mathcal{P}} (1 + 1/|P|^2) \leq \prod_{P \in \mathcal{P}} (1 - 1/|P|^2)^{-1} \\ &= q/(q-1). \end{aligned}$$

d'où,

$$|V_t| \leq \left( \sum_{\substack{K \in \mathcal{X}_M \\ d^0 K > t}} |C_4(M, K)| \right) q/(q-1),$$

et, avec (VI.5)

$$|V_t| \leq (q/(q-1)) \text{Card}(\mathcal{X}_M) q^{-t}.$$

D'autre part; toujours avec (VI.5)

$$|V_t| \leq \sum_{\substack{K \in \mathcal{X}_M \\ d^0 K \leq t}} |K|^{-1} \sum_{\substack{Q \in \mathcal{U} \\ d^0 Q > t - d^0 K}} |Q|^{-2} = (q^{-t}/(q-1)) \sum_{\substack{K \in \mathcal{X}_M \\ d^0 K \leq t}} 1 \leq \text{Card}(\mathcal{X}_M) q^{-t}/(q-1).$$

Les majorations (VI.13) et (VI.18) donnent le résultat annoncé.

On suppose maintenant que  $M$  est un polynôme de degré  $2n$  ou  $2n-1$  strictement positif, tel que  $-M$  ne soit pas carré dans  $F_q[X]$ . On pose

$$-M = U^2 D,$$

où  $U$  est un polynôme unitaire, où  $D$  est non constant et sans facteur carré.

On désigne par  $\chi$  le caractère modulo  $D$  défini sur  $\mathcal{U}$  par les conditions suivantes

(i) si le polynôme  $A$  n'est pas premier à  $D$ ,  $\chi(A) = 0$ ,

(ii) si  $P$  est un polynôme irréductible ne divisant pas  $D$ ,  $\chi(P) = \left(\frac{D}{P}\right)$ .

PROPOSITION VI.13. *Le caractère  $\chi$  n'est pas principal.*

Démonstration. Cela se déduit des propriétés des symboles locaux. (Voir par exemple [18], chapitre XIV, paragraphe 2, proposition 7.)

La fonction  $L(\chi, \cdot)$  associée au caractère modulaire  $\chi$  est définie sur  $\mathbb{C}$  par

$$(VI.20) \quad L(\chi, z) = \sum_{U \in \mathcal{U}} \chi(U) z^{d^0 U}.$$

PROPOSITION VI.14. *La fonction  $L(\chi, \cdot)$  est un polynôme de degré  $d$  où  $d = d^0 D - 2$  si  $d^0 D$  est pair, où  $d = d^0 D - 1$  si  $d^0 D$  est impair; les racines de ce polynôme sont deux à deux conjuguées, de module  $q^{-1/2}$ , et,*

$$(VI.21) \quad L(\chi, z) = \prod_{P \in \mathcal{P}} (1 - \chi(P) z^{d^0 P})^{-1}.$$

Démonstration. Cette proposition est démontrée dans [20], appendice 5.

Posons, pour tout entier  $m \geq 0$ ,

$$(VI.22) \quad h_m = \sum_{\substack{H \in \mathcal{U} \\ d^0 H = m \\ (H, M) = 1}} (\mu^2(H) \chi(H)) / |H|.$$

PROPOSITION VI.15. (1) *La série entière*

$$(VI.23) \quad H(z) = \sum_{m=0}^{\infty} h_m z^m$$

est absolument convergente dans le disque  $|z| < 1$ .

(2) Dans le disque  $|z| < 1$  on a,

$$(VI.24) \quad H(z) = (1/q)(q-z^2)L(\chi, z/q)\Gamma_M(z),$$

où,

$$(VI.25) \quad \Gamma_M(z) = \prod_{\substack{P \in \mathcal{J} \\ P|M}} (1 + \chi(P)(z/q)^{d^{0P}})^{-1} \times \prod_{\substack{P \in \mathcal{J} \\ P|D}} (1 - (z/q)^{2d^{0P}})^{-1}.$$

Démonstration. Le (1) se déduit de la majoration triviale  $|h_m| \leq 1$ .  
Plaçons nous dans le disque  $|z| < 1$ . La fonction

$$U \mapsto \mu^2(U)\chi(U)|U|^{-1}$$

étant multiplicative,

$$H(z) = \prod_{\substack{P \in \mathcal{J} \\ P|M}} (1 + \chi(P)|P|^{-1}z^{d^{0P}}) = \prod_{\substack{P \in \mathcal{J} \\ P|M}} (1 + \chi(P)(z/q)^{d^{0P}}).$$

Si  $P$  ne divise pas  $M$ ,  $P$  ne divise pas  $D$  et  $\chi(P)^2 = 1$ , d'où,

$$H(z) = \prod_{\substack{P \in \mathcal{J} \\ P|M}} (1 - (z/q)^{2d^{0P}})(1 - \chi(P)(z/q)^{d^{0P}})^{-1},$$

$$H(z) = \prod_{P \in \mathcal{J}} (1 - (z/q)^{2d^{0P}})(1 - \chi(P)(z/q)^{d^{0P}})^{-1} \times \\ \times \prod_{\substack{P \in \mathcal{J} \\ P|M}} ((-\chi(P)(z/q)^{d^{0P}})/(1 - (z/q)^{2d^{0P}})),$$

d'où, avec (VI.21),

$$H(z) = (1/q)(q-z^2)L(\chi, z) \left( \prod_{\substack{P \in \mathcal{J} \\ P|M \\ P|D}} (1 + \chi(P)(z/q)^{d^{0P}})^{-1} \right) \left( \prod_{\substack{P \in \mathcal{J} \\ P|D}} (1 - (z/q)^{2d^{0P}})^{-1} \right).$$

