ACTA ARITHMETICA
XCVII.3 (2001)

Sur les fractions continues des séries formelles quadratiques sur $\mathbb{F}_q(X)$

par

Mohamed Mkaouar (Sfax)

Introduction. Soient p un nombre premier et $\mathbb{F}_q$ le corps à q éléments et de caractéristique p. L'ensemble $\mathbb{F}_q((X^{-1}))$ représente le corps des séries formelles à coefficients dans $\mathbb{F}_q$. Un élément $f \in \mathbb{F}_q((X^{-1}))$ est donc de la forme

$$f = \sum_{j=s}^{+\infty} f_j X^{-j}$$

où $s \in \mathbb{Z}$. On note par $[f]$ la partie polynomiale de f, $\deg f = s$ et $\sigma(f) = f_s$. Il est clair que si P est un polynôme de degré n dans $\mathbb{F}_q[X]$ tel que $P = a_n X^n + \ldots + a_0$, alors $\sigma(P) = a_n$. Si f est une série formelle vérifiant l'équation

$$A_m f^m + \ldots + A_1 f + A_0 = 0 \tag{E}$$

où les A_k sont des polynômes de $\mathbb{F}_q[X]$ non tous nuls, on dit que f est *algébrique* sur $\mathbb{F}_q(X)$. Si de plus l'équation (E) vérifie $\deg A_k < \deg A_{m-1}$ pour tout $k \in \{0, \ldots, m\} \setminus \{m-1\}$ et f est de degré m, on dit que f est une *série formelle algébrique de type* (I). Soit $f \in \mathbb{F}_q((X^{-1}))$; alors $f = f_0 = [f] + (f - [f])$. Soient $a_0 = [f_0]$ et $f_1 = (f - [f])^{-1}$, on définit par la suite $f_n = a_n + f_{n+1}^{-1}$ et $a_n = [f_n]$. Finalement, il est clair qu'on peut écrire f sous la forme

$$f = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}} = [a_0; a_1, a_2, \ldots].$$

Cette nouvelle écriture de f est appelé *développement en fraction continue* de f, et la suite de polynômes $(a_n)_{n \geq 0}$ est appelé *suite de quotients partiels* de f. Il est clair que $\deg a_i \geq 1$ pour tout entier strictement positif.

2000 *Mathematics Subject Classification*: 11A55, 30B70.

Soit f une série formelle quadratique $\in \mathbb{F}_q((X^{-1}))$. Alors la suite de quotients partiels de son développement en fraction continue est ultimement périodique (i.e. $f = [b_0; b_1, \ldots, b_s, \overline{a_1, \ldots, a_t}]$). Nous poserons $T(f) = \max_{1 \le i \le t} \deg a_i$ et $\mathrm{Per}(f) = t$ sa période. On dit aussi qu'une série formelle quadratique f est *purement périodique* si sa suite de quotients partiels est périodique (i.e. $f = [a_1; \overline{a_2, \ldots, a_t, a_1}]$) ; si de plus $f = [a_1; \overline{a_2, \ldots, a_t, a_1}]$) $= [a_t; \overline{a_{t-1}, \ldots, a_1, a_t}]$), on dit que f est *palindromique*.

Dans le cas réel Schinzel [8] a montré l'existence de la quantité

$$S(N, n) = \sup_{\mathrm{Per}(x)=n} \mathrm{Per}(Nx),$$

où x est un nombre réel quadratique. Un peu plus tard Cohen [4] a redémontré l'existence de $S(N, n)$; de plus, il a évalué la quantité $S(N, n)$, il a prouvé l'existence de

$$R(N) = \sup_{n \ge 1} \left(\frac{S(N, n)}{n} \right) = \sup_{x \in \mathbb{Q}} \left(\frac{\mathrm{Per}(Nx)}{\mathrm{Per}(x)} \right),$$

et il a donné la valeur exacte de $R(N)$ pour une infinité d'entiers N. D'autre part Cohn a étudié dans [5] la longueur de la période du développement en fraction continue de $d^{1/2}$, où d est un entier qui n'est pas un carré parfait ; il a montré que

$$\mathrm{Per}(\sqrt{d}) < \frac{7}{2\pi^2} \sqrt{d} \log d + O(\sqrt{d}).$$

Dans [6] Lewittes a caractérisé les nombres réels quadratiques qui sont palindromiques et il a évalué le nombre $A(n)$ des réels qui sont palindromiques et dont le discriminant est égal à n.

