ACTA ARITHMETICA
LXVIII.1 (1994)

Polynômes singuliers à plusieurs variables sur un corps fini et congruences modulo p^2

par

El Mostafa Hanine (Toulouse)

1. Introduction. Dans ce travail on s'intéresse à la classification des polynômes singuliers de degré 4 sur un corps fini et aux congruences modulo p^2. Dans toute la suite $\mathbb{K}$ désignera un corps fini de caractéristique p à $q = p^a$ éléments, p un nombre premier impair et $\overline{\mathbb{K}}$ une clôture algébrique de $\mathbb{K}$.

Cette étude s'article comme suit :

• démontrer tout d'abord que si $\operatorname{Card}\mathbb{K} > m^2$, tout $f \in \mathbb{K}[X]$ de degré m, à valeurs carrées dans $\mathbb{K}$, est un carré dans $\mathbb{K}[X]$,

• généraliser un théorème de Carlitz [2] au cas de polynômes à plusieurs variables,

• démontrer aussi que pour tout entier $n \geq 9$ et pour tout $F \in \mathbb{K}[X_1, \ldots, X_n]$ singulier de degré 4 sans terme constant, si $q \geq 37$ il existe $v \in \mathbb{K}$ non carré et g_1, g_2 éléments de $\mathbb{K}[X_1, \ldots, X_n]$ de degré 2 sans termes constants tels que

$$F = \varepsilon(g_1^2 - vg_2^2) \quad \text{où } \varepsilon = \pm 1.$$

Ceci généralise le résultat de D. J. Lewis [5].

Dans [3] on a démontré que pour tout entier $d \geq 1$, il existe des nombres premiers dont la plus petite valeur, $p(d)$, vérifie la propriété suivante : pour tout p nombre premier $\geq p(d)$ et pour tout $F \in \mathbb{Z}_p[X_1, \ldots, X_{2d+1}]$ de degré d sans terme constant, l'équation $F(x_1, \ldots, x_{2d+1}) \equiv 0 \pmod{p^2}$ admet une solution primitive.

Il a été aussi démontré dans le même article que $p(2) = 2$, $p(3) = 3$ et que pour tout $d \geq 4$ on a $p(d) > 2$.

Cette étude va nous permettre de démontrer que 37 est un majorant de $p(4)$.

2. Polynômes à plusieurs variables sur un corps fini à valeurs une puissance e-ième. On va commencer par énoncer le théorème de Carlitz [2].

2.1. Théorème. *Pour tout $m \geq 1$ et pour tout diviseur e de m, il existe un entier $\lambda(m,e) > m$ tel que si $q \geq \lambda(m,e)$ et e divise $q-1$, tout polynôme de $\mathbb{K}[X]$ de degré m dont les valeurs sont des puissances e-ièmes dans $\mathbb{K}$ est une puissance e-ième d'un polynôme de $\mathbb{K}[X]$.*

On généralise ce théorème au cas de polynômes à plusieurs variables comme suit :

2.2. Théorème. *Soient $F \in \mathbb{K}[X_1,\dots,X_n]$ de degré m tel que $F(x)$ soit une puissance e-ième dans $\mathbb{K}$ pour tout $x \in \mathbb{K}^n$ et e un diviseur de m. Si $q \geq \lambda(m,e)$ et e divise $q-1$, alors il existe $f \in \mathbb{K}[X_1,\dots,X_n]$ vérifiant $F = f^e$.*

P r e u v e. Les cas $F = 0$ et $e = 1$ sont triviaux. On suppose maintenant que $F \neq 0$ et $e > 1$. F peut s'écrire $F = F_0 + F_1 + \ldots + F_m$ où F_i désigne la composante homogène de F de degré i et $F_m \neq 0$. Par hypothèse $m < q$, donc $\deg_i F_m \leq q-1$ pour tout $i = 1,\dots,n$. Il existe alors $a \in \mathbb{K}^n - \{(0,\dots,0)\}$ tel que $F_m(a) \neq 0$.