La fonction  $\Gamma_M$  n'a qu'un nombre fini de poles de module  $q$ ; l'égalité (VI.24) donne un prolongement analytique de  $H$  dans le disque  $|z| < q$ . Le nombre  $H(1)$  ayant ainsi un sens, posons

$$(VI.26) \quad \mathfrak{S}_3(M) = H(1) \sum_{K \in \mathcal{X}_M} C_3(M, K).$$

PROPOSITION VI.16. On a les inégalités

$$(VI.27) \quad \frac{q-1}{q} \left( \frac{\sqrt{q}-1}{\sqrt{q}} \right)^{2n-2} \Phi(M)/|M| \\ \leq \mathfrak{S}_3(M) \leq \left( \frac{\sqrt{q}+1}{\sqrt{q}} \right)^{2n-2} (|M|/\Phi(M))^2.$$

Démonstration. La proposition précédente nous donne

$$(i) \mathfrak{S}_3(M) = ((q-1)/q) L(\chi, 1/q) \left( \prod_{\substack{P \in \mathcal{J} \\ P|M}} (1 + \chi(P)|P|^{-1})^{-1} \right) \left( \prod_{\substack{P \in \mathcal{J} \\ P|D}} (1 - |P|^{-2})^{-1} \right) T(M),$$

où,

$$T(M) = \sum_{K \in \mathcal{X}_M} C_3(M, K).$$

On a

$$(q-1)/q \leq ((q-1)/q) \prod_{\substack{P \in \mathcal{J} \\ P|D}} (1 - |P|^{-2})^{-1} \leq ((q-1)/q) \prod_{P \in \mathcal{J}} (1 - |P|^{-2})^{-1},$$

$$(ii) \quad (q-1)/q \leq \prod_{\substack{P \in \mathcal{J} \\ P|D}} (1 - |P|^{-2})^{-1} \leq 1.$$

Le polynôme  $L(\chi, z)$  peut se factoriser de la façon suivante

$$L(\chi, z) = \prod_{i=1}^{d/2} (1 - (\varrho_i + \bar{\varrho}_i)z + qz^2),$$

$\varrho_1, \dots, \varrho_{d/2}$  étant des nombres complexes de module  $q^{1/2}$ , d'où,

$$(1 - q^{-1/2})^d \leq L(\chi, 1/q) \leq (1 + q^{-1/2})^d.$$

Or,  $d$  est égal à  $d^0D - 2$  ou  $d^0D - 1$  suivant que  $D$  diviseur de  $M$  est de degré pair ou impair, le polynôme  $M$  étant de degré  $2n$  ou  $2n-1$ . Donc,

$$d \leq 2n - 2,$$

et,

$$(VI.28) \quad \left( \frac{\sqrt{q}-1}{\sqrt{q}} \right)^{2n-2} \leq L(\chi, 1/q) \leq \left( \frac{\sqrt{q}+1}{\sqrt{q}} \right)^{2n-2}.$$

La définition de l'ensemble  $\mathcal{X}_M$  donne

$$T(M) = \prod_{\substack{P \in \mathcal{J} \\ P|M}} \left( 1 + \sum_{j=1}^{v_P(M)+1} C_3(M, P^{3j}) \right).$$

Désignons par  $\mathcal{D}_0$ , respectivement  $\mathcal{D}_1$ , l'ensemble des diviseurs irréductibles  $P$  de  $M$  tels que  $v_P(M)$  soit pair, respectivement impair. Posons pour  $P \in \mathcal{D}_0$ ,  $v_P(M) = 2u_P$  et pour  $P \in \mathcal{D}_1$ ,  $v_P(M) = 2u_P + 1$ . Posons aussi

$$M_P = MP^{-v_P(M)}.$$



Alors, d'après la proposition VI.8,

$$T(M) = \prod_{P \in \mathcal{D}_0} \left( 1 + \sum_{j=1}^{u_P} (|P|-1)|P|^{-j-1} + |P|^{-u_P-1} \left( \frac{-M_P}{P} \right) \right) \times \\ \times \prod_{P \in \mathcal{D}_1} \left( 1 + \sum_{j=1}^{u_P} (|P|-1)|P|^{-j-1} - |P|^{-u_P-2} \right), \\ T(M) = \prod_{P \in \mathcal{D}_0} \left( 1 + 1/|P| - |P|^{-u_P-1} \left( 1 - \left( \frac{-M_P}{P} \right) \right) \right) \times \prod_{P \in \mathcal{D}_1} \left( 1 + 1/|P| - \right. \\ \left. - |P|^{-u_P-1} - |P|^{-u_P-2} \right).$$

Si  $P \in \mathcal{D}_0$ ,  $v_P(M)$  est pair,  $P$  ne divise pas  $D$  et  $\left( \frac{-M_P}{P} \right) = \chi(P)$ , si  $P \in \mathcal{D}_0$ ,  $u_P \geq 1$ , si  $P \in \mathcal{D}_1$ ,  $u_P \geq 0$ , donc,

$$T(M) \prod_{\substack{P \in \mathcal{J} \\ P|M}} \left( 1 + \chi(P)|P|^{-1} \right)^{-1} = \prod_{P \in \mathcal{D}_0} \left( 1 + \frac{1}{|P|} - |P|^{-u_P-1} (1 - \chi(P)) \right) \times \\ \times \left( 1 + \chi(P)|P|^{-1} \right)^{-1} \prod_{P \in \mathcal{D}_1} (1 + 1/|P|) (1 - |P|^{-u_P-1}) (1 + \chi(P)|P|^{-1})^{-1}, \\ \prod_{\substack{P \in \mathcal{J} \\ P|M}} (1 - 1/|P|) \leq T(M) \prod_{\substack{P \in \mathcal{J} \\ P|M}} \left( 1 + \chi(P)|P|^{-1} \right)^{-1} \leq \prod_{\substack{P \in \mathcal{J} \\ P|M}} (1 + 1/|P|) (1 - 1/|P|)^{-1}, \\ \Phi(M)/|M| \leq T(M) \prod_{\substack{P \in \mathcal{J} \\ P|M}} \left( 1 + \chi(P)|P|^{-1} \right)^{-1} \leq (|M|/\Phi(M))^2.$$

Les relations (i), (ii) et (VI.28) donnent alors (VI.27).