Dans le cas des séries formelles, il est démontré dans [7] que si f est une série formelle quadratique sur $\mathbb{F}_2(X)$ vérifiant $Af^2 + Bf + C = 0$, alors $\mathrm{Per}(f) \le (2^{\deg B} - 1)^2$.

L'objectif de ce travail est de donner dans le cas des séries formelles l'équivalent du théorème de Galois pour le cas quadratique : à savoir la caractérisation des séries formelles quadratiques qui admettent un développement en fraction continue purement periodique. D'autre part, on généralise le résultat établi par Mkaouar [7] sur $\mathbb{F}_2((X^{-1}))$, dans $\mathbb{F}_q((X^{-1}))$, où la caractéristique p du corps > 2 est de donner un majorant à la période d'une série formelle quadratique de type (I) en fonction des coefficients de son polynôme minimal. De plus, si $p \ge 3$, on donne une condition nécessaire et suffisante pour qu'un polynôme $Q \in \mathbb{F}_q[X]$ admet une racine carré dans $\mathbb{F}_q((X^{-1}))$ et que la période du développement en fraction continue de celle-ci est un $O(q^{2 \deg Q})$. Finalement, on donne une caractérisation des séries formelles quadratiques palindromiques.

Enoncé des résultats

THÉORÈME 1. *Soit f une série formelle quadratique sur $\mathbb{F}_q(X)$ et $[f] \neq 0$. Alors f admet un développement en fraction continue purement périodique si et seulement si f est de type* (I).

THÉORÈME 2. *Soit f une série formelle quadratique sur $\mathbb{F}_q(X)$ de type* (I), *vérifiant $Af^2 + Bf + C = 0$. Alors*

$$\mathrm{Per}(f) \leq (q^{\deg B} - 1)^2 q^{2 \deg B} \quad \textit{et} \quad T(f) \leq \deg B.$$

THÉORÈME 3. *Soit f une série formelle algébrique de type* (I) *et de degré m sur $\mathbb{F}_q(X)$, telle que $[f] \neq 0$ et $A_m f^m + \ldots + A_1 f + A_0 = 0$. Alors $[f] = -[A_{m-1}/A_m]$ et la série formelle $h = 1/(f - [f])$ est une série formelle de type* (I).

THÉORÈME 4. *Soient $q \geq 3$ et Q un polynôme de degré pair avec $\sigma(Q)$ un carré parfait. Alors Q admet au moins une racine carrée $f \in \mathbb{F}_q((X^{-1}))$; de plus si Q n'est pas un carré parfait dans $\mathbb{F}_q[X]$, alors toute racine carrée f de Q vérifie*

$$\mathrm{Per}(f) \leq q^{2 \deg Q} \quad \textit{et} \quad T(f) \leq \tfrac{1}{2} \deg Q.$$

THÉORÈME 5. *Soit f une série formelle quadratique sur $\mathbb{F}_q(X)$. Alors f est palindromique si et seulement si elle vérifie une équation de type $Af^2 + Bf - A = 0$ avec $A, B \in \mathbb{F}_q[X]$ et $\deg B > \deg A$. De plus si $A(n,q)$ désigne le nombre de séries formelles palindromiques dont le discriminant est de degré $2n$, alors*

$$A(n,q) = O\left(\frac{q^{2n}}{n^{\alpha}\sqrt{\log 2n}}\right) \quad \textit{avec } \alpha = 1 - \frac{1 + \log\log 2}{\log 2} \quad \textit{si } p \equiv 1 \pmod 4$$

et

$$A(n,q) = O\left(\frac{q^{2n}}{\sqrt{n}}\right) \quad \textit{si } p \equiv 3 \pmod 4.$$

Démonstration du théorème 3. Posons $g = f - [f]$. Alors

$$\begin{aligned} 0 &= \sum_{j=0}^{m} A_j([f] + g)^j \\ &= \sum_{j=0}^{m} A_j \sum_{k=0}^{j} \binom{j}{k} [f]^{j-k} g^k = \sum_{k=0}^{m} \left(\sum_{j=k}^{m} A_j \binom{j}{k} [f]^{j-k} \right) g^k. \end{aligned}$$

Soit

$$C_k = \sum_{j=k}^{m} A_j \binom{j}{k} [f]^{j-k}. \tag{1}$$

Comme $\deg f > 0$ alors $\deg A_k f^k < \deg A_{m-1} f^{m-1}$ pour $k < m-1$, et par suite d'après (E), $\deg A_m f^m = \deg A_{m-1} f^{m-1}$. Ceci donne $\deg f =$

$\deg A_{m-1} - \deg A_m$ et

$$f = -A_{m-1}/A_m - \sum_{j=1}^{m-1} l_j$$

avec $l_j = A_{m-j-1}/A_m f^j$. D'où

$$\deg l_j = \deg A_{m-j-1} + (j-1)\deg A_m - j \deg A_{m-1} < 0,$$

ce qui donne que $[f] = -[A_{m-1}/A_m]$.