Considérons une transformation linéaire, homogène et inversible des variables X_i transformant a en $(1,0,\dots,0)$. On peut écrire $X_i = \sum_{j=1}^{n} a_{ij} Y_j$. Posons $G_m(Y) = F_m(X)$. On a

$$G_m(Y) = \alpha Y_1^m + Y_1^{m-1} A_1(Y_2,\dots,Y_n) + \ldots + Y_1 A_{m-1}(Y_2,\dots,Y_n) + A_m(Y_2,\dots,Y_n)$$

où $G_m((1,0,\dots,0)) \neq 0$, A_i désigne une forme de degré i et $\alpha \in \mathbb{K}^*$. En appliquant la même transformation à F_i pour $i = 1,\dots,m-1$, on obtient un élément G_i de $\mathbb{K}[Y_1,\dots,Y_n]$ tel que $F_i(X) = G_i(Y)$. D'où

$$F(X) = \sum_{i=0}^{m-1} G_i(Y) + G_m(Y) \quad \text{et} \quad \deg_1\Big(\sum_{i=1}^{m-1} G_i(Y)\Big) \leq m-1.$$

Posons $F(X) = G(Y)$. On obtient

$$G(Y) = \alpha Y_1^m + Y_1^{m-1} f_1(Y_2,\dots,Y_n) + \ldots + Y_1 f_{m-1}(Y_2,\dots,Y_n) + f_m(Y_2,\dots,Y_n)$$

où $f_i \in \mathbb{K}[Y_2,\dots,Y_n]$ est un polynôme de degré inférieur ou égal à i.

Soit $(c_2,\dots,c_n) \in \mathbb{K}^{n-1}$. Alors $G(Y_1,c_2,\dots,c_n)$ est un élément de $\mathbb{K}[Y_1]$ de degré m et $G(c_1,c_2,\dots,c_n)$ est une puissance e-ième dans $\mathbb{K}$ pour tout $c_1 \in \mathbb{K}$.

Comme $q \geq \lambda(m,e)$, d'après le théorème 2.1, il existe $P_{c_2,\dots,c_n} \in \mathbb{K}[Y_1]$ tel que $G(Y_1,c_2,\dots,c_n) = (P_{c_2,\dots,c_n}(Y_1))^e$. Par ailleurs, on peut supposer dans l'expression de G que $\alpha = 1$. Donc $P_{c_2,\dots,c_n}$ peut s'écrire sous la forme

$$P_{c_2,\dots,c_n} = Y_1^g + B_1(c_2,\dots,c_n) Y_1^{g-1} + \ldots + B_{g-1}(c_2,\dots,c_n) Y_1 + B_g(c_2,\dots,c_n)$$

où $B_1,\dots,B_g$ sont des applications de $\mathbb{K}^{n-1}$ dans $\mathbb{K}$ et $g = m/e$.

Considérons maintenant les polynômes P_i $(i = 1, \ldots, g)$ définis par

$$P_i(Y_2, \ldots, Y_n) = \sum_{(y_2,\ldots,y_n)\in\mathbb{K}^{n-1}} B_i(y_2, \ldots, y_n) \prod_{j=2}^{n} (1 - (Y_j - y_j)^{q-1}).$$

Montrons que

$$G(Y_1, \ldots, Y_n)$$
$$= (Y_1^g + P_1(Y_2, \ldots, Y_n)Y_1^{g-1} + \ldots + P_{g-1}(Y_2, \ldots, Y_n)Y_1 + P_g(Y_2, \ldots, Y_n))^e.$$

Pour cela on a besoin de la proposition suivante [4, p. 144] :

PROPOSITION. *Soit $f \in \mathbb{K}[X_1, \ldots, X_n]$. Il existe un polynôme unique $\bar{f} \in \mathbb{K}[X_1, \ldots, X_n]$ tel que $\deg_i \bar{f} \leq q - 1$ pour tout $i = 1, \ldots, n$ et $f \equiv \bar{f} \pmod I$ où I est l'idéal de $\mathbb{K}[X_1, \ldots, X_n]$ engendré par les polynômes $X_1^q - X_1$, $X_2^q - X_2, \ldots, X_n^q - X_n$.*

Par construction P_i est à la forme réduite et $P_i(c_2, \ldots, c_n)$=$B_i(c_2, \ldots, c_n)$ pour tout $(c_2, \ldots, c_n) \in \mathbb{K}^{n-1}$. Par suite, on a

$$G(Y_1, \ldots, Y_n) \equiv (Y_1^g + P_1(Y_2, \ldots, Y_n)Y_1^{g-1} + \ldots \\ \ldots + P_{g-1}(Y_2, \ldots, Y_n)Y_1 + P_g(Y_2, \ldots, Y_n))^e \pmod I$$

où I est l'idéal engendré par $Y_1^q - Y_1, \ldots, Y_n^q - Y_n$.