PROPOSITION VI.17. Pour tout entier  $m \geq 0$ ,

$$(VI.29) \quad |h_m| \leq \frac{\sqrt{n}}{\sqrt{\pi}} \left( \frac{4q}{(\sqrt{q}-1)^2} \right)^n q^{-m/2} |M|/\Phi(M).$$

Démonstration. Posons pour  $z \in \mathbb{C}$ ,

$$L(\chi, z) = \sum_{j=0}^d \lambda_j z^j,$$

et, pour  $z \in \mathbb{C}$ , de module strictement inférieur à  $q$ ,

$$\Gamma_M(z) = \sum_{j=0}^{\infty} \gamma_j z^j.$$

Avec (VI.24), on a, pour tout entier  $m \geq 0$ ,

$$(i) \quad h_m = \beta_0 \gamma_m + \dots + \beta_m \gamma_0.$$

où,

$$(ii) \quad \begin{aligned} \beta_0 &= \lambda_0, & \beta_1 &= \lambda_1/q, \\ \beta_k &= \lambda_k q^{-k} - \lambda_{k-2} q^{1-k} & \text{si } k \in \{2, \dots, d\}, \\ \beta_{d+1} &= -\lambda_{d-1} q^{-d}, & \beta_{d+2} &= -\lambda_d q^{-d-1}, \\ \beta_k &= 0 & \text{si } k > d+2. \end{aligned}$$

Le polynôme  $L(\chi, z)$  peut encore se factoriser de la façon suivante:

$$L(\chi, z) = \prod_{j=1}^d (1 - \theta_j z),$$

$\theta_1, \dots, \theta_d$  étant des nombres complexes de module  $q^{1/2}$ ; d'où, pour  $k \in \{0, \dots, d\}$ ,

$$|\lambda_k| \leq \binom{d}{k} q^{k/2} \leq \binom{2n-2}{k} q^{k/2} \leq \binom{2n-2}{n-1} q^{k/2}.$$

Pour  $n > 1$ , la formule de Stirling donne la majoration

$$|\lambda_k| \leq 4^{n-1} \pi^{-1/2} (n-1)^{-1/2} q^{k/2}.$$

Posons

$$(iii) \quad \theta_n = \begin{cases} 1 & \text{si } n = 1, \\ 4^{n-1} \pi^{-1/2} (n-1)^{-1/2} & \text{si } n > 1, \end{cases}$$

on aura pour tout entier  $k \in \{0, \dots, d\}$ ,

$$(iv) \quad |\lambda_k| \leq \theta_n q^{k/2}.$$

Pour  $z = q^{1/2}$ ,

$$|\Gamma_M(z)| \leq \left( \prod_{\substack{P \in \mathcal{P} \\ P|M}} (1 - |P|^{-1/2})^{-1} \right) \left( \prod_{\substack{P \in \mathcal{P} \\ P \nmid M}} (1 - |P|^{-1})^{-1} \right) \leq \left( \frac{\sqrt{q}}{\sqrt{q}-1} \right)^{d^0 M} |M|/\Phi(M).$$

La formule de Cauchy appliquée au cercle  $|z| = q^{1/2}$  donne

$$(v) \quad |\gamma_k| \leq \left( \frac{\sqrt{q}}{\sqrt{q}-1} \right)^{d^0 M} |M| q^{-k/2} / \Phi(M).$$

La majoration de  $|h_m|$  se déduit des relations (i), (ii), (iv) et (v).

Posons

$$\Lambda(M) = \theta_n \left( \frac{\sqrt{q}}{\sqrt{q}-1} \right)^{d^0 M} |M|/\Phi(M).$$

On a pour tout entier  $m \geq 0$ ,

$$|h_m| \leq 2\Lambda(M)(d+1)q^{-m/2},$$

en majorant  $d$  par  $2n-2$ ,  $d^0 M$  par  $2n$ , on obtient avec (iii),

$$|h_m| \leq \frac{4^n \sqrt[n]{n}}{\sqrt{\pi}} \left( \frac{\sqrt{q}}{\sqrt{q-1}} \right)^{2n} |M|/\Phi(M),$$

ce qui est la relation (VI.29).