Soit $h = 1/(f - [f])$, alors la série formelle h vérifie l'équation

$$\sum_{k=0}^{m} C_{m-k} h^k = 0.$$

Comme f est algébrique et degré m, alors h l'est aussi. Donc pour montrer que h est de type (I), il suffit de montrer que $\deg C_1 > \deg C_k$ pour tout $k \in \{0, \ldots, m\} \setminus \{1\}$. Comme $[f] = -[A_{m-1}/A_m]$, alors $A_{m-1} = -[f]A_m + R$ avec $\deg R < \deg A_m$. D'après (1),

$$C_0 = \sum_{j=0}^{m} A_j [f]^j = \Big(\sum_{j=0}^{m-2} A_j [f]^j \Big) + R[f]^{m-1}$$

et

$$C_1 = \sum_{j=0}^{m} j A_j [f]^{j-1} = \Big(\sum_{j=0}^{m-2} j A_j [f]^{j-1} \Big) + A_m [f]^{m-1} + (m-1) R [f]^{m-2}.$$

Il est clair que $\deg C_1 = (m-2)\deg[f] + \deg A_{m-1}$ et que $\deg C_0 \leq (m-2)\deg[f] + \deg A_{m-1}$. Comme $\deg C_k \leq \deg A_{m-1} + (m-k-1)\deg[f]$ pour tout $k \in \{1, \ldots, m\}$, alors, pour tout $k \in \{1, \ldots, m\} \setminus \{1\}$, on a $\deg C_k < \deg C_1$.

Application

COROLLAIRE 1. *Soient $n \in \mathbb{N}^*$ et f une série formelle algébrique sur $\mathbb{F}_q(X)$ vérifiant $[f] \neq 0$ et $Af^{q^n+1} + ABf^{q^n} + 1 = 0$, avec $\deg B > 0$. Alors $f = [a_0; a_1, \ldots]$, où*

$$a_s = (-1)^s A^{(q^{sn} - (-1)^s)/(q^s+1)} B^{q^{sn}}.$$

Preuve. Soit $f_0 = f$, $a_0 = [f_0]$, $P_0 = A$, $Q_0 = AB$, $R_0 = 0$, $S_0 = 1$ et $f_{s+1} = 1/(f_s - [f_s])$. Alors d'après le théorème 3, f_s est de type (I) et vérifie l'équation $P_s f_s^{q^n+1} + Q_s f_s^{q^n} + R_s f_s + S_s = 0$, avec

$$P_{s+1} = P_s a_s^{q^n+1} + Q_s a_s^{q^n} + R_s a_s + S_s, \quad Q_{s+1} = P_s a_s^{q^n},$$

$$R_{s+1} = Q_s + a_s P_s, \quad S_{s+1} = P_s, \quad a_{s+1} = -\left[\frac{Q_{s+1}}{P_{s+1}}\right].$$

A l'aide d'une récurrence simple sur s on montre que

$$P_s = A^{(1+(-1)^s)/2}, \quad Q_s = (-1)^s A^{(1-(-1)^s)/2} A^{(q^{sn}+(-1)^s q^n)/(q^n+1)} B^{q^{sn}},$$
$$R_s = 0, \quad S_s = A^{(1-(-1)^s)/2}$$

et que

$$a_s = (-1)^s A^{(q^{sn}+(-1)^s)/(q^n+1)} B^{q^{sn}}.$$

COROLLAIRE 2 ([1], théorème 6). *Soit $n \in \mathbb{N}$. Alors l'équation*

$$f^{2^n+1} + Qf^{2^n} + Pf + PQ + 1 = 0$$

admet une racine unique dans $\mathbb{F}_2((X^{-1}))$, et

$$f = [Q; Q^{2^{2n}} + P^{2^n}, Q^{2^{3n}} + P^{2^{2n}}, \ldots].$$

Preuve. Il suffit de remarquer que la série formelle $g = 1/(f - Q)$ vérifie

$$g^{2^n+1} + (Q^{2^n} + P)g^{2^n} + 1 = 0$$

d'après le corollaire 1 : il suffit de prendre $A = 1, B = Q^{2^n} + P$ et $q = 2$.