D'autre part, comme

$$(Y_1^g + P_1(Y_2, \ldots, Y_n)Y_1^{g-1} + \ldots + P_{g-1}(Y_2, \ldots, Y_n)Y_1 + P_g(Y_2, \ldots, Y_n))^e \\ = Y_1^m + \sum_{r=1}^{m} \Big(\sum_{i_1+\ldots+i_e=r} P_{i_1} \ldots P_{i_e} \Big) Y_1^{m-r},$$

on a

$$Y_1^m + f_1 Y_1^{m-1} + \ldots + f_{m-1}Y_1 + f_m \\ \equiv Y_1^m + \sum_{r=1}^{m} \Big(\sum_{i_1+\ldots+i_e=r} P_{i_1} \ldots P_{i_e} \Big) Y_1^{m-r} \pmod I.$$

Par conséquent,

$$\sum_{r=1}^{m} \overline{\Big(f_r - \sum_{i_1+\ldots+i_e=r} P_{i_1} \ldots P_{i_e} \Big)} Y_1^{m-r} \equiv 0 \pmod I.$$

Or

$$\deg_i \sum_{r=1}^{m} \overline{\Big(f_r - \sum_{i_1+\ldots+i_e=r} P_{i_1} \ldots P_{i_e} \Big)} Y_1^{m-r} \leq q - 1 \quad \text{pour tout } i = 1, \ldots, n.$$

D'où

$$\sum_{r=1}^{m} \overline{\Big(f_r - \sum_{i_1+\ldots+i_e=r} P_{i_1}\ldots P_{i_e}\Big)} Y_1^{m-r} = 0$$

(d'après la proposition précédente), donc

$$f_r \equiv \sum_{i_1+\ldots+i_e=r} P_{i_1}\ldots P_{i_e} \pmod{I}.$$

Par récurrence sur r on montre que

$$f_r = \sum_{i_1+\ldots+i_e=r} P_{i_1}\ldots P_{i_e} \quad \text{et} \quad \deg P_{i_j} \le i_j \quad \text{pour } i_j \le r$$

(pour tout $r = 1, \ldots, m$).

Finalement,

$$G(Y_1,\ldots,Y_n) = (Y_1^g + P_1(Y_2,\ldots,Y_n)Y_1^{g-1} + \ldots + P_{g-1}(Y_2,\ldots,Y_n)Y_1 + P_g(Y_2,\ldots,Y_n))^e.$$

En revenant aux variables $X_1,\ldots,X_n$, on obtient un polynôme $f \in \mathbb{K}[X_1,\ldots,X_n]$ tel que $F = f^e$.

D'autre part, dans [1] Carlitz a démontré le résultat suivant :

Si f est un polynôme de $\mathbb{K}[X]$ de degré m pair, si $q > (m-1)^2$ et si les valeurs prises par f sur $\mathbb{K}$ sont toujours des carrés non nuls, alors f est un carré dans $\mathbb{K}[X]$.

Dans ce qui suit, on se propose de généraliser ce résultat au cas où f prend des valeurs carrées quelconques. Ceci va nous permettre de donner un majorant de $\lambda(m,2)$.

2.3. Théorème. *Soit $f \in \mathbb{K}[X]$ de degré m tel que $m^2 < q$. Si les valeurs prises par f sur $\mathbb{K}$ sont toujours des carrés, alors m est pair et il existe $g \in \mathbb{K}[X]$ tel que $f = g^2$.*

P r e u v e. Supposons qu'il n'existe pas $g \in \mathbb{K}[X]$ tel que $f = g^2$. D'après le théorème 2c′ de [6, p. 43] on a

$$\Big|\sum_{x\in\mathbb{K}} \chi(f(x))\Big| \le (N-1)q^{1/2}$$

où χ est un caractère d'ordre 2 de $\mathbb{K}^*$ et N le nombre de racines distinctes de f dans $\mathbb{K}$.

Or pour tout $x \in \mathbb{K}$, si $f(x) = 0$, on a $\chi(f(x)) = 0$ et si $f(x) \neq 0$, on a $\chi(f(x)) = 1$ puisque $f(x)$ est un carré dans $\mathbb{K}$. D'où $\sum_{x\in\mathbb{K}} \chi(f(x)) = q - N$. Ceci entraîne que $q - N \le (N-1)\sqrt{q}$ et donne, en élevant au carré, $q^2 - (2N + (N-1)^2)q + N^2 \le 0$. Ainsi $q \le N^2$, ce qui démontre le théorème.