**PROPOSITION VI.18.** *Pour tout réel  $\varepsilon > 0$ , il existe une constante  $\beta(q, \varepsilon)$  ne dépendant que de  $q$  et de  $\varepsilon$ , telle que, pour tout entier  $t \geq 0$ , pour tout polynôme  $M$  de degré  $2n$  ou  $2n-1$  strictement positif, si  $aM$  n'est pas carré dans  $F_q[X]$ , quel que soit  $a \in F_q^*$ .*

(VI.30)

$$|\mathfrak{S}_3(M) - \sum_{\substack{H \in \mathcal{H} \\ d^0 H \leq t}} C_3(M, H)| \leq \beta(q, \varepsilon) \sqrt{n} \text{Sup}(1, \log d^0 M) |M|^\varepsilon \frac{4^n q^n q^{-t/2}}{(\sqrt{q-1})^{2n}}.$$

Démonstration. Posons

$$Z_t = \mathfrak{S}_3(M) - \sum_{\substack{H \in \mathcal{H} \\ d^0 H \leq t}} C_3(M, H).$$

Ici encore les sommes  $C_3(M, H)$  sont nulles sauf si  $H = QK$  avec  $Q$  sans facteur carré, premier à  $M$ , et  $K$  appartenant à l'ensemble  $\mathcal{X}_M$ , et dans ce cas, la proposition (VI.8) donne

$$C_3(M, H) = C_3(M, K) \prod_{\substack{P \in \mathcal{P} \\ P|Q}} |P|^{-1} \left( \frac{-M}{P} \right) = C_3(M, K) \chi(Q) |Q|^{-1},$$

d'où, avec (VI.26),

$$Z_t = H(1) \sum_{K \in \mathcal{X}_M} C_3(M, K) - \sum_{\substack{K \in \mathcal{X}_M \\ d^0 K \leq t}} C_3(M, K) \times \sum_{\substack{Q \in \mathcal{H} \\ (Q, M) = 1 \\ d^0(Q, K) \leq t}} \mu^2(Q) \chi(Q) |Q|^{-1},$$

et, avec (VI.22),

$$Z_t = Z'_t + Z''_t$$

où,

$$Z'_t = H(1) \sum_{\substack{K \in \mathcal{X}_M \\ d^0 K > t}} C_3(M, K) \quad \text{et} \quad Z''_t = \sum_{\substack{K \in \mathcal{X}_M \\ d^0 K \leq t}} C_3(M, K) \sum_{j=t-d^0 K \neq 1}^{\infty} h_j.$$

Avec (VI.24), (VI.25) et (VI.28) il vient

$$\begin{aligned} |H(1)| &\leq \frac{q-1}{q} \left( \frac{\sqrt{q+1}}{\sqrt{q}} \right)^{2n-2} \left( \prod_{\substack{P \in \mathcal{P} \\ P|M}} (1-|P|^{-1})^{-1} \right) \left( \prod_{P \in \mathcal{P}} (1-|P|^{-2})^{-1} \right), \\ |H(1)| &\leq \left( \frac{\sqrt{q+1}}{\sqrt{q}} \right)^{2n-2} |M|/\Phi(M), \end{aligned}$$

d'où, avec (VI.5),

$$|Z'_i| \leq \left( \frac{\sqrt{q}+1}{\sqrt{q}} \right)^{2n-2} |M| q^{-1/2} q^{-1/2} \times \text{Card}(\mathcal{X}_M) \Phi(M)^{-1}.$$

D'autre part, avec (VI.29) et (VI.5),

$$|Z''_i| \leq \sum_{\substack{K \in \mathcal{X}_M \\ d^0 K < i}} |K|^{-1/2} \sum_{j=i-d^0 K+1}^{\infty} q^{-j/2} n^{1/2} \pi^{-1/2} |M| \Phi(M)^{-1} 4^n q^n (\sqrt{q}-1)^{-2n},$$

$$|Z''_i| \leq n^{1/2} \pi^{-1/2} |M| \Phi(M)^{-1} 4^n q^n (\sqrt{q}-1)^{-2n} q^{-i/2} \text{Card}(\mathcal{X}_M) \sum_{j=0}^{\infty} q^{-j/2}.$$

Finalement on obtient la majoration

$$|Z_i| \leq |M| \Phi(M)^{-1} \text{Card}(\mathcal{X}_M) q^{-i/2} \left( \left( \frac{\sqrt{q}+1}{\sqrt{q}} \right)^{2n-2} + \left( \frac{n}{\pi} \right)^{1/2} \left( \frac{\sqrt{q}}{\sqrt{q}-1} \right) \times \right. \\ \left. \times \left( \frac{4q}{(\sqrt{q}-1)^2} \right)^n \right).$$

Les majorations (VI.13) et (VI.18) donnent alors le résultat annoncé avec  $\beta(q, \varepsilon) = a_4 \alpha(q, \varepsilon)$ .

## VII. Estimation de $\mathcal{S}_3(M)$ lorsque $-M$ est carré

Cette estimation nécessite l'évaluation de sommes relatives aux fonctions arithmétiques sur  $\mathcal{U}$ .

PROPOSITION VII.1. Soit, pour tout entier  $k \geq 0$ ,

$$(VII.1) \quad s_k = \sum_{\substack{Q \in \mathcal{U} \\ d^0 Q = k}} \frac{\mu^2(Q)}{|Q|}.$$

Alors,

$$(VII.2) \quad s_0 = s_1 = 1, \\ s_k = 1 - 1/q \quad \text{pour tout entier } k \geq 2.$$

Démonstration. De la majoration triviale  $|s_k| \leq 1$  on déduit que la série entière

$$\varphi(z) = \sum_{k=0}^{\infty} s_k z^k$$

est absolument convergente dans le disque  $|z| < 1$ . Dans ce disque  $\varphi(z)$  s'exprime comme produit absolument convergent

$$\varphi(z) = \prod_{P \in \mathcal{P}} (1 + (z/q)^{d^0 P}) = \prod_{P \in \mathcal{P}} (1 - (z^2/q^2)^{d^0 P}) (1 - (z/q)^{d^0 P})^{-1} = \frac{1 - (z^2/q)}{1 - z};$$

d'où (VII.2).