Démonstration du théorème 1. Ici, on donne l'équivalent du théorème de Galois pour le cas quadratique sur $\mathbb{F}_q((X^{-1}))$. Il est clair que si f est périodique alors f vérifie l'équation $Q_n f^2 + (Q_{n-1} - P_n)f - P_{n-1} = 0$, où $f = [a_1; \overline{a_2, \ldots, a_t, a_1}]$ et $P_n/Q_n = [a_1; a_2, \ldots, a_n]$. On a alors $\deg Q_n < \deg(P_n - Q_{n-1}) = \deg P_n$ et $\deg P_{n-1} < \deg P_n$.

On suppose maintenant que f est de type (I) et vérifie $Af^2 + Bf + C = 0$. Alors f est ultimement périodique, donc f est de la forme $f = [a_1; a_2, \ldots, a_t, f_{t+1}]$, où f_{t+1} est une série formelle périodique. Soit $f = f_1$ et $f_{n+1} = 1/(f_n - a_n)$. Comme f est de type (I), alors d'après le théorème 3, f_n l'est aussi et vérifie l'équation $H_n f_n^2 + K_n f_n + H_{n-1} = 0$, avec $H_0 = C$, $H_1 = A$, $K_1 = B$, $a_1 = -[K_1/H_1]$, et

$$H_{n+1} = a_n^2 H_n + a_n K_n + H_{n-1}, \tag{2}$$

$$K_{n+1} = 2a_n H_n + K_n, \tag{3}$$

$$a_{n+1} = -[K_{n+1}/H_{n+1}]. \tag{4}$$

Soit $\mathrm{Per}(f) = \mathrm{Per}(f_{t+1}) = l$. Alors $H_{t+j} = H_{t+l+j}$, $K_{t+j} = K_{t+l+j}$ et $a_{t+j} = a_{t+j+l}$, pour tout $j \geq 1$. Ceci donne d'après la formule de récurrence (2) pour H_{t+l+2} et H_{t+2} que

$$H_t = H_{t+l}. \tag{5}$$

Par suite,

$$K_{t+l+1} = 2a_{t+l}H_{t+l} + K_{t+l} = 2a_{t+l}H_t + K_{t+l} = K_{t+1} = 2a_t H_t + K_t,$$

ce qui donne

$$2(a_{t+l}-a_t)H_t = K_t - K_{t+l}. \tag{6}$$

Soit alors

$$K_t = [K_t/H_t]H_t + R_t = -a_tH_t + R_t, \tag{7}$$

avec $\deg R_t < \deg H_t$, et

$$K_{t+l} = [K_{t+l}/H_{t+l}]H_{t+l} + R_{t+l} = -a_{t+l}H_{t+l} + R_{t+l}, \tag{8}$$

avec $\deg R_{t+l} < \deg H_t$. En remplaçant K_{t+l} et K_t par leurs expressions dans (6), on obtient

$$(a_{t+l}-a_t)H_t = R_t - R_{t+l}. \tag{9}$$

Comme $\deg(R_t - R_{t+l}) < \deg H_t$, (9) nous permet de dire que $a_t = a_{t+l}$ et $R_t = R_{t+l}$, ce qui donne d'après (5), (7) et (8), $K_t = K_{t+l}$ et par suite d'après les formules de récurrence (2), (3) et (4), $H_{t-1} = H_{t-1+l}, \dots, H_1 = H_{1+l}$, $K_{t-1} = K_{t-1+l}, \dots, K_1 = K_{1+l}$ et $a_{t-1} = a_{t-1+l}, \dots, a_1 = a_{1+l}$, ce qui montre que f est périodique.

Démonstration du théorème 2. Pour la démonstration de ce théorème, on a besoin du lemme suivant :

LEMME 1. *Soit f une série formelle de type* (I) *vérifiant* (E) : $Af^2 + Bf + C = 0$. *Alors f et $-(f + B/A)$ sont les seules solutions de* (E). *De plus si $f = [a_1; \overline{a_2, \dots, a_n, a_1}]$, alors $-(f + B/A) = [0; \overline{-a_n, -a_{n-1}, \dots, -a_1}]$.*