3. Polynômes singuliers sur un corps fini à 9 variables au moins

Définition. Soient $\mathbb{K}$ un corps et F un élément de $\mathbb{K}[X_1,\dots,X_n]$ non nul et sans terme constant. On dit que F est *singulier* si pour tout $x = (x_1,\dots,x_n) \in \mathbb{K}^n - \{(0,\dots,0)\}$ tel que $F(x) = 0$, on a $\frac{\partial F}{\partial X_i}(x) = 0$ pour tout $1 \le i \le n$.

3.1. Théorème. *Soient n un entier ≥ 9 et F un élément de $\mathbb{K}[X_1,\dots,X_n]$ de degré 4, singulier et sans terme constant. Si $q > 36$, il existe un élément v non carré de $\mathbb{K}$, et deux éléments g_1 et g_2 de $\mathbb{K}[X_1,\dots,X_n]$ de degré ≤ 2 et sans terme constant tels que*

$$F = \varepsilon(g_1^2 - vg_2^2) \quad \text{où } \varepsilon = \pm 1.$$

Pour démontrer ce théorème on a besoin des lemmes suivants où F désigne le polynôme défini dans le théorème 3.1.

3.2. Lemme. *Il existe une transformation linéaire homogène et inversible des variables $X_i = L_i(Y_1,\dots,Y_n)$ telle que*

$$\begin{aligned} F(X_1,\dots,X_n) &= G(Y_1,\dots,Y_n) \\ &= Y_1^2 Q(Y_2,\dots,Y_n) + 2Y_1 C(Y_2,\dots,Y_n) + U(Y_2,\dots,Y_n) \end{aligned}$$

où G, Q, C et U sont des éléments de $\mathbb{K}[X_1,\dots,X_n]$ vérifiant les propriétés suivantes : G dépend de Y_1, Q est une forme quadratique, C et U sont sans composante homogène de degré ≤ 1 et respectivement de degré ≤ 3 et ≤ 4.

P r e u v e. Comme F est singulier, la composante homogène de degré 1 est nulle [3]. Ainsi $F = F_4 + F_3 + F_2$ où F_i représente la composante homogène de degré i de F.

D'après le théorème de Warning le nombre d'éléments dans $\mathbb{K}^n$ qui vérifient $F_4(x) = 0$ et $(F_3+F_2)(x) = 0$ est supérieur ou égal à q^{n-7}. Dès lors, il existe x_0, x_1 et x_2 éléments de $\mathbb{K}^n - \{(0,\dots,0)\}$ linéairement indépendants tels que x_0 et x_1 soient des zéros communs de F_4 et de F_3+F_2 et $F_4(x_2) \ne 0$. Il existe alors une transformation homogène linéaire et inversible des variables $X_i = u_i(Z_1,\dots,Z_n)$ qui transforme $(1,1,\dots,0)$, $(-1,1,0,\dots,0)$ et $(1,0,\dots,0)$ respectivement en x_0, x_1 et x_2.

Posons $H(Z_1,\dots,Z_n) = F(X_1,\dots,X_n) = F(u_1,\dots,u_n)$. Alors H peut s'écrire sous la forme

$$H = a_1Z_1^4 + a_2Z_1^3Z_2 + a_3Z_1^2Z_2^2 + a_4Z_1Z_2^3 + a_5Z_2^4 + R + H_3 + H_2$$

où $a_1 \ne 0$, R est une forme nulle ou de degré 4 n'admettant pas de monômes de la forme $\alpha Z_1^{n_1}Z_2^{n_2}$, et H_3 et H_2 sont les composantes homogènes de degré respectivement 3 et 2.

Considérons G_1 et G_2 définis par $G_1(Y_1,\dots,Y_n) = H(Y_1, Y_1+Y_2, Y_3,\dots$ $\dots,Y_n)$ et $G_2 = H(Y_1, -Y_1+Y_2, Y_3,\dots,Y_n)$. Ils s'écrivent alors sous la forme

$$G_1 = (a_1+a_2+a_3+a_4+a_5)Y_1^4 + (a_2+2a_3+3a_4+4a_5)Y_1^3Y_2 + (a_3+3a_4+6a_5)Y_1^2Y_2^2 + (a_4+4a_5)Y_1Y_2^3 + a_5Y_2^4 + R' + H_2' + H_3',$$
$$G_2 = (a_1-a_2+a_3-a_4+a_5)Y_1^4 + (a_2-2a_3+3a_4-4a_5)Y_1^3Y_2 + (a_3-3a_4+6a_5)Y_1^2Y_2^2 + (a_4-4a_5)Y_1Y_2^3 + a_5Y_2^4 + R'' + H_2'' + H_3''$$

où R' et R'' sont des formes nulles ou de degré 4 et ne contiennent pas de monômes de la forme $\alpha Y_1^{n_1}Y_2^{n_2}$, et H_2', H_3', H_2'' et H_3'' sont des formes de degré ≤ 3. Dès lors, G_1 ou G_2 va dépendre de Y_1 : sinon $a_1 = a_2 = a_3 = a_4 = a_5 = 0$, ce qui contredit le fait que $a_1 \neq 0$.