Pour énoncer la deuxième proposition, introduisons la fonction  $\Lambda$  de Von Mangolt définie sur  $\mathcal{U}$  par

$$\Lambda(A) = \begin{cases} d^0 P & \text{si } A \text{ est puissance du polynôme irréductible } P, \\ 0 & \text{sinon.} \end{cases}$$

**PROPOSITION VII.2** *Pour tout polynôme unitaire  $A$ ,*

$$(VII.3) \quad -\mu(A) d^0 A = \sum_{\substack{D \in \mathcal{U} \\ D|A}} \Lambda(D) \mu(A/D).$$

*Démonstration.* Comme pour le théorème 297 de [13].

**PROPOSITION VII.3.** *Pour tout polynôme unitaire  $A$  de degré strictement positif,*

$$(VII.4) \quad -\sum_{\substack{D \in \mathcal{U} \\ D|A}} \frac{\mu(D) d^0 D}{|D|} = |A|^{-1} \Phi(A) \sum_{\substack{P \in \mathcal{P} \\ P|A}} \frac{d^0 P}{|P| - 1}.$$

*Démonstration.* Posons

$$\Sigma_1(A) = -\sum_{\substack{D \in \mathcal{U} \\ D|A}} \frac{\mu(D) d^0 D}{|D|}.$$

Alors, avec (VII.3),

$$\begin{aligned} \Sigma_1(A) &= \sum_{\substack{D \in \mathcal{U} \\ D|A}} \frac{1}{|D|} \sum_{\substack{B \in \mathcal{U} \\ B|D}} \Lambda(B) \mu(D/B) = \sum_{\substack{B \in \mathcal{U} \\ B|A}} \Lambda(B) \sum_{\substack{D \in \mathcal{U} \\ D|A \\ B|D}} \mu(D/B) / |D| \\ &= \sum_{\substack{B \in \mathcal{U} \\ B|A}} \Lambda(B) |B|^{-1} \sum_{\substack{L \in \mathcal{U} \\ L|A/B}} \mu(L) / |L| = \sum_{\substack{B \in \mathcal{U} \\ B|A}} \frac{\Lambda(B) \Phi(A/B)}{|B| |A/B|} \\ &= (1/|A|) \sum_{\substack{B \in \mathcal{U} \\ B|A}} \Lambda(B) \Phi(A/B). \end{aligned}$$

Si  $P$  est un diviseur irréductible de  $A$ , si  $v$  est la valuation  $P$ -adique de  $A$ , pour tout entier  $k \leq v$ ,

$$\Phi(A/P^k) = \begin{cases} \Phi(A) |P|^{-k} & \text{si } k < v, \\ \Phi(A) |P|^{-v+1} (|P| - 1)^{-1} & \text{si } k = v; \end{cases}$$

donc,

$$\Sigma_1(A) = |A|^{-1} \Phi(A) \sum_{\substack{P \in \mathcal{P} \\ P|A}} d^0 P \left( \sum_{k=1}^{v_P(A)-1} |P|^{-k} + |P|^{-v_P(A)-1} (|P|-1)^{-1} \right),$$

d'où (VII.4).

PROPOSITION VII.4. Soit  $A$  un polynôme unitaire différent de 1. Alors,

$$(VII.5) \quad \sum_{\substack{P \in \mathcal{P} \\ P|A}} \frac{d^0 P}{|P|-1} \leq 1 + \frac{q}{q-1} \left( \frac{\log(1+d^0 A)}{\log q} \right)^2.$$

Démonstration. Posons

$$\Sigma_2(A) = \sum_{\substack{P \in \mathcal{P} \\ P|A}} \frac{d^0 P}{|P|-1} \quad \text{et} \quad r = \left\lceil \frac{\log(1+d^0 A)}{\log q} \right\rceil + 1.$$

Alors

$$\begin{aligned} \Sigma_2(A) &= \sum_{\substack{P \in \mathcal{P} \\ P|A \\ d^0 P < r}} \frac{d^0 P}{|P|-1} + \sum_{\substack{P \in \mathcal{P} \\ P|A \\ d^0 P \geq r}} \frac{d^0 P}{|P|-1} \\ &\leq (r-1) \sum_{\substack{P \in \mathcal{P} \\ d^0 P < r}} \frac{1}{|P|-1} + (q^r-1)^{-1} \sum_{\substack{P \in \mathcal{P} \\ P|A}} d^0 P. \end{aligned}$$

Pour tout entier  $j \geq 1$ , il y a au plus  $q^j/j$  polynômes irréductibles unitaires de degré  $j$ . C'est le lemme 20 de [17]. On en déduit la majoration

$$\Sigma_2(A) \leq (r-1) \sum_{j=1}^r \frac{q^j/j}{q^j-1} + (q^r-1)^{-1} d^0 A \leq \frac{q(r-1)^2}{q-1} + 1.$$

PROPOSITION VII.5. Soit  $A$  un polynôme unitaire de degré  $n > 0$ . Soit

$$(VII.6) \quad Y(A) = \sum_{\substack{Q \in \mathcal{U} \\ (Q,A)=1 \\ d^0 Q \leq d^0 A}} \frac{\mu^2(Q)}{|Q|}.$$

Alors,

$$(VII.7) \quad |A|^{-1} \Phi(A) (n(1-1/q) + 1) \leq Y(A) \leq |A|^{-1} \Phi(A) \left( n(1-1/q) + 2 + \left( \frac{\log(1+n)}{\log q} \right)^2 + q^{-n-1} \right).$$