Preuve. Il est facile de vérifier que si f est solution de (E), alors $-(f + B/A)$ l'est aussi, donc on peut supposer sans perte de généralité que $[f] \neq 0$. Dans ce cas d'après le théorème 3, $[f] = -[B/A] = a_1$. Soit $P_n/Q_n = [a_1; a_2, \dots, a_n]$. Il est clair que

$$f = [a_1; a_2, \dots, a_n, f] = \frac{P_nf + P_{n-1}}{Q_nf + Q_{n-1}},$$

ce qui donne $Q_nf^2 + (Q_{n-1} - P_n)f - P_{n-1} = 0$. On a $P_{n-1}/P_n = [0; a_n, a_{n-1}, \dots, a_1]$ et $Q_{n-1}/Q_n = [0; a_n, \dots, a_2]$. Posons $h = [0; \overline{-a_n, \dots, -a_1}]$; alors $h = [0; -a_n, \dots, -a_1 + h]$, ce qui donne $-h = (P_{n-1} - Q_{n-1}h)/(P_n - Q_nh)$ et par suite h vérifie l'équation $Q_nh^2 + (Q_{n-1} - P_n)h - P_{n-1} = 0$. Comme f vérifie la même équation que h, elles sont conjuguées et par conséquent $h = -(f + B/A)$.

Suite de la démonstration du théorème 2. Soit $f \in \mathbb{F}_q((X^{-1}))$ de type (I) vérifiant $Af^2 + Bf + C = 0$. On peut supposer que $[f] \neq 0$. Soit $f = [a_1; \overline{a_2, \dots, a_l, a_1}]$, $f = f_1$ et $f_{n+1} = 1/(f_n - a_n)$. Alors d'après le théorème 3, pour tout $n \in \mathbb{N}^*$, la série f_n est de type (I) et elle vérifie l'équation

$$H_nf_n^2 + K_nf_n + H_{n-1} = 0$$

où les suites de polynômes H_n et K_n sont définies par les relations de récurrences données par (2), (3) et (4). La division euclidienne de K_n par H_n donne $K_n = -a_n H_n + R_n$ avec $\deg R_n < \deg H_n$. Or (3) nous permet de dire que $K_{n+1} = -K_n + 2R_n$, ce qui donne que pour tout entier positif n,

$$\deg K_n = \deg B. \tag{10}$$

Comme f est de type (I), alors d'après le théorème 1, f est purement périodique, donc d'après (10), la suite $W_n = (H_n, K_n)$ l'est aussi et partage la même période l que f. Soit $t \in \mathbb{N}$; alors $W_{t+l} = W_t$ et $W_{t+l+1} = W_{t+1}$. Soit donc $s \in \mathbb{N}^*$ le plus petit entier tel que $W_{t+s} = W_t$ et $W_{t+s+1} = W_{t+1}$. Les formules de récurrences qui relient H_{n+1} et K_{n+1} à H_n, K_n, a_n montrent que $H_{t+s+2} = H_{t+2}$, $H_{t+s+3} = H_{t+3}, \ldots, H_{t+2s} = H_{t+s}$, $K_{t+s+2} = K_{t+2}$, $K_{t+s+3} = K_{t+3}, \ldots$, et que $K_{t+2s} = K_{t+s}$. Ceci montre que s est la période de la suite $W_n = (H_n, K_n)$ et par suite $s = l$. Comme $H_n \neq 0$ et d'après (10), $\deg H_n < \deg K_n = \deg B$, le nombre de termes distincts de la suite W_n est majoré par $(q^{\deg B} - 1)q^{\deg B}$. Alors le nombre de couples (W_n, W_{n+1}) distincts est majoré par $(q^{\deg B} - 1)^2 q^{2\deg B}$. Donc dans les $(q^{\deg B} - 1)^2 q^{2\deg B} + 1$ premiers termes de la suite (W_n, W_{n+1}), on trouve deux couples identiques $(W_t, W_{t+1}) = (W_{t+s}, W_{t+s+1})$, ce qui donne $l = s \leq (q^{\deg B} - 1)^2 q^{2\deg B}$. D'autre part, pour tout entier strictement positif n on a $\deg a_n = \deg K_n - \deg H_n$, et d'après (10), on déduit que $T(f) \leq \deg B$.

Démonstration du théorème 4. Pour la démonstration de ce théorème, on a besoin de quelques lemmes.

Lemme 2. *Soit $q \geq 2$. Alors l'équation* (E) : $AY^2 + BY + C = 0$ *avec* $A, B, C \in \mathbb{F}_q[X] \setminus \{0\}$ *et* $\deg B > \deg A, \deg C$ *admet au moins une racine f dans $\mathbb{F}_q((X^{-1}))$ telle que* $\deg[f] \geq 1$.