Soit G le polynôme qui dépend de Y_1. G peut s'écrire

$$G = aY_1^4 + bY_1^3 + cY_1^2 + Y_1^3(\alpha_2Y_2 + \ldots + \alpha_nY_n) + Y_1^2(Q(Y_2,\ldots,Y_n) + \beta_2Y_2 + \ldots + \beta_nY_n) + Y_1(C(Y_2,\ldots,Y_n) + \gamma_2Y_2 + \ldots + \gamma_nY_n) + U(Y_2,\ldots,Y_n).$$

D'après ce qui précède, la composante homogène de degré 4 de G vérifie $G_4(1,0,\ldots,0) = 0$, d'où $a = 0$. D'autre part, on a les relations

$$G(1,0,\ldots,0) = b + c = 0, \tag{1}$$
$$\frac{\partial G}{\partial Y_1}(1,0,\ldots,0) = 3b + 2c = 0. \tag{2}$$

(2) est vérifiée puisque G est singulier comme F. A partir de (1) et (2) nous déduisons que $b = c = 0$.

Dès lors, $G(x,0,\ldots,0) = 0$ pour tout $x \in \mathbb{K}$, et comme G est singulier on a

$$\frac{\partial G}{\partial Y_i}(x,0,\ldots,0) = \alpha_i x^3 + \beta_i x^2 + \gamma_i x = 0 \quad \text{pour tout } i \in \{2,\ldots,n\}.$$

Comme $\operatorname{Card}\mathbb{K} > 3$, on en déduit que $\alpha_i = \beta_i = \gamma_i = 0$ pour tout $i \in \{2,\ldots,n\}$, d'où le lemme.

3.3. Lemme. (i) *Soit $y \in \mathbb{K}^{n-1}$. Si $Q(y) = 0$, alors $C(y) = 0$.*
(ii) *Q est une forme quadratique non nulle.*
(iii) *U est singulier.*
(iv) *Soit $y \in \mathbb{K}^{n-1}$. Si $U(y) = 0$, alors $C(y) = 0$.*

Preuve. (i) Si $C(y) \neq 0$, on a

$$G\left(\frac{-U(y)}{2C(y)}, y\right) = 0,$$

ce qui donne

$$\frac{\partial G}{\partial Y_1}\left(\frac{-U(y)}{2C(y)}, y\right) = \frac{-2U(y)}{C(y)}Q(y) + 2C(y) \neq 0.$$

Ceci contredit le fait que G est singulier.

(ii) Si Q est nulle, C est nulle d'après (i). Ceci contredit que G dépend de Y_1.

(iii) et (iv) sont des conséquences du fait que G est singulier.

Dans la suite posons $\Delta = C^2 - QU$.

3.4. Lemme. *Si $\Delta = vD^2$ où $D \in \mathbb{K}[Y_2, \ldots, Y_n]$ de degré ≤ 3 et $v \in \mathbb{K}$, alors Q est une forme singulière.*

Preuve. Soit $y \in \mathbb{K}^{n-1}$ tel que $Q(y) = 0$. En vertu du lemme 3.3, $C(y) = 0$ et donc $D(y) = 0$. Par conséquent, $U\frac{\partial Q}{\partial Y_i}(y) = 0$.

• Si $U(y) = 0$, alors y est un zéro singulier de Q. En effet, supposons qu'il existe $i_0 \in \{2, \ldots, n\}$ tel que $\frac{\partial Q}{\partial Y_{i_0}}(y) \neq 0$. Considérons $a \in \mathbb{K}$ tel que

$$a^2 \frac{\partial Q}{\partial Y_{i_0}}(y) + 2a \frac{\partial C}{\partial Y_{i_0}}(y) \neq 0.$$

On a alors $G(a, y) = 0$ et $\frac{\partial G}{\partial Y_{i_0}}(a, y) \neq 0$, ce qui est absurde.

• Si $U(y) \neq 0$, alors $\frac{\partial Q}{\partial Y_i}(y) = 0$.