Démonstration. La formule d'inversion de Möbius donne

$$Y(A) = \sum_{\substack{Q \in \mathcal{U} \\ d^0 Q \leq n}} \frac{\mu^2(Q)}{|Q|} \sum_{\substack{D \in \mathcal{U} \\ D|(Q,A)}} \mu(D) = \sum_{\substack{D \in \mathcal{U} \\ D|A}} \mu(D) |D|^{-1} \sum_{\substack{L \in \mathcal{U} \\ d^0 L \leq n-d^0 D}} \mu^2(L) |L|^{-1}.$$

D'après la proposition VII.1, pour tout diviseur  $D$  de  $A$ ,

$$\sum_{\substack{L \in \mathcal{U} \\ d^0 L \leq n - d^0 D}} \mu^2(L) |L|^{-1} = \begin{cases} 1 & \text{si } d^0 D = n, \\ 2 & \text{si } d^0 D = n - 1, \\ 2 + (n - d^0 D - 1)(1 - 1/q) & \text{si } d^0 D < n - 1, \end{cases}$$

d'où, en posant

$$y_n = n(1 - 1/q) + 1 + 1/q,$$

$$\sum_{\substack{L \in \mathcal{U} \\ d^0 L \leq n - d^0 D}} \mu^2(L) |L|^{-1} = \begin{cases} y_n - (1 - 1/q) d^0 D - 1/q & \text{si } D = A, \\ y_n - (1 - 1/q) d^0 D & \text{si } D \neq A. \end{cases}$$

On a donc

$$Y(A) = y_n \sum_{\substack{D \in \mathcal{U} \\ D|A}} \mu(D) |D|^{-1} - (1 - 1/q) \sum_{\substack{D \in \mathcal{U} \\ D|A}} \frac{\mu(D) d^0 D}{|D|} - \mu(A) q^{-1} |A|^{-1},$$

d'où, avec (VII.4),

$$Y(A) = |A|^{-1} \Phi(A) \left( y_n + (1 - 1/q) \sum_{\substack{P \in \mathcal{U} \\ P|A}} \frac{d^0 P}{|P| - 1} \right) - \mu(A) q^{-1} |A|^{-1}.$$

La minoration de  $Y(A)$  est immédiate; la majoration de  $Y(A)$  se déduit de la proposition précédente.

**PROPOSITION VII.6.** *Il existe des constantes strictement positives  $a_5 = a_5(q)$  et  $a_6 = a_6(q)$ , ne dépendant que de  $q$ , telles que, pour tout polynôme  $A$  de degré  $n \geq 2$*

$$(VII.8) \quad a_5 n (\log n)^{-1} \leq S_3(-A^2) \leq a_6 n.$$

**Démonstration.** Soit  $A$  un polynôme de degré  $n > 1$  et

$$A = a P_1^{u_1} \dots P_r^{u_r}$$

la factorisation de  $A$  en produit d'un élément de  $F_q$  et de polynômes irréductibles unitaires  $P_1, \dots, P_r$ , deux à deux distincts. Soit  $M = -A^2$ . L'étude faite au chapitre précédent montre que dans la somme

$$\mathcal{S}_3(M) = \sum_{\substack{H \in \mathcal{U} \\ d^0 H \leq n}} C_3(M, H)$$

n'interviennent que des polynômes  $H = QK$  où  $Q$  est sans facteur carré premier à  $M$ , où  $K \in \mathcal{K}_M$ , d'où,

$$\mathcal{S}_3(M) = \sum_{\substack{Q \in \mathcal{U} \\ d^0 Q \leq n \\ (Q, M) = 1}} \mu^2(Q) C_3(M, Q) \sum_{\substack{K \in \mathcal{K}_M \\ d^0(QK) \leq n}} C_3(M, K).$$

La proposition VI.8 montre plus précisément que

(i) si  $Q$  est sans facteur carré, premier à  $M$ ,

$$C_3(M, Q) = \prod_{\substack{P \in \mathcal{P} \\ P|Q}} |P|^{-1} \left( \frac{-M}{P} \right) = |Q|^{-1};$$

(ii) les seuls polynômes  $K \in \mathcal{X}_M$  pour lesquels  $\dot{C}_3(M, K)$  n'est pas nul sont les polynômes

$$K = P_1^{k_1} \dots P_r^{k_r},$$

où, pour  $i \in \{1, \dots, r\}$ ,  $k_i \in \{0, 2, \dots, 2u_i, 2u_i + 1\}$ ;

(iii) si  $i \in \{1, \dots, r\}$ ,

$$C_3(M, P_i^{2u_i+1}) = |P_i|^{-u_i-1} \left( \frac{-MP_i^{-2u_i}}{P_i} \right) = |P_i|^{-u_i-1},$$

et, si  $k_i \in \{0, \dots, u_i\}$ ,

$$C_3(M, P_i^{2k_i}) = (|P_i| - 1) |P_i|^{-k_i-1}.$$

Les sommes  $C_3(M, Q)C_3(M, K)$  intervenant dans  $\mathcal{S}_3(M)$  sont positives, d'où,

$$\sum_{\substack{Q \in \mathcal{Q} \\ (Q, M) = 1 \\ d^0 Q \leq n}} \mu^2(Q)/|Q| \leq \mathcal{S}_3(M) \leq T(M) \sum_{\substack{Q \in \mathcal{Q} \\ (Q, M) = 1 \\ d^0 Q \leq n}} \mu^2(Q)/|Q|,$$

où

$$T(M) = \sum_{K \in \mathcal{X}_M} C_3(M, K).$$

Avec (VII.6) il vient

$$Y(A) \leq \mathcal{S}_3(M) \leq Y(A) T(M).$$

On a

$$T(M) = \prod_{i=1}^r \left( 1 + \sum_{j=1}^{u_i} (|P_i| - 1) |P_i|^{-j-1} + |P_i|^{-u_i-1} \right) = \prod_{i=1}^r (1 + |P_i|^{-1}) \leq |A|/\Phi(A).$$

Les propositions VII.5 et VI.11 donnent alors

$$\begin{aligned} (a_4 \log(n))^{-1} (n(1-1/q) + 1) &\leq \mathcal{S}_3(M) \\ &\leq n(1-1/q) + 2 + \left( \frac{\log(1+n)}{\log q} \right)^2 + a_4 q^{-n-1} \log(n); \end{aligned}$$

d'où le résultat annoncé.