Preuve. Soient H_n, K_n et a_n les suites de polynômes définies par $H_0 = C$, $H_1 = A$, $K_1 = B$ et $a_1 = -[K_1/H_1]$, $H_{n+1} = a_n^2 H_n + a_n K_n + H_{n-1}$, $K_{n+1} = 2a_n H_n + K_n$ et $a_{n+1} = -[K_{n+1}/H_{n+1}]$. Il est clair que les termes H_{n+1}, K_{n+1} et a_{n+1} ne sont définis que si $H_n \neq 0$. Pour cela, on suppose que $H_n \neq 0$ pour $n \leq m$. Soient $P_0 = 1, Q_0 = 0$, $P_n/Q_n = [a_1, \ldots, a_n]$ et

$$U_n = AP_n^2 + BP_nQ_n + CQ_n^2,$$
$$V_n = 2P_nP_{n-1}A + (P_nQ_{n-1} + Q_nP_{n-1})B + 2Q_nQ_{n-1}C.$$

Montrons que pour tout $n \in \{1, \ldots, m\}$,

$$U_n = H_{n+1}, \tag{α_n}$$
$$V_n = K_{n+1}. \tag{β_n}$$

Les propriétés (α_n) et (β_n) sont vraies pour $n = 1$. On les suppose vraies pour $n < s \leq m$. Alors en utilisant le fait que pour tout $s \in \mathbb{N}$, $P_s =$

$a_sP_{s-1}+P_{s-2}$ et $Q_s=a_sQ_{s-1}+Q_{s-2}$, on aura

$$\begin{aligned}U_s &= A(a_sP_{s-1}+P_{s-2})^2+B(a_sP_{s-1}+P_{s-2})(a_sQ_{s-1}+Q_{s-2})\\ &\quad +C(a_sQ_{s-1}+Q_{s-2})^2\\ &= a_s^2(AP_{s-1}^2+BP_{s-1}Q_{s-1}+CQ_{s-1}^2)+(AP_{s-2}^2+BP_{s-2}Q_{s-2}+CQ_{s-2}^2)\\ &\quad +a_s(2AP_{s-1}P_{s-2}+B(P_{s-1}Q_{s-2}+Q_{s-1}P_{s-2})+2CQ_{s-1}Q_s)\\ &= a_s^2H_s+a_sK_s+H_{s-1}\\ &= H_{s+1}.\end{aligned}$$

De même

$$\begin{aligned}V_s &= 2(a_sP_{s-1}+P_{s-2})P_{s-1}A+2(a_sQ_{s-1}+Q_{s-2})Q_{s-1}C\\ &\quad +((a_sP_{s-1}+P_{s-2})Q_{s-1}+(a_sQ_{s-1}+Q_{s-2})P_{s-1})B\\ &= 2a_s(P_{s-1}^2A+P_{s-1}Q_{s-1}B+Q_{s-1}^2C)+2Q_{s-2}Q_{s-1}C\\ &\quad +2P_{s-2}P_{s-1}A+(P_{s-2}Q_{s-1}+Q_{s-2}P_{s-1})B\\ &= 2a_sH_s+K_s\\ &= K_{s+1}.\end{aligned}$$

Il est clair maintenant que si $A_n\neq 0$ pour tout $n\leq m$, alors

$$A\left(\frac{P_m}{Q_m}\right)^2+B\left(\frac{P_m}{Q_m}\right)+C=\frac{1}{Q_m^2}A_{m+1}.$$

• S'il existe $m\geq 1$ tel que $A_n\neq 0$ pour tout $n\leq m$ et $A_{m+1}=0$, alors

$$A\left(\frac{P_m}{Q_m}\right)^2+B\left(\frac{P_m}{Q_m}\right)+C=0,$$

ce qui donne que $(P_m/Q_m)=[a_1;\dots,a_m]$ est solution de (E).

• Si $A_n\neq 0$ pour tout $n\in\mathbb{N}$, alors on considère la série formelle $f=\lim(P_n/Q_n)=\lim[a_1;\dots,a_n]$, et par conséquent

$$\begin{aligned}Af^2+Bf+C &= \lim A\left(\frac{P_n}{Q_n}\right)^2+B\left(\frac{P_n}{Q_n}\right)+C\\ &= \lim\frac{1}{Q_n^2}A_{n+1}\\ &= 0 \quad (\text{car pour tout } n\in\mathbb{N},\ \deg A_n<\deg B).\end{aligned}$$

Lemme 3. *Soient $q\geq 3$ et Q un polynôme dans $\mathbb{F}_q[X]$. Alors les deux assertions suivantes sont équivalentes* :

(i) $\deg Q$ *est pair et* $\sigma(Q)$ *est un carré parfait.*

(ii) *Il existe deux couples distincts* $(T,S)\in\mathbb{F}_q[X]^2$ *tels que* $\deg T>\deg S$ *et* $Q=T^2-S$.