3.5. Lemme. *Il existe $\mu \in \mathbb{K}^*$ non carré tel que pour tout $y \in \mathbb{K}^{n-1}$, $\mu\Delta(y)$ soit un carré dans $\mathbb{K}$.*

Preuve. Soit $\mu \in \mathbb{K}^*$ et non carré. S'il existe $y \in \mathbb{K}^{n-1}$ tel que $\mu\Delta(y)$ soit non carré dans $\mathbb{K}$, alors $\mu\Delta(y)\mu^{-1} = \Delta(y)$ est un carré non nul et il existe $k \in \mathbb{K}^*$ tel que $\Delta(y) = k^2$. Comme $\Delta(y) \neq 0$, alors $Q(y) \neq 0$. Dès lors, l'équation $Y_1^2 Q(y) + 2Y_1 C(y) + U(y) = 0$ admet comme racine $(k - C(y))/Q(y)$. Ainsi $((k - C(y))/Q(y), y)$ serait un zéro non singulier de G, ce qui est absurde.

3.6. Lemme. *Soit $Q \in \mathbb{K}[Y_2, \ldots, Y_n]$ une forme quadratique. Si Q est une forme singulière, elle peut s'écrire sous la forme $Q(Y) = \varepsilon[L_1^2 - vL_2^2]$ où $\varepsilon = \pm 1$ et v est non carré dans $\mathbb{K}$, L_1 et L_2 étant deux formes linéaires de $\mathbb{K}[Y_2, \ldots, Y_n]$.*

La preuve résulte du lemme 3.2 de [3].

Preuve du théorème 3.1. D'après le lemme 3.2, il existe une transformation linéaire homogène et inversible des variables telle que $F(X_1, \ldots, X_n) = G(Y_1, \ldots, Y_n)$ où G dépend de Y_1 et s'écrit

$$G(Y_1, \ldots, Y_n) = Y_1^2 Q(Y_2, \ldots, Y_n) + 2Y_1 C(Y_2, \ldots, Y_n) + U(Y_2, \ldots, Y_n). \tag{3}$$

1er cas : Si $U = 0$ alors, d'après le lemme 3.3, $C(a) = 0$ pour tout $a \in \mathbb{K}^{n-1}$. C est alors nul puisque $\deg C \leq 3 < \operatorname{Card} \mathbb{K}$. Par suite, $G(Y) = Y_1^2 Q(Y_2, \ldots, Y_n)$ et Q est singulière. En vertu du lemme 3.6, Q s'écrit $Q = \varepsilon[L_1^2 - vL_2^2]$ où $\varepsilon = \pm 1$ et v est un élément non carré de $\mathbb{K}$, L_1 et L_2 étant deux formes linéaires de $\mathbb{K}[Y_2, \ldots, Y_n]$. Donc

$$G = \varepsilon Y_1^2 [L_1^2 - vL_2^2] = \varepsilon[(Y_1 L_1)^2 - v(Y_1 L_2)^2].$$

Par la transformation inverse, F peut s'écrire sous la forme

$$F(X) = \varepsilon[g_1(X)^2 - vg_2(X)^2].$$

2-ième cas : Si $U \neq 0$, d'après le lemme 3.3 on a $Q \neq 0$. Montrons que $\Delta = vD^2$ où $v \in \mathbb{K}$ est non carré et $D \in \mathbb{K}[Y_2, \ldots, Y_n]$ est de degré ≤ 3 sans terme constant.

D'après le lemme 3.5, il existe $\lambda \in \mathbb{K}$ non carré tel que $\lambda\Delta(a)$ soit un carré dans $\mathbb{K}$ pour tout $a \in \mathbb{K}^{n-1}$. De plus, si d est le degré de $\lambda\Delta$, on a $d \leq 6 < \lambda(d, 2) < 36 \leq \operatorname{Card}\mathbb{K}$. D'après le théorème 2.2, il existe alors $D \in \mathbb{K}[Y_2, \ldots, Y_n]$ de degré ≤ 3 sans terme constant tel que $\lambda\Delta = D^2$, d'où le résultat en posant $v = 1/\lambda$. En vertu du lemme 3.4, Q est singulière; elle peut s'écrire alors

$$Q = \varepsilon[L_1^2 - \mu L_2^2]$$

où μ est non carré dans $\mathbb{K}$ et $\varepsilon = \pm 1$. Dès lors,

$$Q = \varepsilon[L_1^2 - v\mu v^{-1} L_2^2].$$

Comme μv^{-1} est un carré dans $\mathbb{K}$, il existe une forme linéaire L_3 vérifiant $\mu v^{-1} L_2^2 = L_3^2$. Par suite, $Q = \varepsilon[L_1^2 - vL_3^2]$.