La formulation choisie pour énoncer la proposition VII.6 nous oblige à traiter à part les sommes  $\mathcal{S}_3(-A^2)$  lorsque le polynôme  $A$  est de degré 0 ou



1. On ne s'occupe pas du degré 0, l'étude faite au paragraphe V donnant le nombre de représentations d'un polynôme de degré 0 en somme de trois carrés. En reprenant la démonstration précédente on voit facilement que si  $A$  est de degré 1,

$$\mathcal{S}_3(-A^2) = 2 - 1/q,$$

d'où, la

**PROPOSITION VII.7.** *Il existe des constantes strictement positives  $a_7 = a_7(q)$  et  $a_8 = a_8(q)$ , ne dépendant que de  $q$ , telles que, pour tout polynôme  $A$  de degré strictement positif,*

$$(VII.9) \quad a_7 n \text{ Inf}(1, (\log n)^{-1}) \leq \mathcal{S}_3(-A^2) \leq a_8 n.$$

### VIII. Estimation des nombres $R_k(M)$ . (Fin)

Rappelons que pour tout polynôme  $M$  de degré  $2n$  ou  $2n-1$ ,  $R_k(M)$  désigne le nombre de solutions de l'équation

$$M = M_1^2 + \dots + M_k^2$$

en polynômes  $M_1, \dots, M_k$  de degré au plus égal à  $n$ .

Ces nombres s'expriment en fonction de nombres  $A_k(M)$  calculables à partir des résultats établis au paragraphe V. Donnons sur un tableau les différentes valeurs des nombres  $A_k(M)$  suivant que  $M$  est de degré pair ou impair, que  $k$  est pair ou impair, que  $-1$  est ou n'est pas carré dans  $F_q$ , que  $\text{sgn}(M)$  est ou n'est pas carré dans  $F_q$ .

$d^0 M$ impair				
$k = 2j$	-1 carré		-1 non carré	
		$q^{2j-1} - q^{-j-1} + q^j - 1$		$q^{2j-1} - (-1)^j q^{j-1} + (-1)^j q^j - 1$
$k = 2j+1$	$q^{2j} - 1$			
$d^0 M$ pair				
$k = 2j$	-1 carré		-1 non carré	
	$q^{2j-1} - q^{j-1}$		$q^{2j-1} - (-1)^j q^j$	
$k = 2j+1$	sgn(M) carré	sgn(M) non carré	sgn(M) carré	sgn(M) non carré
	$q^{2j} + q^j$	$q^{2j} - q^j$	$q^{2j} + (-1)^j q^j$	$q^{2j} - (-1)^j q^j$

En particulier,

$$A_4(M) = \begin{cases} q(q^2-1) & \text{si } d^0 M \text{ est pair,} \\ (q+1)(q^2-1) & \text{si } d^0 M \text{ est impair,} \end{cases}$$

$$A_3(M) = \begin{cases} q^2-1 & \text{si } d^0 M \text{ est impair,} \\ q^2+q & \text{si } d^0 M \text{ est pair et si } -\text{sgn}(M) \\ & \text{est carré dans } F_q, \\ q^2-q & \text{si } d^0 M \text{ est pair et si } -\text{sgn}(M) \\ & \text{n'est pas carré dans } F_q. \end{cases}$$

Nous pouvons énoncer les théorèmes principaux.

**THÉOREME I.** *Il existe des constantes strictement positives  $C_1$  et  $C_2$ , ne dépendant que de  $q$ , telles que, pour tout entier  $k \geq 5$ , pour tout polynôme  $M$  de degré  $2n$  ou  $2n-1$ ,*

$$R_k(M) = q^{n(k-2)} A_k(M) \mathfrak{S}_k(M) \bmod \mathcal{O}(q^{kn/2}),$$

et

$$C_1 \leq \mathfrak{S}_k(M) \leq C_2,$$

la constante contenue dans le  $\mathcal{O}$  ne dépendant que de  $q$  et de  $k$ .

*Démonstration.* Avec les relations (IV.10), (IV.11), (VI.6) et (VI.8).

**THÉOREME II.** *Pour tout réel  $\varepsilon > 0$ , pour tout polynôme  $M$  de degré  $2n$  ou  $2n-1$ , strictement positif,*

$$R_4(M) = q^{2n} A_4(M) \mathfrak{S}_4(M) \bmod \mathcal{O}(q^{n+n\varepsilon}),$$

avec

$$\mathfrak{S}_4(M) = \frac{q-1}{q} \sum_{\substack{D \in \mathfrak{N} \\ D|M}} |D|^{-1},$$

et

$$\frac{q-1}{q} \leq \mathfrak{S}_4(M) \leq \frac{q-1}{q} |M| \Phi(M)^{-1},$$

la constante impliquée par le  $\mathcal{O}$  ne dépendant que de  $q$  et de  $\varepsilon$ .

*Démonstration.* Avec les relations (IV.10), (IV.11), (VI.16), (VI.17) et la proposition VI.12.