Preuve. (i)⇒(ii). Soit ϱ une racine carré de $\sigma(Q)$. Posons

$$Q = \sum_{k=0}^{2n} \alpha_k X^k, \quad \alpha_{2n} = \varrho^2,$$

$$T_\varrho = \sum_{k=0}^{n} \beta_k X^k, \quad \beta_n = \varrho.$$

Dire que $\deg(Q - T_\varrho^2) < \deg T_\varrho$ signifie pour tout $k \in \{n, n+1, \dots, 2n\}$,

$$\sum_{\substack{0 \le i \le j \le n \\ i+j=k}} (2 - \varepsilon_{ij})\beta_i\beta_j = \alpha_k, \tag{11}$$

où ε_{ij} vaut 1 si $i = j$ et 0 sinon. Si on suppose les β_t connus pour $s \le t \le n$, alors on sait déterminer d'une manière unique β_{s-1} si $s > 0$. En effet, d'après (11),

$$2\beta_{s-1} = \alpha_{n+s-1} - \sum_{\substack{0 \le i \le j < n \\ i+j=n+s-1}} (2 - \varepsilon_{ij})\beta_i\beta_j,$$

or d'après notre supposition, tous les β_i, β_j sont connus dès que $0 \le i \le j < n$ et $i + j = n + s - 1$, ce qui détermine entièrement les coefficients de T_ϱ en fonction de ceux de Q. L'existence de deux couples (T, S) vérifiant (ii) vient du fait que si $\sigma(Q)$ est un carré parfait $\in \mathbb{F}_q$, alors les seules racines carrées de $\sigma(Q)$ sont ϱ et $q - \varrho$ et par conséquent (T_ϱ, S_ϱ) et $(T_{q-\varrho}, S_{q-\varrho})$ sont les seuls couples vérifiant (ii).

(ii)⇒(i). Il est clair que $\deg Q = 2 \deg T$ et que $\sigma(Q) = \sigma(T^2) = \sigma^2(T)$.

Suite de la démonstration du théorème 4. Soit Q un polynôme de degré pair et $\sigma(Q)$ est un carré parfait. Alors d'après le lemme 3, il existe $T, S \in \mathbb{F}_q[X]$ tels que $\deg T > \deg S$ et $Q = T^2 - S$. D'après le lemme 2, l'équation (F) : $SY^2 + 2TY + 1 = 0$ admet au moins une racine g dans $\mathbb{F}_q((X^{-1}))$ telle que $\deg[g] \ge 1$. Soit donc $f = T + 1/g$, qui vérifie l'équation $f^2 = T^2 - S = Q$. Comme Q n'est pas un carré parfait dans $\mathbb{F}_q[X]$, alors d'après le théorème 2, toute racine carrée f de Q vérifie

$$\mathrm{Per}(f) \le (q^{\deg T} - 1)^2 q^{2 \deg T} < q^{2 \deg Q}$$

et

$$T(f) \le \deg T = \tfrac{1}{2} \deg Q.$$

Corollaire 3. *Soient $q \ge 3$ et $A, B, C \in \mathbb{F}_q[X]$. Soient $\Delta = B^2 - 4AC$ et* (E) *l'équation algébrique $AY^2 + BY + C = 0$. Alors* (E) *admet au moins une solution dans $\mathbb{F}_q((X^{-1}))$ si et seulement si $\deg \Delta$ est pair et $\sigma(\Delta)$ est un carré parfait.*

Preuve. Il est clair que si $\deg \Delta$ est pair et $\sigma(\Delta)$ est un carré parfait, alors d'après le théorème 4, Δ admet une racine carrée $\delta \in \mathbb{F}_q((X^{-1}))$.

On vérifie facilement que les séries formelles $(-B \pm \delta)/(2A)$ sont les seules solutions de (E).

Réciproquement, si f est une solution de (E), il est clair que l'on a $\Delta = (2Af+B)^2$, ce qui donne que $\deg \Delta$ est pair et que $\sigma(\Delta)$ est un carré parfait.

Par la suite Δ désigne le discriminant de la série formelle quadratique solution de (E).