Montrons que

$$C = L_1 q_1 - vL_3 q_2$$

où q_1 et q_2 sont deux éléments de $\mathbb{K}[Y_2, \ldots, Y_n]$ de degré ≤ 2 et sans terme constant.

En décomposant Q et $C^2 - vD^2$ dans $\mathbb{K}(v^{1/2})[Y_2, \ldots, Y_n]$ on a

$$\varepsilon(L_1 - v^{1/2}L_3)(L_1 + v^{1/2}L_3)U = (C - v^{1/2}D)(C + v^{1/2}D).$$

Donc $L_1 - v^{1/2}L_3$ divise $(C - v^{1/2}D)(C + v^{1/2}D)$. On a aussi

$$C - v^{1/2}D \neq 0 \quad \text{et} \quad C + v^{1/2}D \neq 0.$$

En effet, si $C + v^{1/2}D = 0$ ou $C - v^{1/2}D = 0$, alors $C = 0$ et $D = 0$ puisque $(1, v^{1/2})$ est une base de $\mathbb{K}[v^{1/2}]$ considéré comme $\mathbb{K}$-espace vectoriel. On a alors $QU = C^2 - vD^2 = 0$ et par conséquent $Q = 0$, ce qui est impossible (lemme 3.3).

En choisissant donc d'avance un signe de D, c'est-à-dire $\pm D$, on peut supposer que $L_1 - v^{1/2}L_3$ divise $C + v^{1/2}D$. Il existe alors $q' \in \mathbb{K}[v^{1/2}][Y_2, \ldots, Y_n]$ de degré ≤ 2 tel que $C + v^{1/2}D = (L_1 - v^{1/2}L_3)q'$. Par ailleurs, q' peut s'écrire $q' = q_1 + v^{1/2}q_2$ où q_1 et q_2 sont des éléments de $\mathbb{K}[Y_2, \ldots, Y_n]$ de degré ≤ 2 et sans terme constant. Ainsi

$$C + v^{1/2}D = (L_1 - v^{1/2}L_3)(q_1 + v^{1/2}q_2)$$

et

$$(C - L_1 q_1 + vL_3 q_2) + (D - L_1 q_2 + L_3 q_1)v^{1/2} = 0.$$

Ceci entraîne que $(C - L_1q_1 + vL_3q_2)(a) = 0$ et $(D - L_1q_2 + L_3q_1)(a) = 0$ pour tout $a \in \mathbb{K}^{n-1}$.

D'autre part, on a $\deg(C - L_1q_1 + vL_3q_2) \leq 3 < \operatorname{Card}\mathbb{K}$, d'où $C - L_1q_1 + vL_3q_2 = 0$ et $C = L_1q_1 - vL_3q_2$.

Montrons que $U = \varepsilon(q_1^2 - vq_2^2)$. On a

$$C + v^{1/2}D = (L_1 - v^{1/2}L_3)(q_1 + v^{1/2}q_2). \tag{4}$$

En appliquant à l'égalité (4) le $\mathbb{K}$-isomorphisme qui transforme $v^{1/2}$ en $-v^{1/2}$, on obtient

$$C - v^{1/2}D = (L_1 + v^{1/2}L_3)(q_1 - v^{1/2}q_2). \tag{5}$$

Multiplions (4) et (5) membre à membre; on obtient

$$C^2 - vD^2 = \varepsilon(L_1^2 - vL_3^2)(q_1^2 - vq_2^2).$$

Comme $Q = \varepsilon(L_1^2 - vL_3^2)$, $C^2 - vD^2 = \varepsilon Q(q_1^2 - vq_2^2)$, on peut écrire

$$QU = C^2 - vD^2 = \varepsilon Q(q_1^2 - vq_2^2)$$

et par suite

$$U = \varepsilon(q_1^2 - vq_2^2).$$

Dans l'expression de G donnée par (3), en remplaçant Q, C et U respectivement par $\varepsilon(L_1^2 - vL_3^2)$, $L_1q_1 - vL_3q_2$ et $\varepsilon(q_1^2 - vq_2^2)$, on obtient

$$\begin{aligned} G(Y) &= \varepsilon Y_1^2(L_1^2 - vL_3^2) + 2Y_1(L_1q_1 - vL_3q_2) + \varepsilon(q_1^2 - vq_2^2) \\ &= \varepsilon[[Y_1L_1 + \varepsilon q_1]^2 - v[Y_1L_3 + \varepsilon q_2]^2]. \end{aligned}$$

Finalement, par la transformation inverse, on a

$$F = \varepsilon[g_1^2 - vg_2^2]$$

où g_1 et g_2 sont deux éléments de $\mathbb{K}[X_1, \ldots, X_n]$ de degré ≤ 2 et sans terme constant.