On remarque que la formule donnant  $\mathfrak{S}_4(M)$  présente des analogies avec la formule donnant le nombre  $\varrho_4(n)$  de représentations d'un entier naturel  $n$  comme somme de 4 carrés. (Voir [2] par exemple.)

**THÉOREME III.** *Pour tout réel  $\varepsilon > 0$ , si  $M$  est un polynôme de degré  $2n$  ou*

$2n-1$  strictement positif, tel que  $aM$  ne soit pas carré dans  $F_q[X]$  quel que soit  $a \in F_q^*$ .

$$R_3(M) = q^n A_3(M) \mathfrak{S}_3(M) \bmod \mathcal{O}(\sqrt{n} \log(n) (4q^{3/2} q^\varepsilon / (\sqrt{q}-1)^2)^n),$$

avec

$$\frac{q-1}{q} \left( \frac{\sqrt{q}-1}{\sqrt{q}} \right)^{2n-2} \Phi(M)/|M|^{-1} \leq \mathfrak{S}_3(M) \leq \left( \frac{\sqrt{q}+1}{\sqrt{q}} \right)^{2n-2} (|M|/\Phi(M))^2,$$

la constante contenue dans le  $\mathcal{O}$  ne dépendant que de  $q$  et de  $\varepsilon$ .

Démonstration. Avec les relations (IV.10), (IV.11), (VI.27) et la proposition VI.18.

Remarquons que le théorème III ne donne une "bonne" évaluation asymptotique de  $R_3(M)$  que pour des corps  $F_q$  tels que  $4q\sqrt{q} < (\sqrt{q}-1)^4$ , c'est à dire pour  $q \geq 53$ .

THÉORÈME III'. Il existe des constantes strictement positives  $C_3$  et  $C_4$  ne dépendant que de  $q$ , telles que, pour tout polynôme  $A$  de degré  $n > 0$ ,

$$C_3 nq^n \text{Inf}(1, (\log n)^{-1}) \leq R_3(-A^2) \leq C_4 nq^n.$$

Démonstration. Avec les relations (IV.10) et (VII.9).

Les théorèmes I et II assurent l'existence de représentations restreintes en sommes de  $k$  carrés,  $k$  étant un entier au moins égal à 4, pour tout polynôme de degré assez élevé. De même, si  $q \geq 53$ , le théorème III assure l'existence d'une représentation restreinte en sommes de 3 carrés, pour tout polynôme  $M$  de degré assez élevé, et tel qu'en plus,  $aM$  ne soit pas carré dans  $F_q[X]$  quel que soit  $a \in F_q^*$ . Enfin le théorème III' montre que pour tout polynôme  $A$  de  $F_q[X]$  de degré strictement positif,  $-A^2$  admet une représentation restreinte en somme de 3 carrés, résultat qui peut être obtenu immédiatement de façon élémentaire.

Le théorème III' mis à part, ces théorèmes ne donnent pas l'existence de représentations restreintes en sommes de  $k$  carrés ( $k \geq 3$ ) pour des polynômes de degré quelconque.

## Bibliographie

- [1] R. Ayoub, *An introduction to the analytic theory of numbers*, Math. Surveys 10, Amer. Math. Soc., 1963.
  - [2] P. Bateman, *On the representation of a number as the sum of three squares*, Trans. Amer. Math. Soc. 71 (1951), p. 70–101.
  - [3] M. Car, *Le problème de Waring pour l'anneau des polynômes sur un corps fini*, C. R. Acad. Sci. Paris 273 (19 juillet 1971), p. 141–144.
  - [4] — *Normes dans  $F_q[X]$  de polynômes de  $F_q h[X]$* , *ibid.* 288 (9 avril 1979), p. 669–672.
  - [5] L. Carlitz, *On the representations of the polynomial on a Galois field as the sum of an even number of squares*, Trans. Amer. Math. Soc. 35 (1933), p. 397–410.
  - [6] — *On the representation of a polynomial on a Galois field as the sum of an odd number of squares*, Duke Math. J. 1 (1935), p. 298–315.
  - [7] — *Sums of squares of polynomials*, *ibid.* 3 (1937), p. 1–7.
  - [8] — *The singular series for sums of squares of polynomials*, *ibid.* 14 (1947), p. 1105–1120.
  - [9] — *A note on sums of three squares in  $GF[q, x]$* , Mathematics Magazine 48 (1975), p. 109–110.
  - [10] Eckford, Cohen, *Sums of an even number of squares in  $GF[p^n, x]$ , I*, Duke Math. J. 14 (1947), p. 251–267.
  - [11] — — *Sums of an even number of squares in  $GF[p^n, x]$ , II*, *ibid.* 14 (1947), p. 543–557.
  - [12] — — *Sums of an odd number of squares in  $GF[p^n, x]$* , *ibid.* 15 (1948), p. 501–511.
  - [13] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, Clarendon Press, Oxford 1962.
  - [14] D. R. Hayes, *The expression of a polynomial as the sum of three irreducibles*, Acta Arith. 11 (1966), p. 461–488.
  - [15] R. M. Kubota, *Waring's problem for  $F_q[x]$* , Diss. Math. 117 (1974).
  - [16] K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin 1957.
  - [17] G. Rhin, *Répartition modulo 1 dans un corps de séries formelles sur un corps fini*, Diss. Math. 95 (1972).
  - [18] J. P. Serre, *Corps locaux*, Hermann, Paris 1962.
  - [19] W. A. Webb, *Waring's problem in  $GF[q, x]$* , Acta Arith. 22 (1973), p. 207–220.
  - [20] A. Weil, *Basic number theory*, Springer-Verlag, Berlin.
-