Un nombre réel x est dit *quadratique* s'il est irrationnel et vérifie une équation du type $ax^2 + bx + c = 0$ avec a, b, c des entiers relatifs premiers entre eux. On note par la suite $\Delta(x) = b^2 - 4ac$ le discriminant de x. Lewittes [6] a montré les deux théorèmes suivants :

THÉORÈME. *Soit x un nombre réel quadratique. Alors les trois propriétés suivantes sont équivalentes* :

(i) *x est palindromique.*
(ii) $\mathrm{Norme}(x) = -1$.
(iii) *$\Delta(x)$ est la somme de deux carrés.*

THÉORÈME. *Soient $A(n)$ l'ensemble des nombres quadratiques x dont le discriminant $\Delta(x)$ égal à n et $w(n)$ le nombre de facteur premier de n. Si $16 \mid n$ ou si n admet un facteur premier $\equiv 3 \pmod 4$, alors $A(n) = 0$. Si tout facteur premier de $n \equiv 1 \pmod 4$, alors $A(n) = A(4n) = 2^{w(n)-1}$ et $A(8n) = 2^{w(n)}$.*

Cela donne dans le cas des séries formelles le théorème 5 :

Démonstration du théorème 5. Soit f une série formelle palindromique. Alors elle est de type (I), donc elle vérifie une équation de type $Af^2 + Bf + C = 0$ avec $\deg B > \deg A, \deg C$. D'après le lemme 1, si $f = [a_1; \overline{a_2, \ldots, a_n, a_1}]$, alors $(f + B/A)^{-1} = [a_n; \overline{a_{n-1}, \ldots, a_1, a_n}]$. Puisque f est palindromique, on a $f = (f + B/A)^{-1}$. D'autre part si $A(n, q)$ est le nombre de séries formelles palindromiques dont le degré du discriminant est égal à $2n$, alors $A(n, q)$ est majoré par $B(n, q)$, le nombre de représentations des polynômes de degré $2n$ sous la forme de la somme de deux carrés dont le degré $\leq n$. Mireille Car [2], [3] a donné une formule asymptotique de $B(n, q)$, à savoir : si $p \equiv 1 \pmod 4$, alors

$$B(n,q) = O\left(\frac{q^{2n}}{n^{\alpha}\sqrt{\log 2n}}\right) \quad \text{avec } \alpha = 1 - \frac{1 + \log\log 2}{\log 2},$$

et si $p \equiv 3 \pmod 4$, alors

$$B(n,q) \sim a\frac{q^{2n}}{\sqrt{n\pi}} \quad \text{avec } a = \prod_{P \in I}(1 - q^{-2\deg P})^{-1/2}$$

et I est l'ensemble de polynômes unitaires et irréductibles dans $\mathbb{F}_q[X]$.

Bibliographie

[1] L. E. Baum and M. M. Sweet, *Continued fraction of algebraic power series in characteristic* 2, Ann. of Math. 103 (1976), 593–610.

[2] M. Car, *Polynômes de* $\mathbb{F}_q[X]$ *ayant un diviseur de degré donné*, Acta Arith. 43 (1984), 131–154.

[3] —, *Normes dans* $\mathbb{F}_q[X]$ *de polynômes de* $\mathbb{F}_{q^h}[X]$, C. R. Acad. Sci. Paris 288 (1979), 669–672; Correction, ibid., 1049.

[4] H. Cohen, *Multiplication par un entier d'une fraction continue périodique*, Acta Arith. 26 (1974–75), 129–148.

[5] J. H. E. Cohn, *The length of the period of the simple continued fraction of* $d^{1/2}$, Pacific J. Math. 71 (1977), 21–32.

[6] J. Lewittes, *Quadratic irrationals and continued fractions*, in: Number Theory (New York, 1991–1995), Springer, New York, 1996, 253–268.

[7] M. Mkaouar, *Sur le développement en fractions continues des séries formelles quadratiques sur* $\mathbb{F}_2(X)$, J. Number Theory 80 (2000), 169–173.

[8] A. Schinzel, *On some problems of the arithmetical theory of continued fractions. I*, Acta Arith. 6 (1961), 394–413; *II*, ibid. 7 (1962), 287–298; Corrigendum, ibid. 47 (1986), 295.

Département de Mathématiques
Faculté des Sciences de Sfax
Route Soukra km 3,5
3038 Sfax-Tunisie
E-mail: mohamed.mkaouar@fss.rnu.tn

Reçu le 12.7.1999
et révisé le 22.5.2000 (3647)