4. Les équations diophantiennes modulo p^2 de degré 4

Définition. On dit que $(x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ est *primitif* si l'un des x_i n'est pas divisible par p.

4.1. Théorème. *Soit p un nombre premier supérieur ou égal à 37. Alors pour tout $f \in \mathbb{Z}_p[X_1, \ldots, X_9]$ de degré quatre et sans terme constant, l'équation $f(x_1, \ldots, x_9) \equiv 0 \pmod{p^2}$ admet une solution primitive.*

Preuve. Considérons $F = \bar{f} \in \mathbb{F}_p[X_1, \ldots, X_9]$.

1er cas : Si F est nul, il existe $h \in \mathbb{Z}_p[X_1, \ldots, X_9]$ tel que $f = ph$. D'après le théorème de Chevalley–Warning, h admet une solution primitive $(x_1, \ldots, x_9)$ qui vérifie $f(x_1, \ldots, x_9) \equiv 0 \pmod{p^2}$.

2-ième cas : Si F est non singulier, ils existent $(x_1,\dots,x_9)\in\mathbb{F}_p^9$ et $1\le i_0\le 9$ tels que

$$F(x_1,\dots,x_9)=0 \quad \text{et} \quad \frac{\partial F}{\partial X_{i_0}}(x_1,\dots,x_9)\neq 0.$$

D'après le lemme de Hensel, il existe $(y_1,\dots,y_9)\in\mathbb{Z}_p^9$ primitif tel que $f(y_1,\dots,y_9)$ soit nul, ce qui implique $f(y_1,\dots,y_9)\equiv 0 \pmod{p^2}$.

3-ième cas : Si F est singulier et de degré 4, écrivons $F=F_4+F_3+F_2$, où F_i désigne la composante homogène de F de degré i. D'après le théorème précédent, on a $F=\varepsilon[g_1^2-vg_2^2]$ où $g_1,g_2\in\mathbb{F}_p[X_1,\dots,X_9]$ sont de degré ≤ 2 et sans terme constant.

D'autre part, soient $g_1',g_2'\in\mathbb{Z}_p[X_1,\dots,X_9]$ de degré ≤ 2 et sans terme constant tels que $\overline{g}_1'=g_1$ et $\overline{g}_2'=g_2$. Considérons $G\in\mathbb{Z}_p[X_1,\dots,X_9]$ tel que

$$f=\varepsilon((g_1'(X))^2-v(g_2'(X))^2)+pG.$$

Le système

$$\begin{aligned} g_1'(x_1,\dots,x_9)&\equiv 0 \pmod p,\\ g_2'(x_1,\dots,x_9)&\equiv 0 \pmod p,\\ G(x_1,\dots,x_9)&\equiv 0 \pmod p \end{aligned}$$

vérifie les hypothèses du théorème de Chevalley–Warning, il admet donc une solution primitive $(x_1,\dots,x_9)\in\mathbb{Z}_p^9$. Cette solution vérifie $f(x_1,\dots,x_9)\equiv 0 \pmod{p^2}$.

4-ième cas : Si F est singulier et de degré ≤ 3, les lemmes 3.2 et 4.1 de [3] permettent de démontrer le théorème dans ce cas.

Ainsi $p(4)\le 37$; mais est-ce que 37 est une valeur optimale?

Références

[1] L. Carlitz, *A problem of Dickson's*, Duke Math. J. 14 (1947), 1139–1140.

[2] —, *A problem of Dickson*, ibid. 19 (1952), 471–474.

[3] E. M. Hanine, *Équations diophantiennes modulo* p^2, Colloq. Math. 64 (1993), 275–286.

[4] K. Ireland and M. Rosen, *Classical Introduction to Number Theory*, 2nd ed., Springer, 1990.

[5] D. J. Lewis, *Singular quartic forms*, Duke Math. J. 21 (1954), 39–44.

[6] W. M. Schmidt, *Equations over Finite Fields, An Elementary Approach*, Lecture Notes in Math. 536, Springer, 1976.

LABORATOIRE D'ALGÈBRE
UNIVERSITÉ PAUL SABATIER
118 ROUTE DE NARBONNE
31062 TOULOUSE CEDEX, FRANCE

Reçu le 29.11.1992
et révisé le 24.2.1994 (2349)